A Relation-Algebraic Treatment of the Dedekind Recursion Theorem

Rudolf Berghammer(✉)

Institut für Informatik, Christian-Albrechts-Universität Kiel,
Olshausenstraße 40, 24098 Kiel, Germany
rub@informatik.uni-kiel.de

Abstract. The recursion theorem of Richard Dedekind is fundamental for the recursive definition of mappings on natural numbers since it guarantees that the mapping in mind exists and is uniquely determined. Usual set-theoretic proofs are partly intricate and become lengthy when carried out in full detail. We present a simple new proof that is based on a relation-algebraic specification of the notions in question and combines relation-algebraic laws and equational reasoning with Scott induction. It is very formal and most parts of it consist of relation-algebraic calculations. This opens up the possibility for mechanised verification. As an application we prove a relation-algebraic version of the Dedekind isomorphism theorem. Finally, we consider two variants of the recursion theorem to deal with situations which frequently appear in practice but where the original recursion theorem is not applicable.

1 Introduction

The so-called recursion theorem of Richard Dedekind, first formulated and proved in [6], pertains to the method of recursively defining mappings $f : \mathbb{N} \to A$ on the set of natural numbers $\mathbb{N}$ by first defining the value of $f(0)$ (in [6] $f(1)$, since there the natural numbers start with 1) and then defining the value of $f(n+1)$ (in [6] $f(n')$, with n' as the successor of n) subject to the value of $f(n)$, for an arbitrary natural number $n \in \mathbb{N}$. It states that there exists precisely one such mapping and this guarantees the correctness of the method. Besides the Peano axioms, Dedekind's original proof (see [6], Satz 126) decisively depends on the linear ordering of the natural numbers which, in contrast with modern approaches, is specified before addition is introduced. About fifty years later proofs have been published which do not use the order but are based only on the zero/one element and the successor mapping, that is, on the vocabulary of the Peano axioms. Two of them can be found in [9,11]. The reader interested in the history of the Dedekind recursion theorem is referred to [7,8], for example.

Nowadays the Dedekind recursion theorem is frequently presented using *Peano structures*. These are algebraic structures (N, z, s) with a non-empty carrier set N, an element $z \in N$ (the *zero element*) and a mapping $s : N \to N$ (the *successor mapping*) such that the following three axioms hold:

U. Fahrenberg et al. (Eds.): RAMiCS 2020, LNCS 12062, pp. 15–30, 2020.
https://doi.org/10.1007/978-3-030-43520-2_2

$$\left.\begin{array}{l}\forall\, x,y \in N : s(x) = s(y) \Rightarrow x = y \\ \neg\exists\, x \in N : s(x) = z \\ \forall\, A \in 2^N : z \in A \wedge (\forall\, x \in A : s(x) \in A) \Rightarrow A = N\end{array}\right\} \qquad (1)$$

Then the recursion theorem states that, given a Peano structure (N, z, s), a non-empty set A, an element $c \in A$ and a mapping $F : A \to A$, there exists precisely one mapping $f : N \to A$ with the following two properties:

$$f(z) = c \qquad \forall\, x \in N : f(s(x)) = F(f(x)) \qquad (2)$$

Modern proofs of the recursion theorem define the mapping f of (2) as a relation, viz. as the intersection of all relations R with source N and target A such that $z\,R\,c$ and for all $x \in N$ and $y \in A$ from $x\,R\,y$ it follows that $s(x)\,R\,F(y)$. For example, in [3], pages 346–348, the partly intricate proof that this intersection in fact is a univalent and total relation (that is, a mapping) and satisfies the two formulae of (2) is carried out in great detail.

Specifying the notions in question in the language of relation algebra and combining relation-algebraic calculations with Scott induction, in Sect. 3 of this paper we present a new proof of the Dedekind recursion theorem that is simpler than the purely set-theoretic proof of [3] or similar proofs. A further advantage of the new proof is that it is very formal and most parts of it consist of equational reasoning. This opens up the possibility for its mechanised verification by means of a theorem-proving tool. As an application of our relation-algebraic version of the recursion theorem we present in Sect. 4 a relation-algebraic version of the Dedekind isomorphism theorem, i.e., prove that all (relational) Peano structures are isomorphic. Finally, in Sect. 5 we consider two cases of recursive definitions of mappings which frequently appear in practice but where the original Dedekind recursion theorem is not applicable since either the mapping f to be defined is not unary or the result of $f(s(x))$ depends not only on the value of $f(x)$ but also on x. For each case we give an example and prove a corresponding variant of the relation-algebraic recursion theorem.

2 Mathematical Preliminaries

We assume the reader to be familiar with the basic concepts of partially ordered sets and complete lattices, including monotone mappings on them, basic fixpoint theory (fixpoint calculus) and the construction of direct products. Otherwise we refer to standard textbooks on ordered sets and lattices, e.g., [4,5], and to [13].

Given a partially ordered set $(A, \leq)$ that is a complete lattice, we denote the least element of A by the symbol $\bot$, the least upper bound of the subset B of A by $\bigsqcup B$ and the greatest lower bound of B by $\bigsqcap B$. Alfred Tarski's well-known fixpoint theorem (see [16]) states that each monotone mapping $f : A \to A$ has a least fixpoint, denoted as $\mu(f)$, and $\mu(f) = \bigsqcap\{x \in A \mid f(x) \leq x\}$ holds. For proving properties of $\mu(f)$ we will apply the principle of *Scott induction*, sometimes also called computational induction or fixpoint induction. Usually the principle is formulated for complete partial orders (CPOs), that is, for partially ordered sets with a least element and the property that each chain possesses a least upper bound. See [10], for example. Scott induction also works in the case of complete lattices, since complete lattices are CPOs.

Assume $(A, \leq)$ to be a complete lattice. Then a predicate P on its carrier set A is called *admissible* (for Scott induction) if for every chain C in $(A, \leq)$ the following implication is true: if for all $x \in C$ it holds $P(x)$, then $P(\bigsqcup C)$ holds, too. Now, Scott induction states that for each monotone mapping $f : A \to A$ and each admissible predicate P on A from the two conditions

$$P(\bot) \qquad\qquad \forall\, x \in A : P(x) \Rightarrow P(f(x)) \tag{3}$$

it follows that $P(\mu(f))$. The left condition of (3) is called the *induction base* and the right one the *induction step* with induction hypothesis $P(x)$. Besides the above version we will also apply a version which in [10] is called *simultaneous*. We consider the case of two complete lattices $(A, \leq_1)$ and $(B, \leq_2)$ with least elements $\bot_1 \in A$ and $\bot_2 \in B$ and two monotone mappings $f_1 : A \to A$ and $f_2 : B \to B$ only. Then if P is an admissible predicate on the direct product $A \times B$, which is ordered by the product order (that is, by $(x_1, x_2) \leq (y_1, y_2)$ iff $x_1 \leq_1 y_1$ and $x_2 \leq_2 y_2$, for all $x_1, y_1 \in A$ and $x_2, y_2 \in B$), then from the two conditions

$$P(\bot_1, \bot_2) \qquad\qquad \forall\, x \in A, y \in B : P(x, y) \Rightarrow P(f_1(x), f_2(y)) \tag{4}$$

it follows that $P(\mu(f_1), \mu(f_2))$. This principle is obtained from the original one by taking in (3) the least element $(\bot_1, \bot_2)$ of the product lattice $(A \times B, \leq)$ as $\bot$ and the product of the two mappings $f_1 : A \to A$ and $f_2 : B \to B$, defined by

$$f_1 \otimes f_2 : A \times B \to A \times B \qquad\qquad (f_1 \otimes f_2)(x, y) = (f_1(x), f_2(y)),$$

as mapping f. Namely, from the monotonicity of f_1 with respect to $\leq_1$ and of f_2 with respect to $\leq_2$ and the definition of the product order $\leq$ it follows that $f_1 \otimes f_2$ is monotone with respect to $\leq$ and $\mu(f_1 \otimes f_2) = (\mu(f_1), \mu(f_2))$.

Given complete lattices $(A, \leq_1)$ and $(B, \leq_2)$, a predicate P on the carrier set $A \times B$ of the product lattice $(A \times B, \leq)$ is admissible (for the simultaneous Scott induction described by (4)) if there exist $\bigsqcup$-distributive mappings $\alpha : A \to C$ and $\beta : B \to C$ into a complete lattice $(C, \leq_3)$ such that $P(x, y)$ iff $\alpha(x) \leq_3 \beta(y)$, for all $x \in A$ and $y \in B$, or $P(x, y)$ iff $\alpha(x) = \beta(y)$, for all $x \in A$ and $y \in B$. See e.g., [10] for a proof of this property.

We assume the reader also to be familiar with the basic concepts of (axiomatic) relation algebra as introduced in [15] by Alfred Tarski. Otherwise we refer again to standard textbooks, e.g., to [12,14].

As in [14] we work with typed relations. For given sets (or objects in case of axiomatic relation algebra) A and B we denote the set of all relations with source A and target B by $[A \leftrightarrow B]$ and write $R : A \leftrightarrow B$ instead of $R \in [A \leftrightarrow B]$. As operations and predicates on relations we use transposition R^{T}, complementation $\overline{R}$, union $R \cup S$, intersection $R \cap S$, composition $R ; S$, inclusion $R \subseteq S$ and equality $R = S$, and as special relations we use the empty relation O, the universal relation L and the identity relation I. As usual, in the latter cases we overload the symbols, i.e., avoid the binding of types to them, since all types can be derived from the context by means of the typing rules of the operations. All basic relation-algebraic laws we will apply in the remainder of the paper are well known for set-theoretic relations; their proofs from the axioms of an (axiomatic) relation algebra can be found in [14], for example.

Many important properties of relations can be specified in a quantifier-free manner using (conjunctions of) inclusions and equations between relation-algebraic expressions only. In this paper we will use that a relation $R : A \leftrightarrow B$ is univalent iff $R^{\mathsf{T}} ; R \subseteq \mathsf{I}$, total iff $R ; \mathsf{L} = \mathsf{L}$ or, equivalently, iff $\mathsf{I} \subseteq R ; R^{\mathsf{T}}$, injective iff $R ; R^{\mathsf{T}} \subseteq \mathsf{I}$ and surjective iff $R^{\mathsf{T}} ; \mathsf{L} = \mathsf{L}$ or, equivalently, iff $\mathsf{I} \subseteq R^{\mathsf{T}} ; R$. For all R and S the following implication is shown in [14] as Proposition 4.2.2.iv:

$$R \subseteq S \wedge S \text{ univalent} \wedge R \text{ total} \implies R = S. \tag{5}$$

Other results of [14] we will apply are Proposition 4.2.2.iii, stating that

$$Q \text{ univalent} \implies R ; Q \cap S = (R \cap S ; Q^{\mathsf{T}}) ; Q, \tag{6}$$

for all Q, R and S, and Proposition 2.4.2.i, stating that

$$(Q \cap R ; \mathsf{L}) ; S = Q ; S \cap R ; \mathsf{L}, \tag{7}$$

for all Q, R and S.

We also need *relational vectors*, which are relations $v : A \leftrightarrow B$ with $v = v ; \mathsf{L}$, and *relational points*, which are injective and surjective relational vectors. In case of set-theoretic relations a little reflection shows that $v : A \leftrightarrow B$ is a relational vector iff there exists a subset V of the set A such that $v = V \times B$, and it is a relational point iff additionally V is a singleton set. Hence, a set-theoretic relational vector models a subset of its source and a set-theoretic relational point models an element of its source. Therefore, the targets are irrelevant and in most applications, also of (axiomatic) relation algebra, relational vectors and points are from a set $[A \leftrightarrow \mathbf{1}]$, where $\mathbf{1}$ is a singleton set (a specific object, respectively). In this case the demand $v = v ; \mathsf{L}$ can be dropped, since it holds because the identity relation and the universal relation from $[\mathbf{1} \leftrightarrow \mathbf{1}]$ coincide.

To treat mappings with more than one argument relation-algebraically, we will use constructions related to direct products, viz. projection relations, products and pairings. Their formal introduction is postponed to Sect. 5.

3 Relation-Algebraic Version of the Recursion Theorem

In this section we formulate the recursion theorem of Dedekind in the language of relation algebra and present a proof that combines relation-algebraic calculations and Scott induction. We start with the following definition of a relational Peano structure. In a similar form its axioms can be found already in [2]. Since the Dedekind recursion theorem is a theorem on sets, in Definition 3.1 and all results we will prove in the remainder of the paper we consider relations as set-theoretic ones. But we will use only the operations of (axiomatic) relation algebra and its laws. As a consequence, our results remain true in this more general setting.

Definition 3.1. *A triple (N, z, S) is called a* relational Peano structure *if N is a non-empty set, $z : N \leftrightarrow \mathbf{1}$ is a relational point, $S : N \leftrightarrow N$ is a univalent, total and injective relation, $S ; z = \mathsf{O}$ and for all relational vectors $v : N \leftrightarrow \mathbf{1}$ from $z \cup S^{\mathsf{T}}; v \subseteq v$ it follows that $v = \mathsf{L}$.*

Compared with the notion of a Peano structure formulated in the introduction we see that the relational point $z : N \leftrightarrow \mathbf{1}$ models the zero element and the univalent, total and injective relation $S : N \leftrightarrow N$ equals the injective successor mapping. The equation $S ; z = \mathsf{O}$ is the relation-algebraic version of the second formula of (1) and that for all relational vectors $v : N \leftrightarrow \mathbf{1}$ from $z \cup S^{\mathsf{T}}; v \subseteq v$ it follows $v = \mathsf{L}$ is the relation-algebraic version of the third formula of (1). To be able to prove totality of relations by means of Scott induction, in the next lemma (following [2]) we specify the last axiom of a relational Peano structure as a least fixpoint equation. Notice, that in the remainder of the paper monotonicity of a mapping on relations always supposes inclusion as order.

Lemma 3.1. *Assume $z : N \leftrightarrow \mathbf{1}$ to be a relational vector, $S : N \leftrightarrow N$ to be a relation and the mapping g to be defined as follows:*

$$g : [N \leftrightarrow \mathbf{1}] \to [N \leftrightarrow \mathbf{1}] \qquad\qquad g(v) = z \cup S^{\mathsf{T}}; v \tag{8}$$

Then g is monotone. Furthermore, we have $\mu(g) = \mathsf{L}$ iff for all relational vectors $v : N \leftrightarrow \mathbf{1}$ from $z \cup S^{\mathsf{T}}; v \subseteq v$ it follows that $v = \mathsf{L}$.

Proof. The monotonicity of the mapping g follows from the monotonicity of union and composition. To show the second claim, we calculate as follows:

$$\begin{aligned} \mu(g) = \mathsf{L} &\iff \textstyle\bigcap\{v \in [N \leftrightarrow \mathbf{1}] \mid g(v) \subseteq v\} = \mathsf{L} && \text{fixpoint theorem} \\ &\iff \textstyle\bigcap\{v \in [N \leftrightarrow \mathbf{1}] \mid z \cup S^{\mathsf{T}}; v \subseteq v\} = \mathsf{L} && \text{by (8)} \\ &\iff \forall\, v \in [N \leftrightarrow \mathbf{1}] : z \cup S^{\mathsf{T}}; v \subseteq v \Rightarrow v = \mathsf{L} && \square \end{aligned}$$

Having specified Peano structures in the language of relation algebra, we now consider the two formulae of the recursive definition of the mapping $f : N \to A$ via (2). If we model the element $z \in N$ by the relational point $z : N \leftrightarrow \mathbf{1}$ of a relational Peano structure (N, z, S), use the univalent, total and injective relation $S : N \leftrightarrow N$ instead of the injective successor mapping $s : N \to N$, model the element $c \in A$ by the relational point $c : A \leftrightarrow \mathbf{1}$, take the mapping $F : A \to A$ as univalent and total relation from $[A \leftrightarrow A]$ and take the mapping $f : N \to A$ as univalent and total relation from $[N \leftrightarrow A]$, then the two formulae of (2) are relation-algebraically specified as follows:

$$z ; c^{\mathsf{T}} \subseteq f \qquad\qquad S ; f = f ; F \tag{9}$$

As next result we show how the two formulae of (9) can be specified by a single fixpoint equation.

Lemma 3.2. *Assume (N, z, S) to be a relational Peano structure, $c : A \leftrightarrow \mathbf{1}$ to be a relational point, $F : A \leftrightarrow A$ to be univalent and total and the mapping h to be defined as follows:*

$$h : [N \leftrightarrow A] \to [N \leftrightarrow A] \qquad\qquad h(X) = z ; c^{\mathsf{T}} \cup S^{\mathsf{T}} ; X ; F \tag{10}$$

Then h is monotone and $\mu(h) : N \leftrightarrow A$ is total. Furthermore, for all univalent and total relations $f : N \leftrightarrow A$ the two formulae of (9) hold iff $f = h(f)$.

Proof. The monotonicity of the mapping h follows again from the monotonicity of union and composition.

With regard to the totality of the relation $\mu(h)$ we prove $\mu(g) \subseteq \mu(h) ; \mathsf{L}$, with the mapping g defined by (8). We apply Scott induction (of the form (4)) with the predicate P on the direct product $[N \leftrightarrow \mathbf{1}] \times [N \leftrightarrow A]$ defined by $P(v, X)$ iff $v \subseteq X ; \mathsf{L}$, for all relational vectors $v : N \leftrightarrow \mathbf{1}$ and relations $X : N \leftrightarrow A$. Since the two equations $\alpha(v) = v$ and $\beta(X) = X ; \mathsf{L}$ define two $\bigcup$-distributive mappings $\alpha : [N \leftrightarrow \mathbf{1}] \rightarrow [N \leftrightarrow \mathbf{1}]$ and $\beta : [N \leftrightarrow A] \rightarrow [N \leftrightarrow \mathbf{1}]$, respectively, the predicate P is admissible due to the criterion mentioned in Sect. 2.

A proof of the induction base $P(\mathsf{O}, \mathsf{O})$ is trivial. For a proof of the induction step, assume an arbitrary relational vector $v : N \leftrightarrow \mathbf{1}$ and an arbitrary relation $X : N \leftrightarrow A$ such that $P(v, X)$ holds. Then we get $P(g(v), h(X))$ by the following calculation:

$$\begin{aligned}
g(v) &= z \cup S^{\mathsf{T}} ; v && \text{by (8)}\\
&\subseteq z \cup S^{\mathsf{T}} ; X ; \mathsf{L} && \text{as } P(v, X)\\
&= z \cup S^{\mathsf{T}} ; X ; F ; \mathsf{L} && F \text{ total}\\
&= z ; \mathsf{L} \cup S^{\mathsf{T}} ; X ; F ; \mathsf{L} && z \text{ relational point (i.e., vector)}\\
&= z ; c^{\mathsf{T}} ; \mathsf{L} \cup S^{\mathsf{T}} ; X ; F ; \mathsf{L} && c \text{ relational point (i.e., surjective)}\\
&= (z ; c^{\mathsf{T}} \cup S^{\mathsf{T}} ; X ; F) ; \mathsf{L} && \\
&= h(X) ; \mathsf{L} && \text{by (10)}
\end{aligned}$$

Therefore, we have $P(\mu(g), \mu(h))$, i.e., $\mu(g) \subseteq \mu(h) ; \mathsf{L}$. Now, $\mathsf{L} = \mu(h) ; \mathsf{L}$ follows from the last axiom of a relational Peano structure and Lemma 3.1.

For a proof of the remaining claim, assume an arbitrary univalent and total relation $f : N \leftrightarrow A$ to be given. To show implication "$\Longrightarrow$", suppose the two formulae of (9) to be true. We start with the following calculation:

$$\begin{aligned}
h(f) &= z ; c^{\mathsf{T}} \cup S^{\mathsf{T}} ; f ; F && \text{by (10)}\\
&= z ; c^{\mathsf{T}} \cup S^{\mathsf{T}} ; S ; f && \text{second formula of (9)}\\
&\subseteq z ; c^{\mathsf{T}} \cup f && S \text{ univalent}\\
&= f && \text{first formula of (9)}
\end{aligned}$$

In combination with Tarski's fixpoint theorem from $h(f) \subseteq f$ we get $\mu(h) \subseteq f$. Now, the desired equation $f = h(f)$ follows from the univalence of f, the totality of $\mu(h)$, inclusion $\mu(h) \subseteq f$ and implication (5). With regard to implication "$\Longleftarrow$", assume $f = h(f)$. The following proof of the first formula of (9) uses definition (10) of the mapping h and $f = h(f)$:

$$z ; c^{\mathsf{T}} \subseteq z ; c^{\mathsf{T}} \cup S^{\mathsf{T}} ; f ; F = h(f) = f$$

The second formula of (9) is shown by the following calculation:

$$\begin{aligned}
S\,;f &= S\,;h(f) && \text{as } f = h(f)\\
&= S\,;(z\,;c^\mathsf{T} \cup S^\mathsf{T}\,;f\,;F) && \text{by (10)}\\
&= S\,;z\,;c^\mathsf{T} \cup S\,;S^\mathsf{T}\,;f\,;F &&\\
&= S\,;S^\mathsf{T}\,;f\,;F && \text{axiom } S\,;z = \mathsf{O}\\
&= f\,;F && S \text{ total and injective} \qquad \Box
\end{aligned}$$

Notice, that in this proof only the univalence of the relation f is used. But from $\mu(h) \subseteq f$ and the totality of $\mu(h)$ the totality of f follows. For F only totality is applied. Now, we are able to prove the following relation-algebraic version of the recursion theorem of Dedekind. Here univalence of F is used, too.

Theorem 3.1. *Let (N, z, S) be a relational Peano structure, $c : A \leftrightarrow \mathbf{1}$ be a relational point and $F : A \leftrightarrow A$ be univalent and total. Then there exists precisely one univalent and total relation $f : N \leftrightarrow A$ that satisfies the two formulae of (9), viz. the least fixpoint $\mu(h)$ of the mapping h of (10).*

Proof. From Lemma 3.2 we already know that $\mu(h)$ is total. To prove that $\mu(h)$ is also univalent, we use Scott induction (of the form (3)) with the predicate P on the set $[N \leftrightarrow A]$ defined by $P(X)$ iff $X^\mathsf{T}\,;X \subseteq \mathsf{I}$, for all relations $X : N \leftrightarrow A$. To verify that P is admissible, assume the subset $\mathcal{C}$ of $[N \leftrightarrow A]$ to be a chain of univalent relations. Then the following calculation shows that also the union (i.e., least upper bound) $\bigcup\mathcal{C}$ is a univalent relation:

$$\begin{aligned}
(\textstyle\bigcup\mathcal{C})^\mathsf{T}\,;(\bigcup\mathcal{C}) &= (\textstyle\bigcup\{R^\mathsf{T} \mid R \in \mathcal{C}\})\,;(\bigcup\mathcal{C})\\
&= \textstyle\bigcup\{R^\mathsf{T}\,;(\bigcup\mathcal{C}) \mid R \in \mathcal{C}\}\\
&= \textstyle\bigcup\{\bigcup\{R^\mathsf{T}\,;S \mid S \in \mathcal{C}\} \mid R \in \mathcal{C}\}\\
&\subseteq \mathsf{I} && \text{see below}
\end{aligned}$$

The last step uses $\bigcup\{R^\mathsf{T}\,;S \mid S \in \mathcal{C}\} \subseteq \mathsf{I}$, for all relations $R \in \mathcal{C}$. This inclusion holds as, given any $R \in \mathcal{C}$, it holds that $R^\mathsf{T}\,;S \subseteq \mathsf{I}$, for all relations $S \in \mathcal{C}$. The latter, in turn, follows from the chain property of $\mathcal{C}$ and since all relations of $\mathcal{C}$ are univalent. Namely, given any $S \in \mathcal{C}$, in case $R \subseteq S$ we get $R^\mathsf{T}\,;S \subseteq S^\mathsf{T}\,;S \subseteq \mathsf{I}$ and in case $S \subseteq R$ we get $R^\mathsf{T}\,;S \subseteq R^\mathsf{T}\,;R \subseteq \mathsf{I}$.

A proof of the induction base $P(\mathsf{O})$ is obvious. To show the induction step, assume an arbitrary relation $X : N \leftrightarrow A$ with $P(X)$. Then $P(h(X))$ holds because of the following calculation:

$$\begin{aligned}
h(X)^\mathsf{T};h(X) &= (z\,;c^\mathsf{T} \cup S^\mathsf{T}\,;X\,;F)^\mathsf{T}\,;(z\,;c^\mathsf{T} \cup S^\mathsf{T}\,;X\,;F) && \text{by (10)}\\
&= (c\,;z^\mathsf{T} \cup F^\mathsf{T}\,;X^\mathsf{T}\,;S)\,;(z\,;c^\mathsf{T} \cup S^\mathsf{T}\,;X\,;F) &&\\
&= c\,;z^\mathsf{T};z;c^\mathsf{T} \cup c\,;z^\mathsf{T};S^\mathsf{T};X\,;F \,\cup &&\\
&\quad\; F^\mathsf{T};X^\mathsf{T};S\,;z\,;c^\mathsf{T} \cup F^\mathsf{T};X^\mathsf{T};S\,;S^\mathsf{T};X\,;F &&\\
&\subseteq \mathsf{I} && \text{see below.}
\end{aligned}$$

Concerning the last step, $c\,;z^\mathsf{T};z\,;c^\mathsf{T} \subseteq c\,;\mathsf{L}\,;c^\mathsf{T} = c\,;c^\mathsf{T} \subseteq \mathsf{I}$ uses that c is a relational point (i.e., an injective relational vector). Equation $c\,;z^\mathsf{T};S^\mathsf{T};X\,;F = \mathsf{O}$

follows from $z^{\mathsf{T}} ; S^{\mathsf{T}} = (S ; z)^{\mathsf{T}} = \mathsf{O}$, where the axiom $S ; z = \mathsf{O}$ of a relational Peano structure is applied. Also $F^{\mathsf{T}} ; X^{\mathsf{T}} ; S ; z ; c^{\mathsf{T}} = \mathsf{O}$ follows from this axiom. Finally, for $F^{\mathsf{T}} ; X^{\mathsf{T}} ; S ; S^{\mathsf{T}} ; X ; F \subseteq F^{\mathsf{T}} ; X^{\mathsf{T}} ; X ; F \subseteq F^{\mathsf{T}} ; F \subseteq \mathsf{I}$ we use that S is injective, X is univalent (due to the induction hypothesis $P(X)$) and F is univalent.

Because of $\mu(h) = h(\mu(h))$ and since $\mu(h)$ is univalent and total, from implication "$\Longleftarrow$" of Lemma 3.2 we get that the two formulae of (9) hold for the univalent and total relation $\mu(h)$, that is, we have $z ; c^{\mathsf{T}} \subseteq \mu(h)$ and $S ; \mu(h) = \mu(h) ; F$.

To show that $\mu(h)$ is the only univalent and total relation from $[N \leftrightarrow A]$ that satisfies the two formulae of (9), let an arbitrary univalent and total relation $f : N \leftrightarrow A$ be given such that $z ; c^{\mathsf{T}} \subseteq f$ and $S ; f = f ; F$. Then implication "$\Longrightarrow$" of Lemma 3.2 shows $f = h(f)$, from which $\mu(h) \subseteq f$ follows. This inclusion, the univalence of f, the totality of $\mu(h)$ and implication (5) yield $\mu(h) = f$. □

The proofs of Lemma 3.2 and Theorem 3.1 contain the decisive ideas which also will be used in Sect. 5 for proving the variants of Theorem 3.1 we have mentioned in the introduction.

4 An Application: The Isomorphism Theorem

Besides the recursion theorem a second important result of [6] is the nowadays called Dedekind isomorphism theorem (see [6], Satz 132). In modern terminology it says that for each pair of Peano structures (N, z, s) and (N_1, z_1, s_1) there exists a bijective mapping $\Phi : N \to N_1$ with the following two properties:

$$\Phi(z) = z_1 \qquad\qquad \forall\, x \in N : \Phi(s(x)) = s_1(\Phi(x)) \tag{11}$$

When translated into the language of relation algebra with relational Peano structures (N, z, S) and (N_1, z_1, S_1), the bijective mapping $\Phi : N \to N_1$ becomes a univalent, total, injective and surjective relation $\Phi : N \leftrightarrow N_1$ for which the following relation-algebraic versions of the two formulae of (11) hold:

$$z ; z_1^{\mathsf{T}} \subseteq \Phi \qquad\qquad S ; \Phi = \Phi ; S_1 \tag{12}$$

To prove the existence of such a relation Φ, we consider the monotone mapping h of (10), where the set A is instantiated by N_1, the relational point c is instantiated by $z_1 : N_1 \leftrightarrow \mathbf{1}$ and the relation F is instantiated by $S_1 : N_1 \leftrightarrow N_1$. So, the mapping we consider is given as follows:

$$h_1 : [N \leftrightarrow N_1] \to [N \leftrightarrow N_1] \qquad\qquad h_1(X) = z ; {z_1}^{\mathsf{T}} \cup S^{\mathsf{T}} ; X ; S_1 \tag{13}$$

Furthermore, we define Φ as least fixpoint of h_1, i.e. by $\Phi := \mu(h_1) : N \leftrightarrow N_1$. Then from Theorem 3.1 we get that Φ is the only univalent and total relation from $[N \leftrightarrow N_1]$ that satisfies the two formulae of (12). So, it remains to verify Φ as injective and surjective. To this end, we consider the following monotone mapping h_2 (that is again a specific instance of the mapping h of (10)):

$$h_2 : [N_1 \leftrightarrow N] \to [N_1 \leftrightarrow N] \qquad\qquad h_2(Y) = z_1 ; z^{\mathsf{T}} \cup S_1^{\mathsf{T}} ; Y ; S \tag{14}$$

It is easy to verify that the mapping $t : [N \leftrightarrow N_1] \rightarrow [N_1 \leftrightarrow N]$, defined by $t(X) = X^{\mathsf{T}}$ for all $X : N \leftrightarrow N_1$, is a lower adjoint of a Galois connection between the complete lattices $([N \leftrightarrow N_1], \subseteq)$ and $([N_1 \leftrightarrow N], \subseteq)$ and that $t \circ h_1 = h_2 \circ t$. Hence, the μ-fusion theorem of the fixpoint calculus (see [13]) yields

$$\Phi^{\mathsf{T}} = \mu(h_1)^{\mathsf{T}} = t(\mu(h_1)) = \mu(h_2).$$

This equation and the univalence and totality of $\mu(h_2)$ (a consequence of Theorem 3.1) yield the injectivity and surjectivity of Φ. Altogether, we have shown the following relation-algebraic version of the Dedekind isomorphism theorem.

Theorem 4.1. *Assume (N, z, S) and (N_1, z_1, S_1) to be relational Peano structures. Then there exists precisely one univalent, total, injective and surjective relation $\Phi : N \leftrightarrow N_1$ that satisfies the two formulae of (12), viz. the least fixpoint $\mu(h_1)$ of the mapping h_1 of (13).*

5 Variants of the Relation-Algebraic Recursion Theorem

When defining a mapping on natural numbers (or on a Peano structure) recursively, it frequently possesses, besides the argument that controls the recursion, additional arguments. An example is the following recursive definition of the addition-mapping *add* $: N \times N \rightarrow N$ on a Peano structure (N, z, s), where the first argument of *add* controls the recursion:

$$\forall\, y \in N : \mathit{add}(z, y) = y \qquad \forall\, x \in N, y \in N : \mathit{add}(s(x), y) = s(\mathit{add}(x, y)) \tag{15}$$

Since the original Dedekind recursion theorem only treats the recursive definition of unary mappings, it cannot immediately be applied to show that there exists precisely one mapping *add* $: N \times N \rightarrow N$ for which the two formulae of (15) hold. Therefore, in the following we present a corresponding variant – in terms of sets as well as in terms of relation algebra. To simplify the presentation, we consider mappings of the kind $f : N \times B \rightarrow A$ only. Taking B as a direct product $\prod_{i=1}^{n} B_i$, this also covers the case of mappings with more than two arguments.

The set-theoretic variant of the Dedekind recursion theorem we have in mind is as follows: Let (N, z, s) be a Peano structure, A and B be non-empty sets and mappings $d : B \rightarrow A$ and $G : A \rightarrow A$ be given. Then there exists precisely one mapping $f : N \times B \rightarrow A$ that satisfies the following two formulae:

$$\forall\, y \in B : f(z, y) = d(y) \qquad \forall\, x \in N, y \in B : f(s(x), y) = G(f(x, y)) \tag{16}$$

If this statement is translated into the language of relation algebra, with a relational Peano structure (N, z, S) and the mappings d and G as univalent and total relations, then we obtain the following variant of Theorem 3.1.

Theorem 5.1. *Assume (N, z, S) to be a relational Peano structure and $d : B \leftrightarrow A$ and $G : A \leftrightarrow A$ to be univalent and total. Then there exists precisely one univalent and total relation $f : N \times B \leftrightarrow A$ that satisfies the following two formulae:*

$$[\![z \,;\, \mathsf{L}, d]\!] \subseteq f \qquad (S \otimes \mathsf{I}) \,;\, f = f \,;\, G \tag{17}$$

The construction $[\![z\,;\mathsf{L}, d]\!]$ of the first formula of (17) is known as the *left pairing* or *strict join* of the point $z\,;\mathsf{L} : N \leftrightarrow A$ and the relation $d : B \leftrightarrow A$. Using point-wise notation, it relates $(x_1, x_2) \in N \times B$ with $y \in A$ iff $x_1\,(z\,;\mathsf{L})\,y$ and $x_2\,d\,y$. In other words, it relates (x_1, x_2) with y iff x_1 is the zero element and d maps x_2 to y. The construction $S \otimes \mathsf{I}$ of the second formula of (17) is called the *product* or *parallel composition* of the relations $S : N \leftrightarrow N$ and $\mathsf{I} : B \leftrightarrow B$. In a point-wise notation it relates $(x_1, x_2) \in N \times B$ with $(y_1, y_2) \in N \times B$ iff $x_1\,S\,y_1$ and $x_2\,\mathsf{I}\,y_2$. Hence, the relation $S \otimes \mathsf{I} : N \times B \leftrightarrow N \times B$ is the relational counterpart of the product $s \otimes \mathsf{I} : N \times B \to N \times B$ of the successor mapping $s : N \to N$ with the identity relation / mapping on the set B in the sense of Sect. 2.

Using relation-algebraic specifications of the two projection relations, left pairings and products and following the lines of the proof of Theorem 3.1, also Theorem 5.1 can be proved with purely relation-algebraic means. To do so, we start with the relation-algebraic definitions $[\![z\,;\mathsf{L}, d]\!] := \pi\,;z\,;\mathsf{L} \cap \rho\,;d : N \times B \leftrightarrow A$ of the left pairing and $S \otimes \mathsf{I} := \pi\,;S\,;\pi^{\mathsf{T}} \cap \rho\,;\mathsf{I}\,;\rho^{\mathsf{T}} : N \times B \leftrightarrow N \times B$ of the product, where $\pi : N \times B \leftrightarrow N$ and $\rho : N \times B \leftrightarrow B$ are the projection relations of the direct product $N \times B$. Up to isomorphism, the latter are specified relation-algebraically by the following four axioms (see also [2,14]):

$$\pi^{\mathsf{T}}\,;\pi = \mathsf{I} \qquad \rho^{\mathsf{T}}\,;\rho = \mathsf{I} \qquad \pi\,;\pi^{\mathsf{T}} \cap \rho\,;\rho^{\mathsf{T}} = \mathsf{I} \qquad \pi^{\mathsf{T}}\,;\rho = \mathsf{L} \tag{18}$$

From the first three formulae of (18) we get that the projection relations π and ρ are univalent, total and surjective. The definition of the left pairing $[\![z\,;\mathsf{L}, d]\!]$ and the univalence of ρ and d imply

$$[\![z\,;\mathsf{L}, d]\!]^{\mathsf{T}}\,;[\![z\,;\mathsf{L}, d]\!] \subseteq (\rho\,;d)^{\mathsf{T}}\,;\rho\,;d = d^{\mathsf{T}}\,;\rho^{\mathsf{T}}\,;\rho\,;d \subseteq \mathsf{I},$$

such that $[\![z\,;\mathsf{L}, d]\!]$ is univalent. Also the product $S \otimes \mathsf{I}$ is univalent, since its definition and the univalence of π and S imply

$$(S \otimes \mathsf{I})^{\mathsf{T}}\,;(S \otimes \mathsf{I}) \subseteq (\pi\,;S\,;\pi^{\mathsf{T}})^{\mathsf{T}}\,;\pi\,;S\,;\pi^{\mathsf{T}} = \pi\,;S^{\mathsf{T}}\,;\pi^{\mathsf{T}}\,;\pi\,;S\,;\pi^{\mathsf{T}} \subseteq \pi\,;\pi^{\mathsf{T}}$$

and its definition and the univalence of ρ imply

$$(S \otimes \mathsf{I})^{\mathsf{T}}\,;(S \otimes \mathsf{I}) \subseteq (\rho\,;\rho^{\mathsf{T}})^{\mathsf{T}}\,;\rho\,;\rho^{\mathsf{T}} = \rho\,;\rho^{\mathsf{T}}\,;\rho\,;\rho^{\mathsf{T}} \subseteq \rho\,;\rho^{\mathsf{T}}$$

such that the third formula of (18) yields $(S \otimes \mathsf{I})^{\mathsf{T}}\,;(S \otimes \mathsf{I}) \subseteq \pi\,;\pi^{\mathsf{T}} \cap \rho\,;\rho^{\mathsf{T}} = \mathsf{I}$. Similar calculations show that $S \otimes \mathsf{I}$ is total and injective.

After these preparations we are able to prove Theorem 5.1 with relation-algebraic means. The idea is the same as in case of Theorem 3.1. We define an appropriate monotone mapping on the set $[N \times B \leftrightarrow A]$ and verify that its least fixpoint satisfies the desired properties. Concretely, we consider the least fixpoint $\mu(h_3) : N \times B \leftrightarrow A$ of the following monotone mapping:

$$h_3 : [N \times B \leftrightarrow A] \to [N \times B \leftrightarrow A] \qquad h_3(X) = [\![z\,;\mathsf{L}, d]\!] \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G \tag{19}$$

The proof that $\mu(h_3)$ is the only univalent and total relation from $[N \times B \leftrightarrow A]$ that satisfies the two formulae of (17) is given by the following four lemmas.

Lemma 5.1. *The relation $\mu(h_3)$ is total.*

Proof. Besides the mapping h_3 of (19) we additionally consider the mapping g of (8) and show $\pi\,;\mu(g) \subseteq \mu(h_3)\,;\mathsf{L}$ using Scott induction (of the form (4)). Then the totality of the projection relation $\pi : N \times B \leftrightarrow N$ and the last axiom of a Peano structure in combination with Lemma 3.1 yield $\mathsf{L} = \pi\,;\mathsf{L} = \pi\,;\mu(g) \subseteq \mu(h_3)\,;\mathsf{L}$.

For the Scott induction we use the admissible predicate P on the direct product $[N \leftrightarrow \mathbf{1}] \times [N \times B \leftrightarrow A]$ defined by $P(v, X)$ iff $\pi\,;v \subseteq X\,;\mathsf{L}$, for all relational vectors $v : N \leftrightarrow \mathbf{1}$ and relations $X : N \times B \leftrightarrow A$. The induction base $P(\mathsf{O}, \mathsf{O})$ is obvious. To show the induction step, assume an arbitrary relational vector $v : N \leftrightarrow \mathbf{1}$ and an arbitrary relation $X : N \times B \leftrightarrow A$ with $P(v, X)$. Then the following calculation shows $P(g(v), h_3(X))$:

$$
\begin{aligned}
\pi\,;g(v) &= \pi\,;(z \cup S^{\mathsf{T}}\,;v) && \text{by (8)}\\
&= \pi\,;z \cup \pi\,;S^{\mathsf{T}}\,;v\\
&= (\pi\,;z\,;\mathsf{L} \cap \rho\,;d\,;\mathsf{L}) \cup (\pi\,;S^{\mathsf{T}} \cap \rho\,;\mathsf{L})\,;v && z \text{ vector and } \rho, d \text{ total}\\
&= (\pi\,;z\,;\mathsf{L} \cap \rho\,;d)\,;\mathsf{L} \cup (\pi\,;S^{\mathsf{T}} \cap \rho\,;\mathsf{L})\,;v && \text{by (7)}\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (\pi\,;S^{\mathsf{T}} \cap \rho\,;\mathsf{L})\,;v && \text{definition left pairing}\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (\pi\,;S^{\mathsf{T}} \cap \rho\,;\rho^{\mathsf{T}}\,;\pi)\,;v && \text{last formula of (18)}\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (\pi\,;S^{\mathsf{T}}\,;\pi^{\mathsf{T}} \cap \rho\,;\rho^{\mathsf{T}})\,;\pi\,;v && \pi \text{ univalent and (6)}\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (\pi\,;S\,;\pi^{\mathsf{T}} \cap \rho\,;\rho^{\mathsf{T}})^{\mathsf{T}}\,;\pi\,;v\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;\pi\,;v && \text{definition product}\\
&\subseteq \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;\mathsf{L} && \text{by } P(v, X)\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket\,;\mathsf{L} \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G\,;\mathsf{L} && G \text{ total}\\
&= (\llbracket z\,;\mathsf{L}, d\rrbracket \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G)\,;\mathsf{L}\\
&= h_3(X)\,;\mathsf{L} && \text{by (19)} \quad \Box
\end{aligned}
$$

Lemma 5.2. *The relation $\mu(h_3)$ is univalent.*

Proof. We use Scott induction (of the form (3)) with the admissible predicate P on the set $[N \times B \leftrightarrow A]$ defined by $P(X)$ iff $X^{\mathsf{T}}\,;X \subseteq \mathsf{I}$, for all relations $X : N \times B \leftrightarrow A$. The induction base $P(\mathsf{O})$ is obvious. To verify the induction step, let an arbitrary relation $X : N \times B \leftrightarrow A$ be given such that $P(X)$ is true. To get $P(h_3(X))$, we start with the calculation

$$
\begin{aligned}
h_3(X)^{\mathsf{T}}\,;h_3(X) &= (\llbracket z\,;\mathsf{L}, d\rrbracket \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G)^{\mathsf{T}}\,;(\llbracket z\,;\mathsf{L}, d\rrbracket \cup (S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G)\\
&= \llbracket z\,;\mathsf{L}, d\rrbracket^{\mathsf{T}}\,;\llbracket z\,;\mathsf{L}, d\rrbracket \cup \llbracket z\,;\mathsf{L}, d\rrbracket^{\mathsf{T}}\,;(S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G\, \cup\\
&\quad\; G^{\mathsf{T}}\,;X^{\mathsf{T}}\,;(S \otimes \mathsf{I})\,;\llbracket z\,;\mathsf{L}, d\rrbracket \cup G^{\mathsf{T}}\,;X^{\mathsf{T}}\,;(S \otimes \mathsf{I})\,;(S \otimes \mathsf{I})^{\mathsf{T}}\,;X\,;G\\
&\subseteq \mathsf{I} \cup (G^{\mathsf{T}}\,;X^{\mathsf{T}}\,;(S \otimes \mathsf{I})\,;\llbracket z\,;\mathsf{L}, d\rrbracket)^{\mathsf{T}} \cup G^{\mathsf{T}}\,;X^{\mathsf{T}}\,;(S \otimes \mathsf{I})\,;\llbracket z\,;\mathsf{L}, d\rrbracket
\end{aligned}
$$

using the definition (19) of the mapping h_3, some basic laws of relation algebra, that $\llbracket z\,;\mathsf{L}, d\rrbracket$, G and X are univalent (X because of the induction hypothesis $P(X)$) and that $S \otimes \mathsf{I}$ is injective. Now, the definitions of $S \otimes \mathsf{I}$ and $\llbracket z\,;\mathsf{L}, d\rrbracket$, the univalence of π and the axiom $S\,;z = \mathsf{O}$ of a relational Peano structure imply

$$
(S \otimes \mathsf{I})\,;\llbracket z\,;\mathsf{L}, d\rrbracket \subseteq \pi\,;S\,;\pi^{\mathsf{T}}\,;\pi\,;z\,;\mathsf{L} \subseteq \pi\,;S\,;z\,;\mathsf{L} = \mathsf{O} \tag{20}
$$

and in combination with the above calculation we get $P(h_3(X))$. □

Lemma 5.3. *The relation $\mu(h_3)$ satisfies the two formulae of (17).*

Proof. Using the definition of the mapping h_3 by (19) and that $\mu(h_3)$ is a fixpoint of h_3 we obtain

$$[\![z\,;\mathsf{L},d]\!] \subseteq [\![z\,;\mathsf{L},d]\!] \cup (S\otimes\mathsf{I})^{\mathsf{T}}\,;\mu(h_3)\,;G = h_3(\mu(h_3)) = \mu(h_3),$$

such that $\mu(h_3)$ satisfies the first formula of (17). The calculation

$$\begin{aligned}
(S\otimes\mathsf{I})\,;\mu(h_3) &= (S\otimes\mathsf{I})\,;h_3(\mu(h_3)) && \mu(h_3)\text{ fixpoint}\\
&= (S\otimes\mathsf{I})\,;([\![z\,;\mathsf{L},d]\!] \cup (S\otimes\mathsf{I})^{\mathsf{T}}\,;\mu(h_3)\,;G) && \text{by (19)}\\
&= (S\otimes\mathsf{I})\,;[\![z\,;\mathsf{L},d]\!] \cup (S\otimes\mathsf{I})\,;(S\otimes\mathsf{I})^{\mathsf{T}};\mu(h_3)\,;G\\
&= \mathsf{O} \cup (S\otimes\mathsf{I})\,;(S\otimes\mathsf{I})^{\mathsf{T}};\mu(h_3)\,;G && \text{by (20)}\\
&= \mu(h_3)\,;G && S\otimes\mathsf{I}\text{ total, inj.}
\end{aligned}$$

shows that $\mu(h_3)$ satisfies the second formula of (17), too. □

Lemma 5.4. *Assume $f : N\times B \leftrightarrow A$ to be univalent and total. If it satisfies the two formulae of (17), then $f = \mu(h_3)$.*

Proof. We start with the calculation

$$\begin{aligned}
h_3(f) &= [\![z\,;\mathsf{L},d]\!] \cup (S\otimes\mathsf{I})^{\mathsf{T}}\,;f\,;G && \text{by (19)}\\
&\subseteq f \cup (S\otimes\mathsf{I})^{\mathsf{T}}\,;f\,;G && \text{first formula of (17)}\\
&= f \cup (S\otimes\mathsf{I})^{\mathsf{T}}\,;(S\otimes\mathsf{I})\,;f && \text{second formula of (17)}\\
&\subseteq f && S\otimes\mathsf{I}\text{ univalent}
\end{aligned}$$

and get $\mu(h_3) \subseteq f$ due to Tarski's fixpoint theorem. This, the univalence of f, the totality of $\mu(h_3)$ (i.e., Lemma 5.1) and implication (5) yield $\mu(h_3) = f$. □

A second situation in which the original Dedekind recursion theorem is not applicable is given when the result of the expression $f(s(x))$ not only depends on the value of $f(x)$ but also on x. The following recursive definition of a mapping $sum : N \to N$ that computes the sum $\sum_{i=z}^{n} i$ by means of the addition-mapping add of (15) is an example for this:

$$sum(z) = z \qquad \forall\, x \in N : sum(s(x)) = add(sum(x), s(x))$$

Such a situation also requires a generalisation of the original Dedekind recursion theorem. The mapping F has to be binary and of type $F : A \times N \to A$ and the recursive definition (2) of $f : N \to A$ changes to the following one:

$$f(z) = c \qquad \forall\, x \in N : f(s(x)) = F(f(x), x) \tag{21}$$

When translated into the language of relation algebra, the statement that there exists precisely one mapping $f : N \to A$ that satisfies the two formulae of (21), leads to the following second variant of Theorem 3.1.

Theorem 5.2. *Assume (N, z, S) to be a relational Peano structure, $c : A \leftrightarrow \mathbf{1}$ to be a relational point and $F : A \times N \leftrightarrow A$ to be univalent and total. Then there exists precisely one univalent and total relation $f : N \leftrightarrow A$ that satisfies the following two formulae:*

$$z\,;c^{\mathsf{T}} \subseteq f \qquad\qquad S\,;f = [f,\mathsf{I}]\!]\,;F \tag{22}$$

Also Theorem 5.2 uses a relation-algebraic notion we have not introduced in Sect. 2. This is the *right pairing* or *fork* $[f,\mathsf{I}]\!]$ of the two relations $f : N \leftrightarrow A$ and $\mathsf{I} : N \leftrightarrow N$. Relation-algebraically it is defined by $[f,\mathsf{I}]\!] := f\,;\pi^{\mathsf{T}} \cap \mathsf{I}\,;\rho^{\mathsf{T}} = [\![f^{\mathsf{T}},\mathsf{I}^{\mathsf{T}}]^{\mathsf{T}} : N \leftrightarrow A \times N$, where $\pi : A \times N \leftrightarrow A$ and $\rho : A \times N \leftrightarrow N$ are now the projection relations of the direct product $A \times N$; see again [2,14]. From the definition of right pairings (generalising that of $[f,\mathsf{I}]\!]$ to arbitrary relations with the same source) and the axioms (18) we get that right pairings of univalent relations are univalent and a composition with a univalent relation from the left distributes over right pairings. These are the only new relation-algebraic properties we will use in the following proof of Theorem 5.2. Concretely, we show that the least fixpoint $\mu(h_4) : N \leftrightarrow A$ of the monotone mapping

$$h_4 : [N \leftrightarrow A] \to [N \leftrightarrow A] \qquad\qquad h_4(X) = z\,;c^{\mathsf{T}} \cup [S^{\mathsf{T}};X, S^{\mathsf{T}}]\!]\,;F \tag{23}$$

is the only univalent and total relation from $[N \leftrightarrow A]$ that satisfies the two formulae of (22). As in case of Theorem 5.1 this is obtained by four lemmas.

Lemma 5.5. *The relation $\mu(h_4)$ is total.*

Proof. By means of the mapping g of (8) and Scott induction (of the form (4)) we show $\mu(g) \subseteq \mu(h_4)\,;\mathsf{L}$, since then the totality of $\mu(g)$ yields $\mathsf{L} = \mu(h_4)\,;\mathsf{L}$. We apply the admissible predicate P on the direct product $[N \leftrightarrow \mathbf{1}] \times [N \leftrightarrow A]$ defined by $P(v, X)$ iff $v \subseteq X\,;\mathsf{L}$, for all relational vectors $v : N \leftrightarrow \mathbf{1}$ and relations $X : N \leftrightarrow A$. The induction base $P(\mathsf{O},\mathsf{O})$ is obvious. To verify the induction step, let an arbitrary relational vector $v : N \leftrightarrow \mathbf{1}$ and an arbitrary relation $X : N \leftrightarrow A$ be given such that $P(v, X)$ holds. Then we have $P(g(v), h_4(X))$ due to the following calculation:

$$\begin{array}{rll}
g(v) & = z \cup S^{\mathsf{T}}\,;v & \text{by (8)} \\
& \subseteq z \cup S^{\mathsf{T}}\,;X\,;\mathsf{L} & \text{by } P(v,X) \\
& = z \cup S^{\mathsf{T}};(X \cap \rho^{\mathsf{T}};\pi)\,;\mathsf{L} & \text{last formula of (18)} \\
& = z \cup S^{\mathsf{T}};(X\,;\pi^{\mathsf{T}} \cap \rho^{\mathsf{T}})\,;\pi\,;\mathsf{L} & \pi \text{ univalent and (6)} \\
& = z \cup S^{\mathsf{T}};[X,\mathsf{I}]\!]\,;\pi\,;\mathsf{L} & \text{definition right pairing} \\
& = z \cup [S^{\mathsf{T}};X, S^{\mathsf{T}}]\!]\,;\pi\,;\mathsf{L} & \text{prop. right pairing } (S \text{ inj.}) \\
& = z\,;c^{\mathsf{T}}\,;\mathsf{L} \cup [S^{\mathsf{T}};X, S^{\mathsf{T}}]\!]\,;\pi\,;\mathsf{L} & z \text{ and } c \text{ relational points} \\
& = z\,;c^{\mathsf{T}}\,;\mathsf{L} \cup [S^{\mathsf{T}};X, S^{\mathsf{T}}]\!]\,;F\,;\mathsf{L} & \pi \text{ and } F \text{ total} \\
& = (z\,;c^{\mathsf{T}} \cup [S^{\mathsf{T}};X, S^{\mathsf{T}}]\!]\,;F)\,;\mathsf{L} & \\
& = h_4(X)\,;\mathsf{L} & \text{by (23)}
\end{array}$$

□

Lemma 5.6. *The relation $\mu(h_4)$ is univalent.*

Proof. We use Scott induction (of the form (3)) with the admissible predicate P on the set $[N \leftrightarrow A]$ defined by $P(X)$ iff $X^{\mathsf{T}} ; X \subseteq \mathsf{I}$, for all relations $X : N \leftrightarrow A$. The induction base $P(\mathsf{O})$ holds trivially. To show the induction step, let an arbitrary relation $X : N \leftrightarrow A$ with $P(X)$ be given. For $P(h_4(X))$ we then start with the following calculation that uses the definition of h_4 via (23):

$$\begin{aligned}
h_4(X)^{\mathsf{T}} ; h_4(X) &= (z ; c^{\mathsf{T}} \cup [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F)^{\mathsf{T}} ; (z ; c^{\mathsf{T}} \cup [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F) \\
&= c ; z^{\mathsf{T}} ; z ; c^{\mathsf{T}} \cup c ; z^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F \cup \\
&\quad\; F^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!]^{\mathsf{T}} ; z ; c^{\mathsf{T}} \cup F^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!]^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F \\
&= c ; z^{\mathsf{T}} ; z ; c^{\mathsf{T}} \cup c ; z^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F \cup \\
&\quad\; (c ; z^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F)^{\mathsf{T}} \cup F^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!]^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F
\end{aligned}$$

From the proof of Theorem 3.1 we know already the inclusion $c ; z^{\mathsf{T}} ; z ; c^{\mathsf{T}} \subseteq \mathsf{I}$. That the second and third expression of the above union are empty follows from

$$z^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] = z^{\mathsf{T}} ; (S^{\mathsf{T}} ; X ; \pi^{\mathsf{T}} \cap S^{\mathsf{T}} ; \rho^{\mathsf{T}}) \subseteq z^{\mathsf{T}} ; S^{\mathsf{T}} ; X ; \pi^{\mathsf{T}} = \mathsf{O},$$

where the definition of $[S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!]$ and the axiom $S ; z = \mathsf{O}$ of a relational Peano structure are applied. To conclude the proof of $h_4(X)^{\mathsf{T}} ; h_4(X) \subseteq \mathsf{I}$ we calculate

$$F^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!]^{\mathsf{T}} ; [S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!] ; F \subseteq F^{\mathsf{T}} ; F \subseteq \mathsf{I},$$

where the right pairing $[S^{\mathsf{T}} ; X, S^{\mathsf{T}}]\!]$ is univalent as its components $S^{\mathsf{T}} ; X$ and S^{T} are univalent due to the injectivity of S and the induction hypothesis $P(X)$ and F is univalent by assumption. □

Lemma 5.7. *The relation $\mu(h_4)$ satisfies the two formulae of (22).*

Proof. The first formula of (22) holds due to

$$z ; c^{\mathsf{T}} \subseteq z ; c^{\mathsf{T}} \cup [S^{\mathsf{T}} ; \mu(h_4), S^{\mathsf{T}}]\!] ; F = h_4(\mu(h_4)) = \mu(h_4),$$

where the definition (23) of the mapping h_4 and that $\mu(h_4)$ is a fixpoint of h_4 are applied. By means of the calculation

$$\begin{aligned}
S ; \mu(h_4) &= S ; h_4(\mu(h_4)) && \mu(h_4) \text{ fixpoint} \\
&= S ; (z ; c^{\mathsf{T}} \cup [S^{\mathsf{T}} ; \mu(h_4), S^{\mathsf{T}}]\!] ; F) && \text{by (23)} \\
&= S ; z ; c^{\mathsf{T}} \cup S ; [S^{\mathsf{T}} ; \mu(h_4), S^{\mathsf{T}}]\!] ; F && \\
&= S ; [S^{\mathsf{T}} ; \mu(h_4), S^{\mathsf{T}}]\!] ; F && \text{as } S ; z = \mathsf{O} \\
&= S ; S^{\mathsf{T}} ; [\mu(h_4), \mathsf{I}]\!] ; F && \text{prop. right pairing } (S \text{ inj.}) \\
&= [\mu(h_4), \mathsf{I}]\!] ; F && S \text{ total and injective}
\end{aligned}$$

the second formula of (22) is verified. □

Lemma 5.8. *Assume $f : N \leftrightarrow A$ to be univalent and total. If it satisfies the two formulae of (22), then $f = \mu(h_4)$.*

Proof. First, we calculate as follows:

$$\begin{aligned}
h_4(f) &= z\,;c^\mathsf{T} \cup [S^\mathsf{T}; f, S^\mathsf{T}]\!]\,;F && \text{by (23)}\\
&\subseteq f \cup [S^\mathsf{T}; f, S^\mathsf{T}]\!]\,;F && \text{first formula of (22)}\\
&= f \cup S^\mathsf{T}; [f, \mathsf{I}]\!]\,;F && \text{property right pairing (S injective)}\\
&= f \cup S^\mathsf{T}; S\,;f && \text{second formula of (22)}\\
&= f && \text{S univalent}
\end{aligned}$$

This yields $\mu(h_4) \subseteq f$ due to Tarski's fixpoint theorem. From this inclusion, the univalence of f, the totality of $\mu(h_4)$ (i.e., Lemma 5.5) and implication (5) we get $\mu(h_4) = f$. □

6 Concluding Remarks

In this paper we have presented a simple new proof of the Dedekind recursion theorem that is based on a relation-algebraic specification of the notions in question and combines relation-algebraic laws and equational reasoning with Scott induction. As a simple application and using the same means, we also have shown the Dedekind isomorphism theorem. Finally, we have treated two cases where the original Dedekind recursion theorem is not applicable and have presented two variants of the relation-algebraic version of the recursion theorem. Their proofs are variations of that of the latter theorem.

It is interesting to look at how Dedekind in [6] treats mappings with more than one argument. From his explanations to the definition of addition and multiplication (see [6], Erklärung 135 and Erklärung 147) it becomes clear that he implicitly uses currying and uncurrying. For example, in case of addition he does not define a binary operation. Instead of that he fixes a natural number m and then uses Satz 126 to define recursively a unary mapping that yields for each natural number n the sum $m + n$. In Erklärung 147 he explicitly speaks of an infinite set of new mappings on N found in such a way. Also in the proof of Satz 4 of [9], where again addition is recursively defined, implicitly currying and uncurrying are used. These approaches can be generalised as given below.

Consider the recursive definition

$$g(z) = d \qquad\qquad \forall\, x \in N : g(s(x)) = G \circ g(x) \tag{24}$$

of a mapping $g : N \to A^B$, where (N, z, s) is a Peano structure and the mappings $d : B \to A$ and $G : A \to A$ are given. Since g is unary, the original Dedekind recursion theorem shows that (24) has a unique solution. We have to instantiate in (2) the set A by the set of mappings A^B, the element c by the mapping d, the mapping F by the higher-order mapping $F : A^B \to A^B$ with $F(h) = G \circ h$, for all $h \in A^B$, and the mapping f by the mapping g. From the unique solution g of (24) we then obtain the unique solution f of (16) via uncurrying, i.e., by defining $f : N \times B \to A$ as $f(x, y) = g(x)(y)$, for all $x \in N$ and $y \in B$, or, shorter, by $f := \mathit{curry}^{-1}(g)$, where curry^{-1} is the inverse of the well-known bijective currying-mapping curry. The definition of f and curry^{-1} and the formulae of

(24) allow to show that f satisfies the two formulae of (16). That it is the only mapping with this property can be shown by means of the definition of f and *curry*, the formulae of (24) and $curry^{-1}(curry(h)) = h$, for all $h : N \times B \rightarrow A$.

All proofs of Sect. 3 to Sect. 5 are very formal and its decisive parts consist of equational reasoning using laws of relation algebra. These are ideal prerequisites for mechanised theorem proving. Concerning mathematical theorems, in the last years especially the proof assistant tools Coq and Isabelle/HOL have been used in this respect. A prominent example is the formal verification of Atle Selberg's elementary proof of the *Prime Number Theorem* in Isabelle/HOL; see [1]. For the future we also plan a mechanised verification of the proofs of this paper using Coq or Isabelle/HOL.

Acknowledgement. I thank the referees for carefully reading the paper and for their very valuable suggestions.

References

1. Avigad, J., Donnelly, K., Gray, D., Raff, P.: A formally verified proof of the prime number theorem. ACM Trans. Comput. Log. **9**(1:2), 1–23 (2007)
2. Berghammer, R., Zierer, H.: Relational algebraic semantics of deterministic and nondeterministic programs. Theor. Comput. Sci. **43**, 123–147 (1986)
3. Berghammer, R.: Mathematik für die Informatik, 3rd edn. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-658-16712-7
4. Birkhoff, G.: Lattice Theory, 3rd edn. American Mathematical Society Colloquium Publications, American Mathematical Society, New York (1967)
5. Davey, B.A., Priestley, H.A.: Introduction to Lattices and Order, 2nd edn. Cambridge University Press, Cambridge (2002)
6. Dedekind, R.: Was sind und was sollen die Zahlen? Vieweg, Braunschweig (1888)
7. Kolman, V.: Zahlen. Walter de Gruyter, Berlin (2016)
8. Lamm, C.: Karl Grandjot und der Dedekindsche Rekursionssatz. Mitt. DMV **24**(1), 37–45 (2016)
9. Landau, E.: Grundlagen der Analysis. Akademische Verlagsgesellschaft, Leipzig (1930)
10. Loeckx, J., Sieber, K.: The Foundations of Program Verification, 2nd edn. Wiley, Chichester (1987)
11. Lorenzen, P.: Die Definition durch vollständige Induktion. Monatsh. Math. Phys **47**(1), 356–358 (1939)
12. Maddux, R.D.: Relation Algebras. Elsevier, Amsterdam (2006)
13. Mathematics Program Construction Group: Fixed-point calculus. Inf. Process. Lett. **53**(3), 131–136 (1995)
14. Schmidt, G., Ströhlein, T.: Relations and Graphs. Monographs on Theoretical Computer Science EATCS. Springer, Heidelberg (1993). https://doi.org/10.1007/978-3-642-77968-8
15. Tarski, A.: On the calculus of relations. J. Symb. Log. **6**(3), 73–89 (1941)
16. Tarski, A.: A lattice-theoretical fixpoint theorem and its applications. Pac. J. Math. **5**(2), 285–309 (1955)