Dines Bjørner Manfred Broy
Igor V. Pottosin (Eds.)

Formal Methods in Programming and Their Applications

International Conference
Academgorodok, Novosibirsk, Russia
June 28 - July 2, 1993
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Dines Bjørner
United Nations University, International Institute for Software Technology
P. O. Box 3058, Macau

Manfred Broy
Institut für Informatik, Technische Universität München
Postfach 20 24 20, D-80290 München, Germany

Igor V. Pottosin
Institute of Informatics Systems
Av. Acad. Lavrentyev 6, Novosibirsk 630090, Russia

CR Subject Classification (1991): F.3-4, D.2-3, I.1-2

ISBN 3-540-57316-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57316-X Springer-Verlag New York Berlin Heidelberg

Printed in Germany

Typesetting: Camera-ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

The volume comprises the papers selected for presentation at the international conference "Formal Methods in Programming and Their Applications", held in Academgorodok (Novosibirsk, Russia), June 28 - July 2, 1993.

The conference was organized by the Institute of Informatics Systems of the Siberian Division of the Russian Academy of Sciences. The Institute is engaged in active research in the field of theoretical programming. The Institute has been an organizer of several international conferences related to programming and formal methods in programming but the latter have been considered together with other problems of programming. The current conference is the first forum organized by the Institute which is entirely dedicated to formal methods.

The main scientific tracks of the conference have been centered around the formal methods of program development and program construction. They include:

— specification, synthesis, transformation and verification of programs;

— parallel and distributed computations;

— semantics and logic of programs;

— theory of compilation and optimization;

— mixed computation, partial evaluation and abstract interpretation.

One of the main goals of the conference has been to promote formal methods in programming and to present and discuss the most interesting approaches to practical programming. A number of papers delivered at the conference are aimed at such a goal.

Scientists from eleven countries have been participants to the conference (Austria, Brazil, Canada, Denmark, England, France, Germany, the Netherlands, Russia, Turkey, and the USA as well as from the Territory of Macau)!

Also in the opinion of the participants the conference has been a success and similar conferences should be held in the future, perhaps, with a greater focus on the application of formal methods and the problems connected with it.

The organizers of the conference express their deep gratitude to the colleagues of Russian and international communities who supported actively the conference by rendering assistance and advice, review and participation.

We would also like to thank the Springer-Verlag for excellent co-operation.

July 1993 Dines Bjørner, Manfred Broy, Igor Pottosin

FMP&TA Organization

Programme Committee Co-Chairs:

Dines Bjørner United Nations University
Intl.Inst.f.Softw.Techn., Macau
Manfred Broy Technische Universität München
Institut für Informatik, Munich, Germany
Igor Pottosin Institute of Informatics Systems
Novosibirsk, Russia

Programme Committee:

Jan Barzdin, Riga
Mikhail Bulyonkov, Novosibirsk
Patrick Cousot, Paris
Pierre Deransart, Rocquencourt
Yuri Ershov, Novosibirsk
Yuri Gurevich, Ann Arbor
Victor Ivannikov, Moscow
Cliff Jones, Manchester
Philippe Jorrand, Grenoble
Vadim Kotov, Palo Alto
Reino Kurki-Suonio, Tampere
Alexander Letichevski, Kiev
Gregory Mints, Stanford
Valery Nepomniaschy, Novosibirsk
Anil Nerode, Ithaca
Amir Pnueli, Rehovot
Mikhail Taitslin, Tver
Boris Trachtenbrot, Tel-Aviv
Enn Tyugu, Stockholm

Invited Speakers

ChaoChen Zhou, Macau
Patrick Cousot, Paris
Yuri Ershov, Novosibirsk
Philippe Jorrand, Grenoble
Bernhard Möller, Augsburg
Peter Pepper, Berlin
Mikhail Taitslin, Tver
Martin Wirsing, Munich

Organizing Committee:

Valery Nepomniaschy, chairman
Victor Sabelfeld, publication of proceedings
Mikhail Bulyonkov, general organization
Alexander Bystrov, treasury
Tatiana Churina, scientific secretary

List of Referees

K.Andrew
J.Barzdin
Yu.Gurevich
P.Deransart
Yu.Ershov
N.Jones
C.Jones
P.Jorrand
R.Kurki-Suonio
A.Letichevsky
G.Mints
B.Möller
T.Mogensen
V.Nepomniaschy
V.Sazonov
V.Sabelfeld
N.Shilov
M.Taitslin
E.Tyugu
M.Valiev
I.Virbitskaite
C.Zhou

TABLE OF CONTENTS

Theory of Domains and Nearby *

Yu. L. Ershov

Novosibirsk State University, RIMIBE
Universitetsky pr. 4
Novosibirsk 630090
Russia

Abstract. The author presents a topological approach to the development of the theory of domains.

0. In the present paper we deal with historical, methodological, and mathematical aspects of the theory of domains. A recent book [1] by A. Jung demonstrates a noticeable progress in the theory.

Theory of domains arose in the late 60s in research that was carried out independently by Prof. D. Scott in Oxford and by the author in Novosibirsk. D. Scott was interested in a natural mathematical model for the type-free λ-calculus, whereas the author developed a theory of partial computable functionals of finite types. Both problems were solved quite satisfactorily. The corresponding results were reported by the author at the International Congress of Mathematicians in Nice, 1970 [2] and by D. Scott at the International Congress for Logic, Methodology, and Philosophy of Science in Bucharest, 1971 [3].

It turned out that there was a great resemblance between the mathematical models developed. The exact relation between these models was established in [4]. In particular, the notion of Scott's domain (S-domain) and the one of complete f_0-space were proved to be equivalent.

N. Bourbaki in *"L'Architecture des mathématiques"* distinguishes three basic mathematical structures: algebraic, topological, and that of partial order. All these structures are found in the theory of domains. The approach of D. Scott to the introduction of S-domain by means of (directed-complete) partial orders dominates in the current literature on computer science, though many basic concepts of the theory, e.g., the way-below relation, are rather difficult to comprehend. This was the reason why D. Scott repeatedly returned to the theory of domains, attempting to clarify the foundations. Thus, for this purpose he introduced information systems [5].

In the author opinion, topology should be the basic structure in the development of the theory. The author supposes that the topological approach of [4] is more preferable than the one based on a partial order, both for better reception and for potentially greater generality that is needed if one wants to study domains which contain only constructive points. In the present paper the author will try to substantiate this point of view following the ideas expressed in [4].

---

* Research supported in part by the Russian Foundation for Fundamental Research (93 011 16014).

1. Let $\langle X, T\rangle$ be a topological space (T is a topology on X, i.e., a family of all open sets). We define a preorder $\leqslant_T$ on X, related to the topology T, as follows: for $x, y \in X$

$$x \leqslant_T y \Leftrightarrow \text{for every open set } V \subseteq X (V \in T)(x \in V \rightarrow y \in V)\,.$$

This relation is a partial order provided that $\langle X, T\rangle$ is a T_0-space, i.e., the weakest separation axiom holds: *for every* $x, y \in X$, *if* $x \neq y$, *then there exists an open set* $V \subseteq X$ *such that* $x \in V$ *and* $y \notin V$, *or* $x \notin V$ *and* $y \in V$.

The subscript T in the notation $\leqslant_T$ will usually be omitted. We introduce the following notation: $\hat{x} = \{y \mid y \in X,\, y \leqslant x\}$, $\check{x} = \{y \mid y \in X,\, x \leqslant y\}$.

If $\langle X, T\rangle$ is a T_1-space (i.e., $\forall x, y \in X\ (x \neq y \rightarrow \exists V \in T(x \in V \wedge y \notin V))$), then the preorder $\leqslant$ degenerates to the identity relation. In the sequel, we will consider only T_0-spaces.

We introduce one more relation, namely the *approximation relation* $\prec$ on elements of X as follows: for $x, y \in X$

$$x \prec y \Leftrightarrow \text{there exists an open set } V \subseteq X \text{ such that } (y \in V \text{ and } \forall z \in V(x \leqslant z))\,.$$

Remark. An equivalent definition may be given as follows: $x \prec y \Leftrightarrow y \in \operatorname{Int} \check{x}$, where $\operatorname{Int} Y$ is the interior of Y, i.e., the largest open subset of the set $Y \subseteq X$. Note that $x \prec y$ implies $x \leqslant y$.

We will use the following notation: $\overset{\curlywedge}{x} = \{y \mid y \in X,\, y \prec x\}$, $\overset{\curlyvee}{x} = \{y \mid y \in X,\, x \prec y\}$.

We call a topological space $\langle X, T\rangle$ *approximative* (or an *α-space*) if the following condition holds: for any open set $V \subseteq X$ and any element $x \in V$ there exists $y \in V$ such that $y \prec x$.

It is easy to see that the following holds:

1. If $\langle X, T\rangle$ is an α-space and a set $V \subseteq X$ is open, then
$$V = \bigcup_{x \in V} \overset{\curlyvee}{x}.$$
2. If $\langle X, T\rangle$ is an α-space and $x \in X$, then for every y, z such that $y \prec x$ and $z \prec x$ there exists $u \prec x$ such that $y \prec u$, $z \prec u$.
3. $x = \sup \overset{\curlywedge}{x}$, i.e., x is the least upper bound (relative to the order $\leqslant$) of the set $\overset{\curlywedge}{x}$.

Let $\langle X, T\rangle$ be an α-space. A set $X_0 \subseteq X$ is called a *base subset of* X if the following condition holds: for any open set $V \subseteq X$ and any $x \in V$ there exists $y \in V \cap X_0$ such that $y \prec x$.

Remark. X is a base subset of X.

Remark. If X_0 is a base subset of X, then $V = \bigcup_{x \in V \cap X_0} \overset{\curlyvee}{x}$ for every open set $V \subseteq X$.

Remark. If X_0 is a base subset of X, then for any $x \in X$ the set $\overset{\blacktriangle}{x} \cap X_0$ is directed and $x = \sup(\overset{\blacktriangle}{x} \cap X_0)$.

Now we proceed to the closure properties of α-spaces. (In the sequel, we will usually omit an explicit indication of the topology.)

Proposition 1. *If X and Y are α-spaces, then the Cartesian product $X \times Y$ is an α-space.*

Remark. The topology of the product $X \times Y$ is defined in a standard way.

Proposition 1 can be extended to products of arbitrary number of spaces, if we impose an additional quite natural restriction. An α-space X is called an α_0*-space* if the partially ordered set $\langle X, \leqslant_T \rangle$ has a least element.

Proposition 1′. *Let X_i, $i \in I$, be a family of α_0-spaces and $X = \prod_{i \in I} X_i$ be the Cartesian product of the family (equipped with the Tychonoff topology). Then X is an α_0-space.*

Many important constructions in the theory use the notions of retract and project. Remind that a continuous mapping $\rho : X \to X$ of a topological space X into itself is called a *retraction* if $\rho^2 = \rho$. The image $\rho(X)$ considered as a subspace of X is called a *retract of* X. A retraction $\rho : X \to X$ is called a *projection* if $\rho(x) \leqslant x$ for all $x \in X$. In this case $\rho(X)$ is called a *project of* X.

Proposition 2. *If X is an $\alpha(\alpha_0)$-space and $Y \subseteq X$ is a retract of X, then Y is an $\alpha(\alpha_0)$-space.*

Now we introduce an important notion of a complete α-space.

An α-space X is called *complete* if, given an α-space Y, its base subset Y_0, and a homeomorphism h of Y_0 into X such that $h(Y_0)$ is a base subset of X, there exists an extension of h to a continuous mapping of Y into X. (This extension will in fact be a homeomorphic embedding of Y into X.)

Proposition 3. *For every α-space Y there exists a complete α-space X and a homeomorphic embedding $\pi : Y \to X$ such that $\pi(Y)$ is a base subset of X.*

The α-space X in Proposition 3 is called *the completion of* Y. It is unique in a reasonable sense.

Now we establish a crucial connection between α-spaces and directed-complete partial orders.

Theorem 4. *If $\langle X, T \rangle$ is a complete α-space, then $\langle X, \leqslant_T \rangle$ is a continuous directed-complete partial order. If $\langle X, \leqslant \rangle$ is a continuous directed-complete partial order, then X, equipped with the Scott-topology, is a complete α-space and the approximation relation $\prec$ coincides with the way-below relation $\ll$.*

2. An important subclass of the class of approximative spaces is the class of finitary spaces. An element x in T_0-space X is called *finitary* if the relation $x \prec x$ holds or, equivalently, if the set $\check{x}$ is open. The set of all finitary elements of a space X will be denoted by $F(X)$. An approximative space X is called a *finitary space* (or a φ*-space*) if $F(X)$ is a base subset of X.

Remark. For an arbitrary base subset X_0 of X we have $F(X) \subseteq X_0$. If X_0 is a base subset of X and $x \in X_0 \backslash F(X)$, then $X_0 \backslash \{x\}$ is a base subset of X. Thus, an α-space X is finitary if and only if it has the least (under set inclusion) base subset.

Theorem 5. *If $\langle X,T \rangle$ is a complete φ-space, then $\langle X, \leqslant_T \rangle$ is an algebraic directed-complete partial order. If $\langle X, \leqslant \rangle$ is an algebraic directed-complete partial order, then X, equipped with the Scott-topology, is a complete φ-space.*

A φ-space X is called an *f-space* if $\langle F(X), \leqslant \rangle$ is a partial upper semilattice, i.e., a partial order such that, for any $x, y \in F(X)$, a consistency of x and y (i.e., $\exists z \in F(X)(x \leqslant z \wedge y \leqslant z)$) implies the existence of the least upper bound $x \sqcup y$ in $F(X)$. An f-space with a least element is called an f_0*-space* (cf. [4]).

Theorem 6. *If $\langle X,T \rangle$ is a complete f_0-space, then $\langle X, \leqslant_T \rangle$ is an S-domain. If $\langle X, \leqslant \rangle$ is an S-domain, then X, equipped with the Scott-topology, is a complete f_0-space.*

A φ-space X is called a *b-space* if $\langle F(X), \leqslant \rangle$ satisfies the condition: every finite subset $F \subseteq F(X)$ is contained in a finite subset $F_0 \subseteq F(X)$ such that

$$\forall F_1 \subseteq F_0 \ \forall x \in F(X) \ (\forall x_0 \in F_1 (x_0 \leqslant x) \rightarrow$$

$$\rightarrow \exists x_1 \in F_0 \ (\forall x_0 \in F_1 (x_0 \leqslant x_1) \wedge x_1 \leqslant x)).$$

Finite sets F_0 satisfying this condition are called *perfect*. A b-space with the least element is called a b_0*-space*.

Theorem 7. *If $\langle X,T \rangle$ is a complete b_0-space, then $\langle X, \leqslant_T \rangle$ is a B-domain. If $\langle X, \leqslant \rangle$ is a B-domain, then X, equipped with the Scott-topology, is a complete b_0-space.*

Remark. Every $f(f_0)$-space is a $b(b_0)$-space.

Proposition 8. *If X is a b-space and Y is a b_0-space, then the set $C(X,Y)$ of all continuous mappings of X into Y, equipped with the topology of pointwise convergence, is a b_0-space. Moreover, if Y is complete, then $C(X,Y)$ is complete.*

We point out the basic elements of the proof.

1. If F_0 is a finite perfect subset of $F(X)$ and $f_0 : F_0 \rightarrow F(Y)$ is monotone, then we can extend f_0 to a continuous mapping $f_0^* : X \rightarrow Y$ as follows. Notice that if $x \in X$, then $\hat{x} \cap F_0$ is empty or contains the greatest element e_x. In the first case we put $f_0^*(x)$ equals $\bot_Y$, the least element of Y; in the second we put $f_0^*(x) = f_0(e_x)$.

2. The finite elements of $C(X,Y)$ are exactly the functions of the form f_0^*.
3. Assume that $f_0^*, \ldots, f_n^*$ are obtained from the monotone mappings $f_0 : F_0 \to F(Y), \ldots, f_n : F_n \to F(Y)$. We put:
   $F_{n+1} \subseteq F(X)$ is a finite perfect subset of $F(X)$, containing $F_0 \cup F_1 \cup \ldots \cup F_n$;
   F_{n+2} is a finite perfect subset of $F(Y)$, containing $\{\perp_Y\} \cup f_0(F_0) \cup \ldots \cup f_n(F_n)$;
   $G = \{f \mid f$ is a monotone mapping of F_{n+1} into $F_{n+2}\}$;
   $G^* = \{f^* \mid f \in G\}$.

Then G^* is a finite perfect subset of $F(C(X,Y))$ and $\{f_0^*, \ldots, f_n^*\} \subseteq G^*$.

Proposition 9. *The category of b_0-spaces is Cartesian closed.*

Remark. A corresponding statement for f_0-spaces was proved in [6].

Remark. The category of b_0-spaces is closed under limits of bispectra, i.e., an analog of Theorem 1 [4, §5] holds.

Since retracts of a Cartesian closed category of topological spaces constitute a Cartesian closed category in themselves, it is useful to obtain a description for retracts of f_0-spaces. It turns out that the following generalization of Theorem 4.1 [1] holds. (We recall that, according to [1], a *deflation* of a topological space X is a continuous mapping $f : X \to X$ of X into itself such that $f(X)$ is finite and $f(x) \leqslant_T x$ for all $x \in X$.)

Proposition 10. *If an α_0-space X is a retract of a b_0-space, then there exists a directed family $f_i, i \in I$, of deflations of X such that* $\sup f_i = \mathrm{id}_X$. *If an α_0-space X possesses such a family of deflations, then X is a project of a b_0-space.*

The second part of the proposition is stronger than the corresponding assertion of Theorem 4.2 [1] even for complete b_0-spaces (= B-domains) and answers the question raised in [1, p. 92].

Remark. An explicit description of retracts (or projects) of complete f_0-spaces as complete A_0-spaces is given in [4].

3. As in [7], we give an effective version of b_0-spaces. Let X be a b_0-space. An enumeration $\nu : \omega \to F(X)$ is called a *constructivization of the base subset of* X if the following conditions hold:

1) the set $\{\langle n, m\rangle \mid n, m \in \omega, \nu n \leqslant \nu m\}$ is recursive;
2) there exists a recursive function $g : \omega \to \omega$ such that for every $n \in \omega$

$$\nu D_n (= \{\nu m \mid m \in D_n\}) \subseteq \nu D_{g(n)} (= \{\nu m \mid m \in D_{g(n)}\})$$

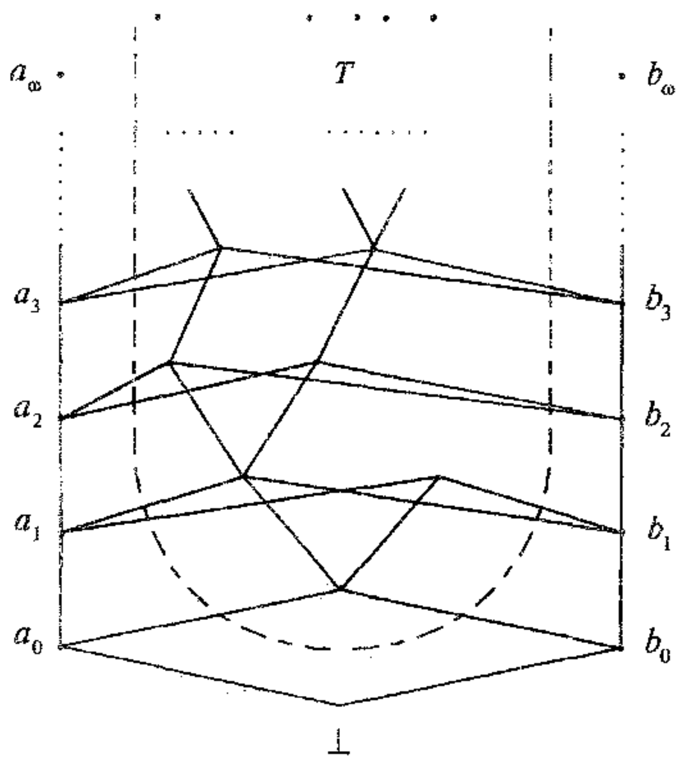
and $\nu D_{g(n)}$ is a perfect subset of $F(X)$. (Here D_n is a finite subset of ω with a canonical index n, cf. [6].)

A b_0-space X *has a constructivizible base* if there exists a constructivization of the base subset $F(X)$ of X.

Proposition 11. *The category of b_0-spaces with constructivizible base subsets is Cartesian closed.*

Let $\nu : \omega \to F(X)$ be a constructivization of the base subset of a b_0-space X. An element $x \in X$ is called *constructive*, if the set $\{n | \nu(n) \leqslant x\}$ is recursively enumerable.

A good theory of f_0-spaces which have constructivizible bases and such that all their elements are constructive is developed in [6]. In particular, the notions of computable enumeration of these spaces, completeness, and principal computable enumerations are defined there. This theory serves as a tool for the construction of partial computable functionals of finite types acting on partial continuous functionals (the model $\mathbb{C}$, [4, 7]). But the theory of b_0-spaces in which all points are constructive is not quite satisfactory as the following example shows.



Here T is an infinite recursive binary tree without infinite recursive branches. Notice that every infinite recursively enumerable branch of a recursive tree is recursive. Hence, there is no infinite recursively enumerable branch in T. The existence of such trees is well known (cf. [8]).

Elements of T at a level n are (minimal) upper bounds of the pair a_n, b_n. We add limit points: a_ω for $a_0, a_1, \ldots$; b_ω for $b_0, b_1, \ldots$; and limit points corresponding to every infinite branch of the tree T. A topology on the obtained set X_T is defined by a subbasis constituted by open sets of the form $\check{c}$ where $c \in F(X_T) = T \bigcup \{a_0, b_0, \ldots\}$. Then X_T is a complete b_0-space (or a B-domain; moreover, a BL-domain in terms of [1]). Obviously, the base subset $F(X_T)$ is constructivizible. The points a_ω and b_ω are constructive, whereas all other limit points (which are the upper bounds of a_ω, b_ω) are not. Thus, a_ω and b_ω, being consistent in X_T, are inconsistent in the subspace $C(X_T)$ of all constructive points of X_T.

The example shows that from the "constructive" point of view f_0-spaces behave better than b_0-spaces.

To conclude, we mention that spaces with constructive points can be used to define an effective semantics which, in turn, can serve as a programming language (semantic programming, cf. [9]). Moreover, effective versions of the spaces enable one to obtain generalizations of the theory through the use of arbitrary admissible sets (instead of ω) as it was done in [10] in the case of f_0-spaces.

References

1. Jung, A.: Cartesian Closed Categories of Domains. CWI Tract **66** Stichting Math. Centrum Amsterdam (1989)
2. Ershov, Yu. L.: La théorie des énumération. Actes Congr. Intern. Math. **1** Gauthier-Villars Paris (1971) 223–227
3. Scott, D.: Models for various type-free calculi. LMPS IV. Studies in Logic No 74 North–Holland Amsterdam (1973) 157–188
4. Ershov, Yu. L.: Theory of A-spaces. Algebra i Logika **12** No 4 (1973) 369–416
5. Scott, D.: Domains for denotational semantics. ICALP 82. Springer LNCS No 140 (1982) 577–613
6. Ershov, Yu. L.: Theory of enumerations [in Russian]. Nauka Moscow (1977)
7. Ershov, Yu. L.: Model $\mathbb{C}$ of partial continuous functionals. Logic Colloq.'76. Studies in Logic No 87 North–Holland Amsterdam (1977) 455–467
8. Peretyat'kin, M. G.: Strongly constructive models and enumerations of the boolean algebra of recursive sets. Algebra i Logika **10** No 5 (1971) 535–557
9. Goncharov, S. S., Ershov, Yu. L., and Sviridenko, D. I.: Semantic programming. Information Processing 86. North–Holland Amsterdam (1986) 1993–1100
10. Ershov, Yu. L.: On f_A-spaces. Algebra i Logika **25** No 5 (1986) 533–543