Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 37 (2004) 707–716
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

An objective representation of the Gaussian integers

Marcelo Fiore[a,*], Tom Leinster[b]

[a] *Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK*
[b] *Department of Mathematics, University of Glasgow, Glasgow G12 8QW, UK*

Received 20 December 2002; accepted 6 October 2003

Abstract

A rig is a r*i*ng without *n*egatives. We analyse the free rig on a generator x subject to the equivalence $x \sim 1 + x + x^2$, showing that in it the non-constant polynomials form a ring. This ring can be identified with the Gaussian integers, which thus acquire objective meaning.

1. Introduction

Quotient polynomial rings serve as mathematical models in a wide variety of applications and have been extensively studied; see, e.g. Buchberger and Winkler (1998). The corresponding situation for rigs (also known as semirings) is underdeveloped. The interest for investigating this is that rigs provide direct mathematical models in scenarios where additive inverses have, a priori, no meaning or interpretation.

One such scenario arises naturally in the context of category theory, and yields applications in programming and type theory. Consider the notion of a *distributive category*: a category with finite sums and finite products with the latter distributing over the former. In such a category, sums and products endow the set of isomorphism classes of objects with the structure of a rig, its so-called *Burnside rig*. The Burnside rig of a distributive category is in fact a ring iff the category is trivial. Thus the natural algebraic structure arising in this context is that of a rig rather than a ring.

* Corresponding author. Tel.: +44-1223-334622; fax: +44-1223-334678.
E-mail address: Marcelo.Fiore@cl.cam.ac.uk (M. Fiore).

0747-7171/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2003.10.002

Following the investigations of Lawvere (1991) and Blass (1995), Gates (1998) showed that the Burnside rig of the free distributive category $\mathcal{D}[X]/(X \cong p(X))$ on a generator X equipped with an isomorphism $X \cong p(X)$, where $p \in \mathbb{N}[x]$ has non-zero constant term, is the quotient polynomial rig $\mathbb{N}[x]/(x = p(x))$ of the rig $\mathbb{N}[x]$ under the least congruence identifying x and $p(x)$. Thus the structure of $\mathbb{N}[x]/(x = p(x))$ and calculations in it give information on the isomorphisms satisfied by objects $X \cong p(X)$ in distributive categories. For instance, suppose that $p_1, p_2 \in \mathbb{N}[x]$ with $p_1 = p_2$ in $\mathbb{N}[x]/(x = p(x))$: then for all objects X of a distributive category $\mathcal{D}$,

$$X \cong p(X) \Longrightarrow p_1(X) \cong p_2(X).$$

Moreover, every derivation of the equality in the algebra $\mathbb{N}[x]/(x = p(x))$ yields an isomorphism in the category $\mathcal{D}$.

The distributive categories $\mathcal{D}[X]/(X \cong p(X))$ can be described as categories with objects given by types (e.g., the generator amounts to a recursively defined type) and morphisms given by programs. The use of the rig $\mathbb{N}[x]/(x = p(x))$ in this context yields interesting applications to programming and type theory; see Fiore (2004) for details.

In Fiore and Leinster (in press) and Fiore (2004), we started the study of the quotient polynomial rigs $\mathbb{N}[x]/(x = p(x))$ where $p \in \mathbb{N}[x]$ has a non-zero constant term; Fiore and Leinster (in press) contains the case of polynomials p with degree at least two, and Fiore (2004) encompasses all polynomials. Among other things, we showed that these quotient polynomial rigs have a decidable word problem. The result for polynomials p of degree at least two is obtained as a consequence of the following decomposition:

$$\mathbb{N}[x]/(x = p(x)) \cong \mathbb{N} \uplus \mathbb{Z}[x]/(x - p(x)) \tag{1}$$

which gives a complete and well-understood description of the rig. Here $\uplus$ is disjoint union and the algebraic structure of the right-hand side has additive and multiplicative units respectively given by 0 and 1, addition extended by the obvious action of $\mathbb{N}$ on $\mathbb{Z}[x]/(x - p(x))$, and multiplication extended freely. (The corresponding decomposition result for linear p is more subtle: see Fiore, 2004.)

In particular, $\mathbb{Z}[x]/(x - p(x))$ embeds as the set of (equivalence classes of) non-constant polynomials in $\mathbb{N}[x]/(x = p(x))$; addition and multiplication are preserved by this embedding, but the additive and multiplicative units of $\mathbb{Z}[x]/(x - p(x))$ correspond, inevitably, to elements of $\mathbb{N}[x]/(x = p(x))$ other than 0 and 1. There are two remarkable aspects to this: first, that the non-constant elements of the rig $\mathbb{N}[x]/(x = p(x))$ carry a ring structure at all, and second, that this ring is $\mathbb{Z}[x]/(x - p(x))$, which can be thus realised by isomorphism classes of objects in $\mathcal{D}[X]/(X \cong p(X))$.

In this companion paper to Fiore and Leinster (in press) and Fiore (2004) we analyse one important example of the above situation in detail: the case $p(x) = 1 + x + x^2$. There are various reasons for doing this. One is that we can establish the decomposition (1) in a very simple, though insightful, manner, and can prove the further result (akin to the situation in the theory of Gröbner bases for rings) that the word problem can be solved by a finite strongly normalising reduction system. Whether this kind of result holds in

generality is open. Another motivation, which gives name to this paper, is to show that the ring of Gaussian integers

$$\mathbb{Z}[x]/(1+x^2) \cong \mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{C}$$

has objective meaning in the sense that it arises as the set of isomorphism classes of objects in a distributive category with the algebraic operations of addition and multiplication corresponding respectively to the categorical operations of sum and product. (Recall from above that the additive and multiplicative units cannot arise as the initial and terminal objects.) We leave open the problem of finding a distributive category with Burnside rig $\mathbb{N}[x]/(x = 1 + x + x^2)$ which would provide the Gaussian integers with an even more direct (e.g. combinatorial, geometric, or topological) objective meaning.

Section 2 presents the results of the paper, whilst Section 3 gives an application to programming and type theory using the following argument (which we invite the reader to consider before studying the rest of the paper). Since, as we will see shortly, the identity $x = x^5$ holds in $\mathbb{N}[x]/(x = 1 + x + x^2)$, it follows that in any distributive category the implication

$$X \cong 1 + X + X^2 \Longrightarrow X \cong X^5 \tag{2}$$

holds. In particular, for the distributive category of sets and functions (with additive structure given by the empty set and disjoint union, and multiplicative structure given by the singleton and cartesian product) the set of *Motzkin trees* (that is, unlabelled planar unary- and/or binary-branching trees) clearly satisfies the hypothesis of the implication (2). Thus, there is an isomorphism in the language of distributive categories (not merely in set theory) between the sets of Motzkin trees and five-tuples of Motzkin trees.

2. Results

A *rig* is a set R equipped with elements 0 and 1 and binary operations $+$ and $\cdot$ such that $(R, 0, +)$ is a commutative monoid, $(R, 1, \cdot)$ is a monoid, and the distributive laws

$$\begin{array}{cc} 0 = a0 & 0 = 0a \\ ab + ac = a(b + c) & ba + ca = (b + c)a \end{array}$$

hold for all $a, b, c \in R$.

The free rig on a generator x is the set of polynomials $\mathbb{N}[x]$ with natural number coefficients equipped with the usual addition and multiplication of polynomials and their respective units. The main object of study in this paper is the quotient polynomial rig

$$\mathbb{N}[x]/(x = 1 + x + x^2)$$

defined as the quotient rig $\mathbb{N}[x]/\sim$, where $\sim$ is the smallest congruence on the rig $\mathbb{N}[x]$ satisfying $x \sim 1 + x + x^2$.

While studying the work of Blass (1995) we noticed that there is an unfolding/folding procedure that works well as a calculational heuristic method for establishing many identities in quotient polynomial rigs $\mathbb{N}[x]/(x = p(x))$. In exploring the quotient polynomial rig $\mathbb{N}[x]/(x = 1 + x + x^2)$ we soon observed that the generator x behaves

very much like the imaginary unit. For instance, we have $x \sim x^5$. This can be seen from the following calculation, exemplifying the unfolding/folding procedure referred to above, in which an unfolding step replaces x^{n+1} with $x^n + x^{n+1} + x^{n+2}$ ($n \geq 0$) whilst a folding step does the opposite.

$$\begin{aligned}
x &\sim 1 + x + x^2 && \text{(unfolding } x\text{)} \\
&\sim 1 + x + x + x^2 + x^3 && \text{(unfolding } x^2\text{, aiming at cancelling 1)} \\
&\sim x + x + x^3 && \text{(cancelling 1 and } x^2 \text{ by folding } 1 + x + x^2\text{)} \\
&\sim x + x + x^2 + x^3 + x^4 && \text{(unfolding } x^3\text{, aiming at cancelling } x\text{)} \\
&\sim x + x^2 + x^4 && \text{(cancelling } x \text{ and } x^3 \text{ by folding } x + x^2 + x^3\text{)} \\
&\sim x + x^2 + x^3 + x^4 + x^5 && \text{(unfolding } x^4\text{, aiming at cancelling } x\text{)} \\
&\sim x^2 + x^4 + x^5 && \text{(cancelling } x \text{ and } x^3 \text{ by folding } x + x^2 + x^3\text{)} \\
&\sim x^2 + x^3 + x^4 + x^5 + x^5 && \text{(unfolding } x^4\text{, aiming at cancelling } x^2\text{)} \\
&\sim x^3 + x^5 + x^5 && \text{(cancelling } x^2 \text{ and } x^4 \text{ by folding } x^2 + x^3 + x^4\text{)} \\
&\sim x^3 + x^4 + x^5 + x^5 + x^6 && \text{(unfolding } x^5\text{, aiming at cancelling } x^3\text{)} \\
&\sim x^4 + x^5 + x^6 && \text{(cancelling } x^3 \text{ and } x^5 \text{ by folding } x^3 + x^4 + x^5\text{)} \\
&\sim x^5 && \text{(cancelling } x^4 \text{ and } x^6 \text{ by folding } x^4 + x^5 + x^6\text{).}
\end{aligned}$$

The reasons for which this calculation goes through are explained by the following proposition.

Let $\underline{-1} = x^2$, $\underline{0} = 1 + \underline{-1}$, and $\underline{1} = 1 + \underline{0}$ in $\mathbb{N}[x]$.

Proposition 1. (1) *For $n \geq 0$, $x^n\underline{0} \sim \underline{0}$.*

(2) *For all non-constant p in $\mathbb{N}[x]$, $p + \underline{0} \sim p$.*

(3) *For all non-zero p in $\mathbb{N}[x]$, $p\underline{0} \sim \underline{0}$.*

(4) *For all non-constant p in $\mathbb{N}[x]$, $p\underline{1} \sim p$.*

(5) *For all non-zero p in $\mathbb{N}[x]$, $p + \underline{-1}p \sim \underline{0}$.*

(6) *For all non-constant p, q in $\mathbb{N}[x]$ and for any r in $\mathbb{N}[x]$, the cancellation law*

$$p + r \sim q + r \implies p \sim q$$

holds.

(7) *For p in $\mathbb{N}[x]$ and n in $\mathbb{N}$, $p \sim n$ if and only if $p = n$.*

Proof. (1) $x\underline{0} = x + x^3 \sim 1 + x + x^2 + x^3 \sim 1 + x^2 = \underline{0}$.

(2) Since $x + \underline{0} \sim x$, we also have that

$$x^{n+1} + \underline{0} \sim x^{n+1} + x^n\underline{0} = x^n(x + \underline{0}) \sim x^{n+1}$$

for all $n \geq 0$.

(3) We have from (2) that $n\underline{0} \sim \underline{0}$ for all $n \geq 1$. Hence,

$$\left(\sum_{i \in I} x^{n_i}\right)\underline{0} = \sum_{i \in I}(x^{n_i}\underline{0}) \sim \sum_{i \in I}\underline{0} \sim \underline{0}$$

for all finite non-empty I.

(4) Follows from (2) and (3).
(5) Follows from (3).
(6) For p, q non-constant and r non-zero we have that

$$\begin{aligned} p + r \sim q + r &\implies p + r + \underline{-1}r \sim q + r + \underline{-1}r \\ &\implies p + \underline{0} \sim q + \underline{0} \\ &\implies p \sim q. \end{aligned}$$

(7) Consider the unique rig homomorphism from $\mathbb{N}[x]/(x = 1 + x + x^2)$ to the rig of countable cardinals mapping x to $\aleph_0$. □

In the light of the proposition, the previous derivation of $x = x^5$ in $\mathbb{N}[x]/(x = 1 + x + x^2)$ amounts to the following one:

$$x \sim x + \underline{0}(x^2 + x^3) = x + x^2 + x^3 + x^4 + x^5 = \underline{0}(x + x^2) + x^5 \sim x^5.$$

Theorem 2. *The subset of $\mathbb{N}[x]/(x = 1 + x + x^2)$ consisting of (equivalence classes of) non-constant polynomials, equipped with the usual addition and multiplication but with additive unit $\underline{0}$ and multiplicative unit $\underline{1}$, is a ring; negatives are given by multiplication with $\underline{-1}$. Further, this ring is (isomorphic to) the ring of Gaussian integers.*

Proof. The first part is a corollary of Proposition 1. For the second part, write R for the ring in question; then the isomorphism is given by the restriction to R of the unique generator-preserving rig homomorphism $\mathbb{N}[x]/(x = 1+x+x^2) \to \mathbb{Z}[x]/(1+x^2)$ and by the unique generator-preserving *ring* homomorphism $\mathbb{Z}[x]/(1 + x^2) \to R$. □

Explicitly, the isomorphism in the proof amounts to the mappings below.

$$\begin{array}{rcl@{\qquad}rcl} R & \to & \mathbb{Z}[i] & \mathbb{Z}[i] & \to & R \\ p(x) & \mapsto & p(i) & \pm m \pm ni & \mapsto & \underline{\pm 1}m + \underline{\pm 1}nx \ (m, n \in \mathbb{N}). \end{array}$$

It follows that the Gaussian integers are represented in $\mathbb{N}[x]/(x = 1 + x + x^2)$ by the polynomials

$$m + 1 + x^2,\ m + nx\ (n \neq 0),\ m + nx^3\ (n \neq 0),\ mx^2 + nx,\ mx^2 + nx^3 \qquad (3)$$

where $m, n \in \mathbb{N}$ are not both 0.

Remark. Proposition 1(7) and Theorem 2 together imply that $\mathbb{N}[x]/(x = 1 + x + x^2)$ is formed by extending the addition and multiplication of the rigs $\mathbb{N}$ and $\mathbb{Z}[i]$ to their disjoint union

$$\mathbb{N} \uplus (\mathbb{Z} \times \mathbb{Z})$$

with additive and multiplicative units respectively given by 0 and 1, and with addition extended by the obvious action of $\mathbb{N}$ on $\mathbb{Z}[i]$:

$$\ell + (m, n) = (m, n) + \ell = (\ell + m, n) \qquad (\ell \in \mathbb{N}, m, n \in \mathbb{Z}),$$

and multiplication extended freely:

$$\ell \cdot (m, n) = (m, n) \cdot \ell = \sum_{\ell} (m, n) \qquad (\ell \in \mathbb{N}, m, n \in \mathbb{Z}).$$

Corollary 3. *For all non-constant p and q in $\mathbb{N}[x]$ the following are equivalent.*

1. $p = q$ in $\mathbb{N}[x]/(x = 1 + x + x^2)$.
2. $p = q$ in $\mathbb{Z}[x]/(1 + x^2)$.
3. $p(i) = q(i)$ in $\mathbb{Z}[i]$.

Corollary 4. *The word problem in $\mathbb{N}[x]/(x = 1 + x + x^2)$ is decidable.*

Proof. Given two polynomials in $\mathbb{N}[x]$, if they are both non-constant then evaluate them at i and test for equality in $\mathbb{Z}[i]$; otherwise, by Proposition 1(7), they are equivalent if and only if they are equal. □

Our analysis yields an algorithm for obtaining a derivation of the equality of two polynomials in $\mathbb{N}[x]/(x = 1 + x + x^2)$. Indeed, for non-constant p and q in $\mathbb{N}[x]$ use the division algorithm in $\mathbb{Z}[x]$ to obtain

$$p(x) - q(x) = (w_1(x) - w_2(x))(1 + x^2) + r(x)$$

with w_1, w_2 in $\mathbb{N}[x]$ and with remainder r satisfying $r = 0$ or $0 \leq \deg(r) \leq 1$. By Corollary 3, p and q are equal in $\mathbb{N}[x]/(x = 1 + x + x^2)$ if and only if $r = 0$. In that case we can obtain a derivation of the equality by noticing that

$$\begin{aligned} p(x) + (w_1(x) + w_2(x))x &\sim p(x) + w_1(x)x + w_2(x)(1 + x + x^2) \\ &= q(x) + w_1(x)(1 + x + x^2) + w_2(x)x \\ &\sim q(x) + (w_1(x) + w_2(x))x \end{aligned}$$

and then deriving $p \sim q$ using the cancellation law (Proposition 1(6)).

Example 5. Since $2+i^2 = i^4$ in $\mathbb{Z}[i]$, it follows that $2+x^2 = x^4$ in $\mathbb{N}[x]/(x = 1+x+x^2)$. A derivation of this equality using the above method follows.

$$\begin{aligned} 2 + x^2 &\sim 2 + x^2 + (2 + x^2)x + \underline{-1}(2 + x^2)x \\ &\sim 2 + x^2 + 2x + x^2(1 + x + x^2) + \underline{-1}(2 + x^2)x \\ &= x^4 + 2(1 + x + x^2) + x^2x + \underline{-1}(2 + x^2)x \\ &\sim x^4 + (2 + x^2)x + \underline{-1}(2 + x^2)x \\ &\sim x^4. \end{aligned}$$

It is interesting to note that a more direct derivation of the above can be obtained by the unfolding/folding procedure:

$$\begin{aligned} 2 + x^2 &\sim 1 + 1 + x + x^2 + x^3 && \text{(unfolding } x^2\text{, aiming at cancelling 1)} \\ &\sim 1 + x + x^3 && \text{(cancelling 1 and } x^2 \text{ by folding } 1 + x + x^2\text{)} \\ &\sim 1 + x + x^2 + x^3 + x^4 && \text{(unfolding } x^3\text{, aiming at cancelling 1)} \\ &\sim x + x^3 + x^4 && \text{(cancelling 1 and } x^2 \text{ by folding } 1 + x + x^2\text{)} \\ &\sim x + x^2 + x^3 + x^4 + x^4 && \text{(unfolding } x^3\text{, aiming at cancelling } x\text{)} \\ &\sim x^2 + x^4 + x^4 && \text{(cancelling } x \text{ and } x^3 \text{ by folding } x + x^2 + x^3\text{)} \\ &\sim x^2 + x^3 + x^4 + x^4 + x^5 && \text{(unfolding } x^4\text{, aiming at cancelling } x^2\text{)} \\ &\sim x^3 + x^4 + x^5 && \text{(cancelling } x^2 \text{ and } x^4 \text{ by folding } x^2 + x^3 + x^4\text{)} \\ &\sim x^4 && \text{(cancelling } x^3 \text{ and } x^5 \text{ by folding } x^3 + x^4 + x^5\text{).} \end{aligned}$$

Theorem 6. *Two polynomials in* $\mathbb{N}[x]$ *are equal in* $\mathbb{N}[x]/(x = 1 + x + x^2)$ *if and only if they have the same normal form in the following strongly normalising reduction system:*

$$\begin{cases} x^4 \to 2 + x^2 \\ x + x^3 \to 1 + x^2 \\ x^n + 1 + x^2 \to x^n \qquad (1 \leq n \leq 3). \end{cases}$$

Proof. The reduction system is terminating, as whenever $p \to q$ we have that $p(2) > q(2)$. Further, all critical pairs are joinable and so the reduction system is also confluent.

To conclude the proof we show that the normal forms are exactly given by the constants together with the polynomial representation (3) of the Gaussian integers. That is, the normal forms are the polynomials

$$m + 1 + x^2, \qquad m + nx, \qquad m + nx^3, \qquad mx^2 + nx, \qquad mx^2 + nx^3$$

with $m, n \in \mathbb{N}$.

By successive applications of the first reduction rule (in the form of $x^{m+4} \to 2x^m + x^{m+2}$) every polynomial reduces to one of degree less than or equal to 3. Further, since $a + bx + cx^2 + dx^3 (a, b, c, d \in \mathbb{N})$ reduces to

$$(a + \min(b, d)) + (c + \min(b, d))x^2 + (b \dot{-} d)x + (d \dot{-} b)x^3,$$

normal forms are either of the form (i) $k + \ell x^2 + nx^3$ or (ii) $k + \ell x^2 + nx$ with $k, \ell, n \in \mathbb{N}$. We analyse each case in turn.

(i) If $n = 0$ then the polynomial is of the form $k + \ell x^2$; in which case, if $\ell > k$ it reduces to $(\ell - k)x^2$, and if $\ell \leq k$ it reduces to k if $\ell = 0$ and to $(k - \ell) + 1 + x^2$ if $\ell \neq 0$.

If $n \neq 0$ then the polynomial reduces to $(k \dot{-} \ell) + (\ell \dot{-} k)x^2 + nx^3$ which is either of the form $m + nx^3$ or $mx^2 + nx^3$ with $m, n \in \mathbb{N}$.

(ii) If $n = 0$ then the polynomial is of the form $k + \ell x^2$, and we are in the situation of the first case above.

If $n \neq 0$ then the polynomial reduces to $(k \dot{-} \ell) + (\ell \dot{-} k)x^2 + nx$ which is either of the form $m + nx$ or $mx^2 + nx$ with $m, n \in \mathbb{N}$. □

It follows that the word problem in $\mathbb{N}[x]/(x = 1 + x + x^2)$ is decidable in polynomial time.

Example 7. (1) For $m \geq 1$, we have that $x^{m+4} \to 2x^m + x^{m+2} \to x^m + x^{m-1} + x^{m+1} \to x^m$. Hence, as we saw in the introduction, $x^5 = x$ in $\mathbb{N}[x]/(x = 1 + x + x^2)$.

(2) In $\mathbb{N}[x]/(x = 1 + x + x^2)$, we have that $x(1 + x^3)^8 \sim 16x$. Indeed, $(1 + x^3)^2 = 1 + 2x^3 + x^6 \to^* 1 + 2x^3 + x^2 \to 2x^3$. It follows that $(1 + x^3)^4 \sim 4x^6 \to^* 4x^2$ and so $(1 + x^3)^8 \sim 16x^4 \to^* 32 + 16x^2 \to^* 17 + x^2$. Finally, $x(1 + x^3)^8 \sim 17x + x^3 \to 16x + 1 + x^2 \to 16x$.

3. An application

We conclude the paper with an application to programming and type theory.

As briefly mentioned in the introduction, the rig $\mathbb{N}[x]/(x = 1 + x + x^2)$ has straightforward objective realisation by types; see Fiore (2004) for details. Indeed, in the programming language ML, the generator is realised by the type of Motzkin trees defined as follows:

```
datatype  X = e | s of X | m of X * X
```

Importantly, calculations in the rig translate as programs that establish isomorphisms between the associated types. Thus, for instance, the identity $x = x^5$ in $\mathbb{N}[x]/(x = 1+x+x^2)$ entails an isomorphism (in the language of distributive categories) between Motzkin trees and five-tuples of Motzkin trees, and using the methods of this paper a program realising it can be automatically constructed. We illustrate this by working this example out manually.

First, consider the second derivation in Example 5 establishing the identity $x^4 = 2+x^2$ in $\mathbb{N}[x]/(x = 1 + x + x^2)$. It yields an isomorphism between

```
type X4 = X * X * X * X
```

and

```
datatype  U = o1 | o2 | p of X * X
```

given explicitly by the following program:

```
val fold1: X4 -> U = fn t => case t of

   ( e, e, e, e )           => o1

 | ( e, e, e, s(e) )        => o2

 | ( e, e, e, s(s(t)) )     => p( e, t )

 | ( e, e, e, s(m(t1,t2)) ) => p( s(t1), t2 )

 | ( e, e, e, m(t1,t2) )    => p( m(e,t1), t2 )

 | ( e, e, s(t1), t2 )      => p( m(s(e),t1), t2 )

 | ( e, e, m(t1,t2), t3 )   => p( m(s(s(t1)),t2), t3 )

 | ( e, s(t1), t2, t3 )     => p( m(s(m(e,t1)),t2), t3 )

 | ( e, m(t1,t2), t3, t4 )  => p( m(s(m(s(t1),t2)),t3), t4 )

 | ( s(t1), t2, t3, t4 )    => p( m(m(t1,t2),t3), t4 )

 | ( m(t1,t2), t3, t4, t5 ) => p( m(s(m(m(t1,t2),t3)),t4), t5 )
```

Now, following Example 7(1), we exhibit an isomorphism between the types `X * U` and `X`. A program corresponding to the derivation

$$x(2+x^2) = 2x + x^3 \sim 1 + 2x + x^2 + x^3 \sim 1 + x + x^2 \sim x$$

follows.

```
val fold2: X * U -> X = fn t => case t of

    ( t, o1 )          =>  s(t)

  | ( e, o2 )          =>  e

  | ( s(t), o2 )       =>  m(e,t)

  | ( m(t1,t2), o2 )   =>  m(s(t1),t2)

  | ( t1, p(t2,t3) )   =>  m(m(t1,t2),t3)
```

Finally, an isomorphism between the types `X * X4` and `X` can be given by composing the previous programs:

```
val fold: X * X4 -> X = fn t => case t of

    ( t1, t2to5 )  =>  fold2( t1, fold1( t2to5 ) )
```

Acknowledgements

Our calculations fell into place after a conversation with Bill Lawvere in which he mentioned a result of Steve Schanuel that the infinite-dimensional elements (see Schanuel, 1991) of some quotient polynomial rigs actually form a ring. This led to the results of this paper and the generalisations presented elsewhere (Fiore and Leinster, in press; Fiore, 2004). Marcelo Fiore was supported by an EPSRC Advanced Research Fellowship.

References

Blass, A., 1995. Seven trees in one. J. Pure Appl. Algebra 103, 1–21.

Buchberger, B., Winkler, F. (Eds.), 1998. Gröbner bases and applications. In: Proc. of the International Conference “33 Years of Groebner Bases”. London Mathematical Society Lecture Note Series, vol. 251. Cambridge University Press, Cambridge, UK.

Fiore, M., 2004. Isomorphisms of generic recursive polynomial types. In: Proc. of the 31st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. ACM Press, pp. 77–88.

Fiore, M., Leinster, T., 2002. Objects of categories as complex numbers. Adv. Math. (in press).

Gates, R., 1998. On the generic solution to $P(X) \cong X$ in distributive categories. J. Pure Appl. Algebra 125, 191–212.

Lawvere, F.W., 1991. Some thoughts on the future of category theory. In: Proc. Como 1990. Lecture Notes in Mathematics, vol. 1488. Springer-Verlag, Berlin, pp. 1–13.

Schanuel, S.H., 1991. Negative sets have Euler characteristic and dimension. In: Proc. Como 1990. Lecture Notes in Mathematics, vol. 1488. Springer-Verlag, Berlin, pp. 379–385.