UNIVERSITÄT AUGSBURG
Universitätsbibliothek

OPEN ACCESS
OPUS AUGSBURG

Shorter paths to graph algorithms

Bernhard Möller, Martin Russling

Angaben zur Veröffentlichung / Publication details:

Möller, Bernhard, and Martin Russling. 1994. "Shorter paths to graph algorithms." *Science of Computer Programming* 22 (1-2): 157–80. https://doi.org/10.1016/0167-6423(94)90011-6.

Nutzungsbedingungen / Terms of use: **CC BY-NC-ND 4.0**

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under these conditions:
CC-BY-NC-ND 4.0: Creative Commons: Namensnennung - Nicht kommerziell - Keine Bearbeitung
Weitere Informationen finden Sie unter: / For more information see:
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

Shorter Paths to Graph Algorithms

Bernhard Möller and Martin Russling

Institut für Mathematik, Universität Augsburg,
Universitätsstr. 2, W-8900 Augsburg, Germany,
e-mail: {moeller,russling}@uni-augsburg.de

Abstract. We illustrate the use of formal languages and relations in compact formal derivations of some graph algorithms.

1 Introduction

The transformational or calculational approach to program development has by now a long tradition (see Burstall, Darlington 1977, Bauer et al. 1985, Bauer et al. 1989, Meertens 1986, Bird 1989). In it, one starts from a (possibly non-executable) specification and transforms it into a (hopefully efficient) program using semantics-preserving rules. Many derivations, however, suffer from the use of lengthy expressions involving formulae from predicate calculus. However, in particular in the case of graph algorithms the calculus of formal languages and relations allows considerable compactification. We use a simplified and straightened version of the framework introduced in Möller 1991 to illustrate this with derivations of algorithms for computing the length of a shortest path between two graph vertices and for cycle detection.

2 The Framework

In connection with graph algorithms we use formal languages to describe sets of paths. The letters of the underlying alphabet are interpreted as graph nodes. As a special case of formal languages we consider relations of arities ≤ 2. Relations of arity 1 represent node sets, whereas binary relations represent the edge sets. The only two nullary relations (the singleton relation consisting just of the empty word and the empty relation) play the role of the Boolean values. This also allows easy definitions of assertions, conditional, and guards.

Essential operations on languages are (besides union, intersection, and difference) concatenation, composition, and join. As special cases of composition we obtain image and inverse image as well as tests for intersection, emptiness, and membership. The join corresponds to path concatenation on directed graphs; special cases yield restriction.

Proofs are either straightforward or given by Möller 1991 and therefore omitted.

2.1 Operations on Sets

Given a set A we denote by $\mathcal{P}(A)$ its **powerset**. The cardinality of A is, as usual, denoted by $|A|$. To save braces, we identify a singleton set with its only element.

Frequently, we will extend set-valued operations

$$f : A_1 \times \cdots \times A_n \to \mathcal{P}(A_{n+1}) \qquad (n > 0)$$

to the powersets $\mathcal{P}(A_i)$ of the A_i. In these cases we use the same symbol f also for the extended function

$$f : \mathcal{P}(A_1) \times \cdots \times \mathcal{P}(A_n) \to \mathcal{P}(A_{n+1})$$

defined by

$$f(U_1, \ldots, U_n) \stackrel{\text{def}}{=} \bigcup_{x_1 \in U_1} \cdots \bigcup_{x_n \in U_n} f(x_1, \ldots, x_n) \tag{1}$$

for $U_i \subseteq A_i$. By this definition, the extended operation distributes through union in all arguments:

$$f(U_1, \ldots U_{i-1}, \bigcup_{j \in J} U_{ij}, U_{i+1}, \ldots, U_n) = \bigcup_{j \in J} f(U_1, \ldots U_{i-1}, U_{ij}, U_{i+1}, \ldots, U_n) \ . \tag{2}$$

By taking $J = \emptyset$ we obtain strictness of the extended operation w.r.t. $\emptyset$:

$$f(U_1, \ldots U_{i-1}, \emptyset, U_{i+1}, \ldots, U_n) = \emptyset \ . \tag{3}$$

By taking $J = \{1, 2\}$ and using the equivalence

$$U \subseteq V \ \Leftrightarrow \ U \cup V = V$$

we also obtain monotonicity w.r.t. $\subseteq$ in all arguments:

$$\begin{array}{l} U_{i1} \subseteq U_{i2} \ \Rightarrow \\ \qquad f(U_1, \ldots U_{i-1}, U_{i1}, U_{i+1}, \ldots, U_n) \subseteq f(U_1, \ldots U_{i-1}, U_{i2}, U_{i+1}, \ldots, U_n) \ . \end{array} \tag{4}$$

Moreover, bilinear equational laws are preserved (see e.g. Lescanne 1982).

2.2 Languages and Relations

Consider an alphabet A. We denote the empty word over A by ε and concatenation by $\bullet$. It is associative, with ε as the neutral element:

$$u \bullet (v \bullet w) = (u \bullet v) \bullet w \ , \tag{5}$$

$$\varepsilon \bullet u = u = u \bullet \varepsilon \ . \tag{6}$$

As usual, a singleton word is not distinguished from the only letter it contains. The **length** of a word u, i.e., the number of letters from A in u, is denoted by

$||u||$. The **reverse** of a word $u = a_1 \bullet \cdots \bullet a_{||u||}$ is the word $u^{-1} \stackrel{\text{def}}{=} a_{||u||} \bullet \cdots \bullet a_1$. The set of all words over A is denoted by $A^{(*)}$.

A **(formal) language** is a subset of $A^{(*)}$. Concatenation is extended pointwise to languages. Since the above laws are bilinear, they carry over to languages U, V, W over A:

$$U \bullet (V \bullet W) = (U \bullet V) \bullet W \ , \tag{7}$$

$$\varepsilon \bullet U = U = U \bullet \varepsilon \ . \tag{8}$$

The **diagonal** V^{Δ} over a subset $V \subseteq A$ is defined by

$$V^{\Delta} \stackrel{\text{def}}{=} \bigcup_{x \in V} x \bullet x \ . \tag{9}$$

A **relation of arity** n is a language R such that all words in R have length n. Note that $\emptyset$ is a relation of any arity. For $R \neq \emptyset$ we denote the arity of R by $\mathsf{ar}\, R$. There are only two 0-ary relations, viz. $\emptyset$ and ε. For a relation R its **converse** R^{-1} consists of the reverses of all its words.

2.3 Composition

For languages V and W over alphabet A we define their **composition** $V\,;W$ by

$$V\,;W \stackrel{\text{def}}{=} \bigcup_{x \in A} \bigcup_{v \bullet x \in V} \bigcup_{x \bullet w \in W} v \bullet w \ . \tag{10}$$

If V and W are binary relations this coincides with the usual definition of relational composition (see e.g. Tarski 1941, Schmidt, Ströhlein 1989).

Composition is associative:

$$U\,;(V\,;W) \ = \ (U\,;V)\,;W \quad \Leftarrow \quad \forall\, y \in V : ||y|| \geq 2 \ . \tag{11}$$

Composition associates with concatenation:

$$U \bullet (V\,;W) = (U \bullet V)\,;W \quad \Leftarrow \quad \forall\, y \in V : ||y|| \geq 1 \ , \tag{12}$$

$$U\,;(V \bullet W) = (U\,;V) \bullet W \quad \Leftarrow \quad \forall\, y \in V : ||y|| \geq 1 \ . \tag{13}$$

We shall omit parentheses whenever one of these laws applies. Moreover, $\bullet$ and $;$ bind stronger than $\cup$ and $\cap$.

Interesting special cases of relational composition arise when one of the operands has arity 1. Suppose $1 = \mathsf{ar}\, R \leq \mathsf{ar}\, S$. Then

$$R\,;S \ = \ \bigcup_{x \in R} \bigcup_{x \bullet v \in S} v \ .$$

In other words, $R\,;S$ is the image of R under S. Likewise, if $1 = \mathsf{ar}\, T \leq \mathsf{ar}\, S$, then $S\,;T$ is the inverse image of T under S. For these reasons we may define domain and codomain of a binary relation R by

$$\mathsf{dom}\, R \stackrel{\text{def}}{=} R\,;A \ , \tag{14}$$

$$\mathsf{cod}\, R \stackrel{\text{def}}{=} A\,;R \ . \tag{15}$$

Suppose now $\mathsf{ar}\, R = 1 = \mathsf{ar}\, S$ and $||x|| = 1 = ||y||$. Then

$$R\,;S = \begin{cases} \varepsilon \text{ if } R \cap S \neq \emptyset \ , \\ \emptyset \text{ if } R \cap S = \emptyset \ , \end{cases} \tag{16}$$

$$R\,;R = \begin{cases} \varepsilon \text{ if } R \neq \emptyset \ , \\ \emptyset \text{ if } R = \emptyset \ , \end{cases} \tag{17}$$

$$x\,;R = R\,;x = \begin{cases} \varepsilon \text{ if } x \in R \ , \\ \emptyset \text{ if } x \notin R \ , \end{cases} \tag{18}$$

$$x\,;y = y\,;x = \begin{cases} \varepsilon \text{ if } x = y \ , \\ \emptyset \text{ if } x \neq y \ . \end{cases} \tag{19}$$

Because these "tests" will be used frequently, we introduce more readable notations for them by setting

$$R \neq \emptyset = R\,;R \ , \tag{20}$$

$$x \in R = x\,;R \ , \tag{21}$$

$$(x = y) = x\,;y \ , \tag{22}$$

$$R \subseteq S = (R \cup S = S) \ . \tag{23}$$

For binary R and $x \in \mathsf{dom}\, R, y \in \mathsf{cod}\, R$ we have

$$x\,;R\,;y = \begin{cases} \varepsilon \text{ if } x \bullet y \in R \ , \\ \emptyset \text{ otherwise } . \end{cases} \tag{24}$$

Finally, we note that diagonals are neutral w.r.t. composition. Assume $P \supseteq \mathsf{dom}\, V$ and $Q \supseteq \mathsf{cod}\, V$. Then

$$P^{\Delta}\,;V = V \ , \tag{25}$$

$$V\,;Q^{\Delta} = V \ . \tag{26}$$

2.4 Assertions

As we have just seen, the nullary relations ε and $\emptyset$ characterize the outcomes of certain test operations. More generally, they can be used instead of Boolean values; therefore we call expressions yielding nullary relations **assertions**. Note that in this view "false" and "undefined" both are represented by $\emptyset$. Negation is defined by

$$\overline{\emptyset} \stackrel{\text{def}}{=} \varepsilon \ , \tag{27}$$

$$\overline{\varepsilon} \stackrel{\text{def}}{=} \emptyset \ . \tag{28}$$

Note that this operation is not monotonic.

For assertions B, C we have e.g. the properties

$$B \bullet C = B \cap C \ , \tag{29}$$

$$B \bullet B = B \ , \tag{30}$$
$$B \bullet \overline{B} = \emptyset \ , \tag{31}$$
$$B \cup \overline{B} = \varepsilon \ , \tag{32}$$
$$\overline{B \bullet C} = \overline{B} \cup \overline{C} \ . \tag{33}$$

Conjunction and disjunction of assertions are represented by their intersection and union. To improve readability, we write $B \wedge C$ for $B \cap C = B \bullet C$ and $B \vee C$ for $B \cup C$.

For assertion B and arbitrary language R we have

$$B \bullet R = R \bullet B = \begin{cases} R \text{ if } B = \varepsilon \ , \\ \emptyset \text{ if } B = \emptyset \ . \end{cases} \tag{34}$$

Hence $B \bullet R$ (and $R \bullet B$) behaves like the expression

$$B \rhd R = \mathsf{if}\ B\ \mathsf{then}\ R\ \mathsf{else}\ \mathsf{error}\ \mathsf{fi}$$

in Möller 1989. We will use this construct for propagating assertions through recursions.

2.5 Conditional

Using assertions we can also define a conditional by

$$\mathsf{if}\ B\ \mathsf{then}\ R\ \mathsf{else}\ S\ \mathsf{fi} \stackrel{\text{def}}{=} B \bullet R \ \cup \ \overline{B} \bullet S \ , \tag{35}$$

for assertion B and languages R, S. Note that this operation is not monotonic in B.

2.6 Join

A useful derived operation is provided by a special case of the join operation as used in database theory (see e.g. Date 1988). Given two languages R, S, their **join** $R \bowtie S$ consists of all words that arise from "glueing" together words from R and from S along a common intermediate letter. By our previous considerations, the beginnings of words ending with $x \in A$ are obtained as $R\,;x$ whereas the ends of words which start with x are obtained as $x\,;S$. Hence we define

$$R \bowtie S \stackrel{\text{def}}{=} \bigcup_{x \in A} R\,;x \bullet x\,;S \ . \tag{36}$$

Again, $\bowtie$ binds stronger than $\cup$ and $\cap$.

Join and composition are closely related. To explain this we consider two binary relations $R, S \subseteq A \bullet A$:

$$R\,;S = \bigcup_{z \in A} \{x \bullet y : x \bullet z \in R \wedge z \bullet y \in S\} \ ,$$
$$R \bowtie S = \bigcup_{z \in A} \{x \bullet z \bullet y : x \bullet z \in R \wedge z \bullet y \in S\} \ .$$

Thus, whereas $R\,;S$ just states whether there is a path from x to y via some point $z \in A$, the relation $R \bowtie S$ consists of exactly those paths $x \bullet z \bullet y$. In particular, the relations

$$\begin{array}{c} R \ , \\ R \bowtie R \ , \\ R \bowtie (R \bowtie R) \ , \\ \vdots \end{array}$$

consist of the paths of edge numbers $1, 2, 3, \ldots$ in the directed graph associated with R.

Other interesting special cases arise when the join is taken w.r.t. the minimum of the arities involved. Suppose $1 = \mathsf{ar}\, R \leq \mathsf{ar}\, S$. Then

$$\begin{aligned} & R \bowtie S \\ = & \bigcup_{x \in A} R\,; x \bullet x \bullet x\,; S \\ = & \bigcup_{x \in R} x \bullet x\,; S \ . \end{aligned}$$

In other words, $R \bowtie S$ is the restriction of S to R. Likewise, for T with $1 = \mathsf{ar}\, T \leq \mathsf{ar}\, S$, the language $S \bowtie T$ is the corestriction of S to T.

If even $\mathsf{ar}\, R = \mathsf{ar}\, S = 1$ we have

$$R \bowtie S = R \cap S \ . \tag{37}$$

In particular, if $\mathsf{ar}\, R = 1$ and $||x|| = 1 = ||y||$,

$$R \bowtie R = R \ , \tag{38}$$

$$x \bowtie R = R \bowtie x = \begin{cases} x \text{ if } x \in R \ , \\ \emptyset \text{ if } x \notin R \ , \end{cases} \tag{39}$$

$$x \bowtie y = y \bowtie x = \begin{cases} x \text{ if } x = y \ , \\ \emptyset \text{ if } x \neq y \ . \end{cases} \tag{40}$$

For binary R, $x \in \mathsf{dom}\, R$, and $y \in \mathsf{cod}\, R$ this implies

$$x \bowtie R \bowtie y = \begin{cases} x \bullet y \text{ if } x \bullet y \in R \ , \\ \emptyset \quad \text{otherwise} \ . \end{cases} \tag{41}$$

In special cases the join can be expressed by a composition: Assume $\mathsf{ar}\, P = 1 = \mathsf{ar}\, Q$. Then

$$P \bowtie R = P^{\Delta}\,; R \ , \tag{42}$$

$$R \bowtie Q = R\,; Q^{\Delta} \ . \tag{43}$$

By the associativity of composition (11) also join and composition associate:

$$(R \bowtie S)\,; T = R \bowtie (S\,; T) \ , \tag{44}$$

$$R\,; (S \bowtie T) = (R\,; S) \bowtie T \ , \tag{45}$$

provided $\mathsf{ar}\, S \geq 2$.

Moreover, also joins associate:

$$R \bowtie (S \bowtie T) = (R \bowtie S) \bowtie T \ . \tag{46}$$

2.7 Kleene Algebras and Closures

A **Kleene algebra** (see Conway 1971) is a tuple $(S, \Sigma, \circ, 0, 1)$ consisting of a set S, operations $\Sigma : \mathcal{P}(S) \to S$, $\circ : S \bullet S \to S$ and elements $0, 1 \in S$ such that $(S, \circ, 1)$ is a monoid and

$$\begin{array}{rcll} \Sigma\,\emptyset & = & 0 & , \\ \Sigma\,\{x\} & = & x & (x \in S) \ , \\ \Sigma(\cup\mathcal{K}) & = & \Sigma\,\{\Sigma\,K : K \in \mathcal{K}\} & (\mathcal{K} \subseteq \mathcal{P}(S)) \ , \\ \Sigma\,(K \circ L) & = & (\Sigma\,K) \circ (\Sigma\,L) & (K, L \in \mathcal{P}(S)) \ , \end{array} \tag{47}$$

where in this latter equation $\circ$ is the pointwise extension of the monoid operation. Note that this implies that 0 is a zero with respect to $\circ$ or, in other words, that $\circ$ is strict with respect to 0:

$$0 \circ x \ = \ 0 \ = \ x \circ 0 \ . \tag{48}$$

The binary version of Σ is

$$x + y \stackrel{\text{def}}{=} \Sigma\,\{x, y\} \ , \tag{49}$$

which makes $(S, +, 0)$ a commutative monoid. By our definitions, for an alphabet A,

$$\begin{array}{rcl} LAN & \stackrel{\text{def}}{=} & (\mathcal{P}(A^{(*)}),\ \bigcup, \bullet,\ \emptyset,\ \varepsilon) \ , \\ REL & \stackrel{\text{def}}{=} & (\mathcal{P}(A \bullet A),\ \bigcup,\ ;,\ \emptyset,\ A^{\Delta}) \ , \\ PAT & \stackrel{\text{def}}{=} & (\mathcal{P}(A^{(*)}\backslash\varepsilon),\ \bigcup,\ \bowtie,\ \emptyset,\ A) \ , \end{array}$$

all form Kleene algebras. Given a Kleene algebra one can define a partial order $\leq$ by

$$x \leq y \stackrel{\text{def}}{\Leftrightarrow} x + y \ = \ y \ . \tag{50}$$

This makes $(S, \leq)$ into a complete lattice. Moreover, $\circ$ is continuous w.r.t. $\leq$. In our examples $\leq$ coincides with $\subseteq$. One can then define a **closure** operator $.^*$ by

$$x^* \stackrel{\text{def}}{=} \mu\, y\,.\ 1 + x \circ y \ , \tag{51}$$

where μ is the least fixpoint operator. Using continuity we can represent the closure also by Kleene's approximation sequence (see Kleene 1952) as

$$x^* \ = \ \Sigma\{x^j : j \in \mathbb{N}\} \ , \tag{52}$$

where

$$x^0 \stackrel{\text{def}}{=} 1 \ , \tag{53}$$

$$x^{j+1} \stackrel{\text{def}}{=} x \circ x^j \ . \tag{54}$$

For our particular Kleene algebras we denote the closure operations by $.^{(*)}$, $.^*$, and $.^{\Rightarrow}$, resp.

Consider now a binary relation $R \subseteq A \bullet A$ and let G be the directed graph associated with R, i.e., the graph with vertex set A and arcs between the vertices corresponding to the pairs in R. We have, in REL,

$$x \,;\, R^i \,;\, y = \begin{cases} \varepsilon \text{ if there is a path with } i \text{ edges from } x \text{ to } y \text{ in } G \ , \\ \emptyset \text{ otherwise } . \end{cases} \tag{55}$$

Hence,

$$x \,;\, R^* \,;\, y = \begin{cases} \varepsilon \text{ if there is a path from } x \text{ to } y \text{ in } G \ , \\ \emptyset \text{ otherwise } . \end{cases} \tag{56}$$

For $S \subseteq A$, the set $S \,;\, R^*$ gives all points in A reachable from points in S via paths in G, whereas $R^* ; S$ gives all points in A from which some point in S can be reached. Finally,

$$S \,;\, R^* ; T = \begin{cases} \varepsilon \text{ if } S \text{ and } T \text{ are connected by some path in } G \ , \\ \emptyset \text{ otherwise } . \end{cases} \tag{57}$$

As usual, we set

$$R^+ \stackrel{\text{def}}{=} R \,;\, R^* \;=\; R^* \,;\, R \ . \tag{58}$$

Analogously the path closure $R^{\Rightarrow}$ in PAT consists of all finite paths in G. Hence

$$x \bowtie R^{\Rightarrow} \bowtie y \tag{59}$$

is the language of all paths between x and y in G.

Moving away from the graph view, the path closure also is useful for general binary relations. Let e.g. $\leq$ be a partial order. Then $\leq^{\Rightarrow}$ is the language of all $\leq$-non-decreasing sequences. If $\leq$ is even a linear order then $\leq^{\Rightarrow}$ is the language of all sequences which are sorted w.r.t. $\leq$. This is exploited in Möller 1993b, Russling 1992 for the derivation of sorting algorithms.

We now state some important induction principles for closures. We call a predicate P over a Kleene algebra $(S, \Sigma, \circ, 0, 1)$ **continuous** if for all $T \subseteq S$

$$(\bigwedge_{x \in T} P[x]) \;\Rightarrow\; P[\Sigma\, T] \ . \tag{60}$$

Lemma 1. *Consider a fixed $z \in S$ and let P be continuous. If $P[1]$ and $P[x] \Rightarrow P[z \circ x]$ or $P[x] \Rightarrow P[x \circ z]$ then $P[z^*]$ holds as well.*

Proof. A straightforward induction shows $P[z^i]$ for all $i \in \mathbb{N}$. Now Kleene's approximation (52) and continuity show the claim. □

Corollary 1. *Consider fixed $U \in \mathcal{P}(A^{(*)})$, $R \subseteq A \bullet A$ and suppose that P is a continuous predicate on $\mathcal{P}(A^{(*)})$. If $P[U]$ and $P[V] \Rightarrow P[V \,;\, R]$ then $P[U \,;\, R^*]$ as well.*

Proof. Define $Q[X]$ over $\mathcal{P}(A \bullet A)$ by

$$Q[X] \stackrel{\text{def}}{\Leftrightarrow} P[U \,;\, X] \ .$$

Then Q satisfies the assumptions of Lemma 1 showing the claim. □

A variant of the general induction principle of Lemma 1 allows us to extend properties of x to x^*:

Lemma 2. *Let P be continuous and assume $P[1]$ and $P[x] \wedge P[y] \Rightarrow P[x \circ y]$. Then $P[x] \Rightarrow P[x^*]$ holds as well.*

Proof. Analogous to the proof of Lemma 1. □

We shall see various applications of these principles later on.

3 Graph Algorithms

We now want to apply the framework in case studies of some simple graph algorithms.

3.1 Length of a Shortest Connecting Path

Specification and First Recursive Solution. We consider a finite set A of vertices and a binary relation $R \subseteq A \bullet A$. The problem is to find the length of a shortest path from a vertex x to a vertex y. Therefore we define

$$\mathit{shortestpath}(x, y) \stackrel{\text{def}}{=} \mathit{min}(\mathit{edgelengths}(x \bowtie R^{\Rightarrow} \bowtie y)) \ , \tag{61}$$

where, for a set S of (non-empty) paths,

$$\mathit{edgelengths}(S) \stackrel{\text{def}}{=} \bigcup_{s \in S} (||s|| - 1) \tag{62}$$

calculates the set of path lengths, i.e., the number of edges in each path, and, for a set N of natural numbers,

$$\mathit{min}(N) \stackrel{\text{def}}{=} \begin{cases} k \text{ if } k \in N \wedge N \subseteq k; \leq \ , \\ \emptyset \text{ if } N = \emptyset \ . \end{cases} \tag{63}$$

It is obvious that *edgelengths* is strict and distributes through union. Moreover, for unary S,

$$\mathit{edgelengths}(S \bowtie T) \ = \ 1 + \mathit{edgelengths}(S \,; T) \ , \tag{64}$$

and

$$\mathit{min}(M \cup N) = \mathit{min}(\mathit{min}(M) \cup \mathit{min}(N)) \ , \tag{65}$$

$$\mathit{min}(0 \cup M) = 0 \ . \tag{66}$$

For deriving a recursive version of *shortestpath* we generalize this to a function *sp* which calculates the length of a shortest path from a set S of vertices to a vertex y:

$$\mathit{sp}(S, y) \stackrel{\text{def}}{=} \mathit{min}(\mathit{edgelengths}(S \bowtie R^{\Rightarrow} \bowtie y)) \ . \tag{67}$$

The embedding

$$shortestpath(x, y) \;=\; sp(x, y) \tag{68}$$

is straightforward.

We calculate

$$\begin{array}{ll} & sp(S, y) \\ = & \quad \{\![\text{ definition }]\!\} \\ & min(edgelengths(S \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ by (51) }]\!\} \\ & min(edgelengths(S \bowtie (A \;\cup\; R \bowtie R^{\Rightarrow}) \bowtie y)) \\ = & \quad \{\![\text{ distributivity }]\!\} \\ & min(edgelengths(S \bowtie A \bowtie y) \;\cup\; edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ by (37) }]\!\} \\ & min(edgelengths(S \bowtie y) \;\cup\; edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \;\; . \end{array}$$

By (39) the subexpression $S \bowtie y$ can be simplified according to whether $y \in S$ or not.

Case 1: $y \in S$.

$$\begin{array}{ll} & min(edgelengths(S \bowtie y) \;\cup\; edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ by (39), since } y \in S \;]\!\} \\ & min(edgelengths(y) \;\cup\; edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ definition of } edgelengths \;]\!\} \\ & min(0 \cup edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ by (66) }]\!\} \\ & 0 \;\; . \end{array}$$

Case 2: $y \notin S$.

$$\begin{array}{ll} & min(edgelengths(S \bowtie y) \;\cup\; edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ by (39), since } y \notin S \;]\!\} \\ & min(edgelengths(\emptyset) \;\cup\; edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ strictness, neutrality }]\!\} \\ & min(edgelengths(S \bowtie R \bowtie R^{\Rightarrow} \bowtie y)) \\ = & \quad \{\![\text{ by (64) }]\!\} \end{array}$$

$$
\begin{array}{ll}
 & min(1 + edgelengths(S\,;R \bowtie R^{\Rightarrow} \bowtie y)) \\
= & \quad \{\![\text{ distributivity }]\!\} \\
 & 1 + min(edgelengths(S\,;R \bowtie R^{\Rightarrow} \bowtie y)) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & 1 + sp(S\,;R\ ,\ y)\ .
\end{array}
$$

Altogether we have derived the recursion equation

$$sp(S, y)\ =\ \mathsf{if}\ y \in S\ \mathsf{then}\ 0\ \mathsf{else}\ 1 + sp(S\,;R\ ,\ y)\ \mathsf{fi}\ . \tag{69}$$

Note, however, that termination cannot be guaranteed for this recursion. To make progress in that direction we show some additional properties of sp.

Lemma 3. $sp(S \cup T\ ,\ y)\ =\ min(sp(S, y) \cup sp(T, y))$.

Proof.
$$
\begin{array}{ll}
 & sp(S \cup T\ ,\ y) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & min(edgelengths((S \cup T) \bowtie R^{\Rightarrow} \bowtie y)) \\
= & \quad \{\![\text{ distributivity }]\!\} \\
 & min(edgelengths(S \bowtie R^{\Rightarrow} \bowtie y)\ \cup\ edgelengths(T \bowtie R^{\Rightarrow} \bowtie y)) \\
= & \quad \{\![\text{ by (65) }]\!\} \\
 & min(min(edgelengths(S \bowtie R^{\Rightarrow} \bowtie y))\ \cup\ min(edgelengths(T \bowtie R^{\Rightarrow} \bowtie y))) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & min(sp(S, y) \cup sp(T, y))\ .
\end{array}
$$

□

We now consider again the case $y \notin S$. From (69) we obtain

$$sp(S\,;R\ ,\ y) \leq sp(S, y)\ , \tag{70}$$

and hence

$$
\begin{array}{ll}
 & sp(S, y) \\
= & \quad \{\![\text{ by } y \notin S \text{ and (69) }]\!\} \\
 & 1 + sp(S\,;R\ ,\ y) \\
= & \quad \{\![\text{ by (70) }]\!\} \\
 & 1 + min(sp(S, y) \cup sp(S\,;R\ ,\ y)) \\
= & \quad \{\![\text{ by Lemma 3 }]\!\} \\
 & 1 + sp(S \cup S\,;R\ ,\ y)\ ,
\end{array}
$$

so that a second recursion equation for sp is

$$sp(S, y) \;=\; \mathsf{if}\ y \in S\ \mathsf{then}\ 0\ \mathsf{else}\ 1 + sp(S \cup S\,;R\ ,\ y)\ \mathsf{fi}\ . \tag{71}$$

Now, although the first parameter is non-decreasing in each recursive call, still nontermination is guaranteed if there is no path from S to y. However, in that case by finiteness of A the recursive calls of sp eventually become stationary, i.e., eventually $S = S \cup S\,;R$ holds, which is equivalent to $S\,;R \subseteq S$. We consider that case in the following lemma:

Lemma 4. *If $y \notin S$ and $S\,;R \subseteq S$ then $S \bowtie R^{\Rightarrow} \bowtie y = \emptyset$, i.e., there is no path from set S to vertex y, and therefore $sp(S, y) = \emptyset$.*

Proof. We use the induction principle of Lemma 1 with the predicate

$$P[X] \stackrel{\text{def}}{\Leftrightarrow} S \bowtie X \bowtie y \subseteq \emptyset\ .$$

To show $P[A]$ we calculate

$$\begin{array}{ll} & S \bowtie A \bowtie y \\ = & \quad \{\![\text{ neutrality of } A \ ]\!\} \\ & S \bowtie y \\ = & \quad \{\![\text{ by (37), since } y \notin S \ ]\!\} \\ & \emptyset\ . \end{array}$$

Now assume $P[X]$. We calculate

$$\begin{array}{ll} & S \bowtie R \bowtie X \bowtie y \\ = & \quad \{\![\text{ by (42) }]\!\} \\ & S^{\Delta}\,;R \bowtie X \bowtie y \\ \subseteq & \quad \{\![\text{ by } S^{\Delta} \subseteq S \bullet S \text{ and monotonicity }]\!\} \\ & S \bullet S\,;R \bowtie X \bowtie y \\ \subseteq & \quad \{\![\text{ by } S\,;R \subseteq S \text{ and monotonicity }]\!\} \\ & S \bullet S \bowtie X \bowtie y \\ \subseteq & \quad \{\![\text{ by } P[X] \text{ and monotonicity }]\!\} \\ & S \bullet \emptyset \\ = & \quad \{\![\text{ strictness }]\!\} \\ & \emptyset\ . \end{array}$$

Now the claim is immediate from the definition of sp. □

Altogether we have:

$$\begin{aligned} &\mathit{shortestpath}(x,y) \;=\; \mathit{sp}(x,y) \;\;, \\ &\mathit{sp}(S,y) \;=\; \mathsf{if}\;\; y \in S\,\mathsf{then}\,0 \\ &\qquad\qquad\qquad\qquad \mathsf{else}\;\; \mathsf{if}\;\; S\,;R \;\subseteq\; S\,\mathsf{then}\,\emptyset \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathsf{else}\;\; 1 + \mathit{sp}(S \cup S\,;R\;,\;y)\;\;\mathsf{fi}\;\;\mathsf{fi}\;\;. \end{aligned} \tag{72}$$

Now termination is guaranteed, since S increases for each recursive call and is bounded by the finite set A of all vertices.

Improving Efficiency. One may argue that in the above version accumulating vertices in the parameter S is not efficient because it makes calculating $S\,;R$ more expensive. So, in an improved version of the algorithm, we shall keep as few vertices as possible in the parameter S and the set of vertices already visited in an additional parameter T, tied to S by an assertion. Let

$$\mathit{sp2}(S,T,y) \;\stackrel{\text{def}}{=}\; (S \cap T \;=\; \emptyset \;\wedge\; y \notin T) \bullet \mathit{sp}(S \cup T\;,\;y) \;\;, \tag{73}$$

with the embedding

$$\mathit{shortestpath}(x,y) \;=\; \mathit{sp2}(x,\emptyset,y) \;\;. \tag{74}$$

Now assume $S \cap T \;=\; \emptyset \;\wedge\; y \notin T$. Again we distinguish two cases:

Case 1: $y \in S$.

$$\begin{aligned} &\mathit{sp2}(S,T,y) \\ =\;\; &\{\![\text{ definition }]\!\} \\ &\mathit{sp}(S \cup T\;,\;y) \\ =\;\; &\{\![\text{ by } y \in S \subseteq S \cup T \text{ and (72) }]\!\} \\ &0\;\;. \end{aligned}$$

Case 2: $y \notin S$.

$$\begin{aligned} &\mathit{sp2}(S,T,y) \\ =\;\; &\{\![\text{ definition }]\!\} \\ &\mathit{sp}(S \cup T\;,\;y) \\ =\;\; &\{\![\text{ by } y \notin S \cup T \text{ and (72) }]\!\} \\ &\mathsf{if}\;\; (S \cup T)\,;R \;\subseteq\; S \cup T\,\mathsf{then}\,\emptyset \\ &\qquad\qquad\qquad\qquad \mathsf{else}\;\; 1 + \mathit{sp}(S \cup T \cup (S \cup T)\,;R\;,\;y)\;\;\mathsf{fi} \end{aligned}$$

$=$ $\{\![$ set theory $]\!\}$

$\quad$ if $(S \cup T)\,;R \subseteq S \cup T$ then $\emptyset$
$\qquad\qquad$ else $1 + sp(((S \cup T)\,;R)\backslash(S \cup T) \ \cup\ (S \cup T)\ ,\ y)$ fi

$=$ $\{\![$ definition and $y \notin S \cup T$ $]\!\}$

$\quad$ if $(S \cup T)\,;R \subseteq S \cup T$ then $\emptyset$
$\qquad\qquad$ else $1 + sp2(((S \cup T)\,;R)\backslash(S \cup T)\ ,\ S \cup T\ ,\ y)$ fi .

Altogether,

$$shortestpath(x,y) \ =\ sp2(x,\emptyset,y)\ ,$$

$$\begin{aligned} sp2(S,T,y) \ =\ & (S \cap T = \emptyset \wedge y \notin T) \bullet \\ & \text{if } y \in S \\ & \text{then } 0 \\ & \text{else if } (S \cup T)\,;R \subseteq S \cup T \\ & \qquad \text{then } \emptyset \\ & \qquad \text{else } 1 + sp2(((S \cup T)\,;R)\backslash(S \cup T)\ ,\ S \cup T\ ,\ y) \text{ fi fi } . \end{aligned}$$

This version still is very inefficient. However, a simple analysis shows that the assertion of *sp2* can be strengthened by the conjunct $T\,;R \subseteq S \cup T$. Thus, one can simplify the program to

$$shortestpath(x,y) \ =\ sp3(x,\emptyset,y)\ ,$$

$$\begin{aligned} sp3(S,T,y) \ =\ & (S \cap T = \emptyset \wedge y \notin T \wedge T\,;R \subseteq S \cup T) \bullet \\ & \text{if } y \in S \\ & \text{then } 0 \\ & \text{else if } S\,;R \subseteq S \cup T \\ & \qquad \text{then } \emptyset \\ & \qquad \text{else } 1 + sp3((S\,;R)\backslash(S \cup T)\ ,\ S \cup T\ ,\ y) \text{ fi fi } . \end{aligned}$$

The formal derivation steps for this are similar to the ones above and hence we omit them.

Termination is guaranteed, since T increases for each recursive call and is bounded by the finite set A of all vertices.

Note that a tail-recursive variant can easily be derived from *sp3* by introducing an accumulator. A corresponding algorithm in iterative form can be found in the literature, e.g. in Gondran, Minoux 1979 (but there unfortunately not faultless).

Further, our algorithm also solves the problem whether a vertex y is reachable from a vertex x, since

$$reachable(x,y) \ =\ (shortestpath(x,y) \neq \emptyset)\ . \tag{75}$$

3.2 Cycle Detection

Problem Statement and First Solution. Consider again a finite set A of vertices and a binary relation $R \subseteq A \bullet A$. The problem consists in determining whether R contains a **cyclic path**, i.e., a path in which a node occurs twice.

Lemma 5. *The following statements are equivalent:*
(1) R *contains a cyclic path.*
(2) $R^+ \cap A^\Delta \neq \emptyset$.
(3) $R^{|A|} \neq \emptyset$.
(4) $R^{|A|} ; A \neq \emptyset$.
(5) $A ; R^{|A|} \neq \emptyset$.

Proof. (1) $\Rightarrow$ (2) Let $p = u \bullet x \bullet v \bullet x \bullet w$ with $x \in A$ and $u, v, w \in A^{(*)}$ be a cyclic path. Then $x \bullet x \in R^+$ and the claim follows.

(2) $\Rightarrow$ (3) Assume $x \bullet x \in R^+$ and let n be the smallest number such that there are $x_0, \ldots, x_n \in A$ with $\bigcup_{i=0}^{n-1} x_i \bullet x_{i+1} \subseteq R$ and $x_0 = x = x_n$. Then $\bullet_{i=0}^{|A|} x_{i \bmod n}$ is a path as well and hence the claim holds.

(3) $\Rightarrow$ (4) Trivial, since $R^{|A|} ; A$ is the domain of $R^{|A|}$.

(4) $\Rightarrow$ (5) Trivial, since a relation with nonempty domain also has a nonempty codomain.

(5) $\Rightarrow$ (1) We have $y \in A ; R^{|A|}$ iff there is an $x \in A$ and a path from x to y with $|A| + 1$ nodes. By the pigeonhole principle this path must contain at least one node twice and hence is cyclic. □

By (5) we may specify our problem as

$$\mathit{hascycle} \stackrel{\text{def}}{=} (A ; R^{|A|} \neq \emptyset) \ .$$

To compute $A ; R^{|A|}$ we define $A_i \stackrel{\text{def}}{=} A ; R^i$ and use the properties of the powers of R:

$$\begin{aligned} A_0 &= A ; R^0 = A ; A^\Delta = A \ , \\ A_{i+1} &= A ; R^{i+1} = A ; (R^i ; R) = (A ; R^i) ; R = A_i ; R \ . \end{aligned}$$

The associated function

$$f : X \mapsto X ; R$$

is monotonic. We now prove a general theorem about monotonic functions on noetherian partial orders. A partial order $(M, \leq)$ is **noetherian** if each of its nonempty subsets has a minimal element w.r.t. $\leq$. An element $x \in S \subseteq M$ is **minimal** in S if $y \in S$ and $y \leq x$ imply $y = x$. Using reflexivity of $\leq$ we therefore have that x is minimal in S iff

$$\leq ; x \cap S = x \ . \tag{76}$$

Viewing a function $f : M \to M$ as a binary relation, we can form its closure f^*. Then, for $x \in M$, we have

$$x \,;\, f^* \;=\; \{f^i(x) : i \in \mathbb{N}\} \;\;, \tag{77}$$

where the f^i are defined as usual.

Theorem 1. *Let $(M, \leq)$ be a noetherian partial order and $f : M \to M$ a monotonic total function.*
(1) *If for $x \in M$ we have $f(x) \leq x$ then $x_\infty = \mathsf{glb}\,(x; f^*)$ exists and is a fixpoint of f.*
(2) *Assume x as in (1) and $y \in M$ with $x_\infty \leq y \leq x$. Then also $y_\infty = \mathsf{glb}\,(y; f^*)$ exists and $y_\infty = x_\infty$.*
(3) *If M has a greatest element $\top$ then $\top_\infty$ exists and is the greatest fixpoint of f.*

Proof. We first restate in relational notation some of the notions involved.

(a) f is a total function iff $A^\Delta \subseteq f \,;\, f^{-1}$ and $f^{-1} \,;\, f \subseteq A^\Delta$.
(b) f is monotonic iff $\leq \,; f \subseteq f; \leq$.
(c) $u \leq v$ is equivalent to both $u \subseteq \leq \,; v$ and $v \subseteq u; \leq$.
(d) By our convention about singleton sets $f(x)$ and $x \,;\, f$ are the same for a total function f.

In particular, (a) implies, for $S \subseteq M$,

$$(S \,;\, f)^\Delta \;=\; f^{-1} \,;\, S^\Delta \,;\, f \;\;. \tag{78}$$

We now treat the claims in order.

(1) We first show that

$$\forall\; y \in x \,;\, f^* : f(y) \leq y \;\;. \tag{79}$$

Relationally this means $(x \,;\, f^*)^\Delta \subseteq f; \leq$. We use the induction principle from Corollary 1 with the predicate

$$P[X] \stackrel{\text{def}}{\Leftrightarrow} X^\Delta \subseteq f; \leq$$

and $U = x, R = f$. $P[x]$ holds by assumption. To infer $P[X \,;\, f]$ from $P[X]$ we calculate

$$\begin{array}{ll} & (X \,;\, f)^\Delta \\ = & \quad \{\![\text{ by (78) }]\!\} \\ & f^{-1} \,;\, X^\Delta \,;\, f \\ \subseteq & \quad \{\![\text{ by } P[X] \text{ and monotonicity }]\!\} \\ & f^{-1} \,;\, f; \leq \,; f \\ \subseteq & \quad \{\![\; f \text{ a function, neutrality }]\!\} \end{array}$$

$$
\begin{array}{ll}
 & \leq\,;f \\
\subseteq & \quad \{\![\ f \text{ monotonic }]\!\} \\
 & f;\leq\ .
\end{array}
$$

Since $(M,\leq)$ is noetherian, $x\,;\,f^*$ has a minimal element x_∞. For this we calculate

$$
\begin{array}{ll}
 & x_\infty \\
= & \quad \{\![\ \text{by minimality (76)}\ ]\!\} \\
 & \leq\,;x_\infty \cap x\,;\,f^* \\
\supseteq & \quad \{\![\ \text{by (79) and monotonicity of } \cap\ ]\!\} \\
 & x_\infty\,;\,f \cap x\,;\,f^* \\
= & \quad \{\![\ \text{since } x_\infty\,;\,f \subseteq x\,;\,f^*\ ]\!\} \\
 & x_\infty\,;\,f\ .
\end{array}
$$

But by totality of f this means $x_\infty\,;\,f = x_\infty$ so that x_∞ is a fixpoint of f. We shall see below that $x_\infty = \mathsf{glb}\ (x\,;\,f^*)$.

(2) Using the induction principle from Lemma 2 it is immediate to show the following facts:

$$X\,;\,f \subseteq X \Rightarrow X\,;\,f^* \subseteq X\ , \tag{80}$$

$$\leq\,;f \subseteq f;\leq \Rightarrow \leq\,;f^* \subseteq f^*;\leq\ , \tag{81}$$

$$x\,;\,f \subseteq \leq\,;x \Rightarrow x\,;\,f^* \subseteq \leq\,;x\ . \tag{82}$$

From (80) and $X \subseteq X\,;\,f^*$ by $A^{\Delta} \subseteq f^*$ we infer

$$X\,;\,f \subseteq X \Rightarrow X\,;\,f^* = X\ . \tag{83}$$

Now consider $u,v \in M$ with $u \leq v$. Then

$$
\begin{array}{ll}
 & u \leq v \\
\Leftrightarrow & \quad \{\![\ \text{image}\ ]\!\} \\
 & v \subseteq u;\leq \\
\Rightarrow & \quad \{\![\ \text{monotonicity}\ ]\!\} \\
 & v\,;\,f^* \subseteq u;\leq\,;f^* \\
\Rightarrow & \quad \{\![\ f \text{ monotonic and (81)}\ ]\!\} \\
 & v\,;\,f^* \subseteq u\,;\,f^*;\leq\ ,
\end{array}
$$

so that $u\,;\,f^*$ is a minorant for $v\,;\,f^*$. In particular, taking $u = x_\infty$ and $v = x$ or $v = y$ and using (83) and (82) we see that x_∞ is a lower bound for both $y\,;f^*$ and $x\,;f^*$. This also implies $x_\infty = \mathsf{glb}\ (x\,;f^*)$. Moreover, $y\,;f^*$ is a minorant of $x\,;f^*$ so that every lower bound z for $y\,;f^*$ also is a lower bound for $x;f^*$ and hence satisfies $z \leq x_\infty$. But this shows $x_\infty = \mathsf{glb}\ (y;f^*) = y_\infty$.

(3) Trivially, $f(\top) \leq \top$, and hence $\top_\infty$ exists by (1). Let x be a fixpoint of f. By the proof of (2) we know that $\top\,;f^* \subseteq x\,;f^*; \leq\, = x; \leq$ so that x is a lower bound for $\top\,;f^*$. This implies $x \leq \mathsf{glb}\ (\top\,;f^*) = \top_\infty$.

□

A similar theorem has been stated by Cai, Paige 1989.

Corollary 2. *If $\top_\infty \leq x$ for some $x \in M$ then $\top_\infty = x_\infty$.*

Proof. By (2) of the above theorem. □

To actually calculate x_∞ we define a function *inf* by

$$inf(y) \stackrel{\text{def}}{=} (x_\infty \leq y \leq x) \bullet x_\infty$$

which determines x_∞ using an upper bound y. We have the embedding $x_\infty = inf(x)$. Now from the proof of the above theorem the following recursion is immediate:

$$inf(y) \;=\; (x_\infty \leq y \leq x) \;\bullet\; \mathsf{if}\ y = f(y)\ \mathsf{then}\ y\ \mathsf{else}\ inf(f(y))\ \mathsf{fi}\ .$$

This recursion terminates for every y satisfying $f(y) \leq y$, since monotonicity then also shows $f(f(y)) \leq f(y)$, so that in each recursive call the parameter decreases properly. In particular, the call $inf(x)$ terminates. This algorithm is an abstraction of many iteration methods on finite sets.

We now return to the special case of cycle detection. By finiteness of A the partial order $(\mathcal{P}(A), \subseteq)$ is noetherian with greatest element A. Therefore A_∞ exists. Moreover, we have

Corollary 3. $A_{|A|} = A_\infty$.

Proof. The length of any properly descending chain in $\mathcal{P}(A)$ is at most $k+1$. Hence we have $A_{k+1} = A_k$ and thus $A_k = A_\infty$. □

So we have reduced our task to checking whether $A_\infty \neq \emptyset$, i.e., whether $inf(A) \neq \emptyset$. For our special case the recursion for *inf* reads (omitting the trivial part $W \subseteq A$)

$$inf(W) \;=\; (A_\infty \subseteq W) \;\bullet\; \mathsf{if}\ W = W\,;R\ \mathsf{then}\ W\ \mathsf{else}\ inf(W\,;R)\ \mathsf{fi}\ .$$

We want to improve this by avoiding the computation of $W\,;R$. By the above considerations we may strengthen the assertion of *inf* by adding the conjunct $W\,;R \subseteq W$. We define

$$src(W) \stackrel{\text{def}}{=} W \backslash (W\,;R)\ .$$

This is the set of **sources** of W, i.e., the set of nodes in W which do not have a predecessor in W.

Now, assuming $W\,;R \subseteq W$, we have $W = W\,;R \Leftrightarrow src(W) = \emptyset$ and $W\,;R = W\backslash src(W)$ so that we can rewrite inf into

$$\begin{aligned} inf(W) = (A_\infty \subseteq W \wedge W\,;R \subseteq W) \bullet \\ \mathsf{if}\ src(W) = \emptyset\ \mathsf{then}\ W\ \mathsf{else}\ inf(W\backslash src(W))\ \mathsf{fi}\ . \end{aligned}$$

This is an improvement in that $src(W)$ usually will be small compared to W; moreover, the computation of $src(W)$ can be facilitated by a suitable representation of R.

Plugging this into our original problem of cycle recognition we obtain

$$hascycle = hcy(A)\ , \tag{84}$$

where

$$\begin{aligned} hcy(W) = (A_\infty \subseteq W \wedge W\,;R \subseteq W) \bullet \\ \mathsf{if}\ src(W) = \emptyset\ \mathsf{then}\ W \neq \emptyset\ \mathsf{else}\ hcy(W\backslash src(W))\ \mathsf{fi}\ , \end{aligned} \tag{85}$$

which is one of the classical algorithms which works by successive removal of sources (see e.g. Berghammer 1986). Note that Lemma 5(4) suggests a dual specification to the one we have used; replaying our development for it would lead to an algorithm that works by successive removal of sinks.

Improving Efficiency. We want to improve the computation of the sets $src(W)$. We observe that

$$\begin{aligned} & x \in src(W) \\ = \ & x \in W\backslash(W\,;R) \\ = \ & x \in W \wedge x \notin W\,;R \\ = \ & x \in W \wedge R\,;x \cap W = \emptyset \\ = \ & x \in W \wedge |R\,;x \cap W| = 0\ . \end{aligned}$$

So we define for $W \subseteq A$ the relation $in(W)$ by

$$x\,;in(W) \stackrel{\text{def}}{=} |R\,;x \cap W|\ . \tag{86}$$

Hence $x\,;in(W)$ gives the indegree of x w.r.t. W and

$$src(W) = W \cap in(W);0\ . \tag{87}$$

In a final implementation, $in(W)$ will, of course, be realized by an array. We aim at an incremental updating of in in the course of our algorithm. We calculate

$$\begin{aligned} & x\,;in(W\backslash src(W)) \\ = \ & \quad \{\![\ \text{definition}\ ]\!\} \\ & |R\,;x \cap (W\backslash src(W))| \\ = \ & \quad \{\![\ \text{set theory}\ ]\!\} \end{aligned}$$

$$
\begin{array}{ll}
 & |(R\,;x\cap W)\backslash src(W)| \\
= & \quad \{\![\ |A\backslash B| = |A| - |A\cap B|\ ]\!\} \\
 & |(R\,;x\cap W)| - |R\,;x\cap W\cap src(W)| \\
= & \quad \{\![\ src(W)\subseteq W\ ]\!\} \\
 & |(R\,;x\cap W)| - |R\,;x\cap src(W)| \\
= & \quad \{\![\ \text{definition}\ ]\!\} \\
 & x\,;in(W) - x\,;in(src(W))\ .
\end{array}
$$

For binary relations f, g with the same domain and subsets of $\mathbb{N}$ as codomains and arithmetic operator $\wr$ we define $f\wr g$ by

$$x\,;(f\wr g) \stackrel{\text{def}}{=} (x\,;f)\wr(x\,;g)\ . \tag{88}$$

Then

$$in(W\backslash src(W)) = in(W) - in(src(W))\ . \tag{89}$$

For the computation of in we observe that

$$in(\emptyset) = \mathbf{0}\ , \tag{90}$$

where

$$x\,;\mathbf{0} \stackrel{\text{def}}{=} 0\ . \tag{91}$$

If $S\neq\emptyset$ and $q\in S$ is arbitrary we have

$$
\begin{array}{ll}
 & x\,;in(S) \\
= & x\,;in(q\cup S\backslash q) \\
= & |R\,;x\cap(q\cup S\backslash q)| \\
= & |(R\,;x\cap q)\cup(R\,;x\cap S\backslash q)| \\
= & |R\,;x\cap q| + |R\,;x\cap S\backslash q| \\
= & x\,;in(q) + x\,;in(S\backslash q)\ ,
\end{array}
$$

where

$$x\,;in(q)\ =\ \mathsf{if}\ q\,;R\,;x\,\mathsf{then}\,1\,\mathsf{else}\,0\ \mathsf{fi}\ . \tag{92}$$

Then

$$in(S) = in(q) + in(S\backslash q)\ . \tag{93}$$

We forego a transformation of in into tail recursive form, since this is completely standard using associativity of $+$.

Now we can administer the source sets more efficiently: We introduce additional parameters for carrying along $src(W)$ and $in(W)$ and adjust these parameters by the technique of finite differencing (see e.g. Partsch 1990). We set, for $S\subseteq W\subseteq A$ and relation f,

$$hc(W,S,f) \stackrel{\text{def}}{=} (S = src(W)\ \wedge\ f = in(W))\bullet hcy(W)\ , \tag{94}$$

with the embedding

$$hcy(W) \;=\; hc(W, src(W), in(W)) \;\; . \tag{95}$$

Now

$$\begin{array}{ll}
 & hc(W,S,f) \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & \mathsf{if}\ src(W) = \emptyset\ \mathsf{then}\ W \neq \emptyset\ \mathsf{else}\ hcy(W \backslash src(W)) \\
= & \quad \{\![\text{ assertion }]\!\} \\
 & \mathsf{if}\ S = \emptyset\ \mathsf{then}\ W \neq \emptyset\ \mathsf{else}\ hcy(W \backslash S) \\
= & \quad \{\![\text{ embedding }]\!\} \\
 & \mathsf{if}\ S = \emptyset\ \mathsf{then}\ W \neq \emptyset\ \mathsf{else}\ hc(W \backslash S\ ,\ src(W \backslash S)\ ,\ in(W \backslash S)) \\
= & \quad \{\![\text{ introducing auxiliaries }]\!\} \\
 & \mathsf{if}\ S = \emptyset\ \mathsf{then}\ W \neq \emptyset \\
 & \qquad \mathsf{else}\ \mathsf{let}\ T \stackrel{\text{def}}{=} W \backslash S \\
 & \qquad\quad \mathsf{let}\ g \stackrel{\text{def}}{=} in(T) \\
 & \qquad\quad \mathsf{in}\ \ hc(T, src(T), g)\ \ \mathsf{fi} \\
= & \quad \{\![\text{ by (89) and (87) }]\!\} \\
 & \mathsf{if}\ S = \emptyset\ \mathsf{then}\ W \neq \emptyset \\
 & \qquad \mathsf{else}\ \mathsf{let}\ T \stackrel{\text{def}}{=} W \backslash S \\
 & \qquad\quad \mathsf{let}\ g \stackrel{\text{def}}{=} f - in(S) \\
 & \qquad\quad \mathsf{in}\ \ hc(T,\ T \cap g\,;0,\ g)\ \ \mathsf{fi}\ \ .
\end{array}$$

A final improvement would consist in merging the computation of g with that of $T \cap g\,;0$ using the tupling strategy (see e.g. Partsch 1990).

4 Conclusion

The calculus of formal languages and relations has proved to speed up derivations, in particular the way from "non-operational" specifications involving the closures R^* and $R^{\Rightarrow}$ to first recursive solutions. But also the tuning steps in improving the recursions have benefitted from the quantifier-free notation. If the resulting derivations still appear lengthy, this is to a great deal due to the fact that the assertions have been constructed in a stepwise fashion (for mastering complexity) rather than in one blow. Further case studies which demonstrate the viability of the approach in more complicated examples are under way. Moreover, the framework has been applied to other problem areas as well (see Möller 1993a, 1993c).

Currently we are working on the definition of a more general program development language based on this approach. While other authors use a purely

relational approach employing mostly even only binary relations, we find that relations with their fixed arity are too unflexible and lead to a lot of unnecessary encoding and decoding.

Acknowledgement

We are grateful to H. Partsch and to anonymous referees for a number of valuable remarks.

References

F.L. Bauer, R. Berghammer, M. Broy, W. Dosch, F. Geiselbrechtinger, R. Gnatz, E. Hangel, W. Hesse, B. Krieg-Brückner, A. Laut, T.A. Matzner, B. Möller, F. Nickl, H. Partsch, P. Pepper, K. Samelson, M. Wirsing, H. Wössner: The Munich project CIP. Volume I: The wide spectrum language CIP-L. Lecture Notes in Computer Science **183**. Berlin: Springer 1985

F.L. Bauer, B. Möller, H. Partsch, P. Pepper: Formal program construction by transformations — Computer-aided, Intuition-guided Programming. IEEE Transactions on Software Engineering **15**, 165–180 (1989)

R. Berghammer: A transformational development of several algorithms for testing the existence of cycles in a directed graph. Institut für Informatik der TU München, TUM-I8615

R. Bird: Lectures on constructive functional programming. In M. Broy (ed.): Constructive methods in computing science. NATO ASI Series. Series F: Computer and systems sciences **55**. Berlin: Springer 1989, 151–216

R.M. Burstall, J. Darlington: A transformation system for developing recursive programs. J. ACM **24**, 44–67 (1977)

J. Cai, R. Paige: Program derivation by fixed point computation. Science of Computer Programming **11**, 197–261 (1989)

J.H. Conway: Regular algebra and finite machines. London: Chapman and Hall 1971

C.J. Date: An introduction to database systems. Vol. I, 4th edition. Reading, Mass.: Addison-Wesley 1988

M. Gondran, M. Minoux: Graphes et algorithmes. Paris: Eyrolles 1979

S.C. Kleene: Introduction to metamathematics. New York: van Nostrand 1952

P. Lescanne: Modèles non déterministes de types abstraits. R.A.I.R.O. Informatique théorique **16**, 225–244 (1982)

L.G.L.T. Meertens: Algorithmics — Towards programming as a mathematical activity. In J. W. de Bakker et al. (eds.): Proc CWI Symposium on Mathematics and Computer Science. CWI Monographs Vol **1**. Amsterdam: North-Holland 1986, 289–334

B. Möller: Applicative assertions. In: J.L.A. van de Snepscheut (ed.): Mathematics of Program Construction. Lecture Notes in Computer Science **375**. Berlin: Springer 1989, 348–362

B. Möller: Relations as a program development language. In B. Möller (ed.): Constructing programs from specifications. Proc. IFIP TC2/WG 2.1 Working Conference on Constructing Programs from Specifications, Pacific Grove, CA, USA, 13–16 May 1991. Amsterdam: North-Holland 1991, 373–397

B. Möller: Towards pointer algebra. Institut für Mathematik der Universität Augsburg, Report No. 279, 1993. Also to appear in Science of Computer Programming

B. Möller: Algebraic calculation of graph and sorting algorithms. In: V.K. Sabelfeld (ed.): Proc. International Conference on Formal Methods in Programming and their Applications, Novosibirsk, June 29 – July 2, 1993. Lecture Notes in Computer Science. Berlin: Springer (to appear)

B. Möller: Derivation of graph and pointer algorithms. Institut für Mathematik der Universität Augsburg, Report No. 280, 1993. Also to appear in B. Möller, H.A. Partsch, S.A. Schuman (eds.): Formal program development. Proc. of an IFIP TC2/WG 2.1 State of the Art Seminar. Lecture Notes in Computer Science. Berlin: Springer (to appear)

H.A. Partsch: Specification and transformation of programs — A formal approach to software development. Berlin: Springer 1990

M. Russling: Hamiltonian sorting. Institut für Mathematik der Universität Augsburg, Report Nr. 270, 1992

G. Schmidt, T. Ströhlein: Relationen und Graphen. Berlin: Springer 1989. English version: Relations and graphs (forthcoming)

A. Tarski: On the calculus of relations. J. Symbolic Logic **6**, 73–89 (1941)