August 1997

Singular and plural non-deterministic parameters

Sigurd Meldal
San Jose State University, sigurd.meldal@sjsu.edu

M. A. Walicki

Follow this and additional works at: http://scholarworks.sjsu.edu/computer_eng_pub

Part of the Computer Engineering Commons

Recommended Citation
SINGULAR AND PLURAL NONDETERMINISTIC PARAMETERS*

MICHAL WALICKI† AND SIGURD MELDAL†

Abstract. The article defines algebraic semantics of singular (call-time-choice) and plural (run-time-choice) nondeterministic parameter passing and presents a specification language in which operations with both kinds of parameters can be defined simultaneously. Sound and complete calculi for both semantics are introduced. We study the relations between the two semantics and point out that axioms for operations with plural arguments may be considered as axiom schemata for operations with singular arguments.

Key words. algebraic specification, many-sorted algebra, nondeterminism, sequent calculus

AMS subject classifications. 68Q65, 68Q60, 68Q10, 68Q55, 03F60, 08A70

PII. S0097-5397(97)03178-0

1. Introduction. The notion of nondeterminism arises naturally in describing concurrent systems. Various approaches to the theory and specification of such systems, for instance, CCS [16], CSP [9], process algebras [1], and event structures [26], include the phenomenon of nondeterminism. But nondeterminism is also a natural concept in describing sequential programs, either as a means of indicating a “don’t care” attitude as to which among a number of computational paths will actually be utilized in a particular computation (e.g., [3]) or as a means of increasing the level of abstraction [14, 25]. The present work proceeds from the theory of algebraic specifications [4, 27] and generalizes the theory so that it can be applied to describing nondeterministic operations.

In deterministic programming the distinction between call-by-value and call-by-name semantics of parameter passing is well known. The former corresponds to the situation where the actual parameters to function calls are evaluated and passed as values. The latter allows parameters which are function expressions, passed by a kind of Algol copy rule [21], and which are evaluated whenever a need for their value arises. Thus call-by-name will terminate in many cases when the value of a function may be determined without looking at (some of) the actual parameters, i.e., even if these parameters are undefined. Call-by-value will, in such cases, always lead to undefined result of the call. Nevertheless, the call-by-value semantics is usually preferred in the actual programming languages since it leads to clearer and more tractable programs.

Following [20], we call the nondeterministic counterparts of these two notions singular (call-by-value) and plural (call-by-name) parameter passing. Other names applied to this, or closely related distinction, are call-time-choice vs. run-time-choice [2, 8] or inside-out (IO) vs. outside-in (OI), which reflect the substitution order corresponding to the respective semantics [5, 6]. In the context where one allows nondeterministic parameters, the difference between the two semantics becomes quite apparent even without looking at their termination properties. Let us suppose that
we have defined operation \( g(x) \) as “if \( x = 0 \) then \( a \) else (if \( x = 0 \) then \( b \) else \( c ) \)" and that we have a nondeterministic choice operation \( \sqcup \) returning an arbitrary element from the argument set. The singular interpretation will satisfy the formula \( \phi: g(x) = ( \text{if } x = 0 \text{ then } a \text{ else } c ) \), whereas the plural interpretation need not satisfy this formula. For instance, under the singular interpretation \( g(\sqcup \{0, 1\}) \) will yield either \( a \) or \( c \), whereas the set of possible results of \( g(\sqcup \{0, 1\}) \) under the plural interpretation will be \( \{a, b, c\} \). (Notice that in a deterministic environment both semantics would yield the same results.) The fact that the difference between the two semantics occurs already in very trivial examples of terminating nondeterministic operations motivates our investigation.

We discuss the distinction between the singular and the plural passing of nondeterministic parameters in the context of algebraic semantics, focusing on the associated reasoning systems. The singular semantics is given by multialgebras, that is, algebras where functions are set valued and where these values correspond to the sets of possible results returned by nondeterministic operations. Thus, if \( f \) is a nondeterministic operation, \( f(t) \) will denote the set of possible results returned by \( f \) when applied to \( t \). We introduce the calculus \( \text{NEQ} \) which is sound and complete with respect to this semantics.

Although terms may denote sets, the variables in the language range only over individuals. This is motivated by the interest in describing unique results returned by each particular application of an operation (execution of the program). It gives us the possibility of writing instead of a formula \( \Phi(f(t)) \), which expresses something about the whole set of possible results of \( f(t) \), the formula corresponding to \( x \in f(t) \Rightarrow \Phi(x) \), which express something about each particular result \( x \) returned by \( f(t) \). Unfortunately, this poses the main problem of reasoning in the context of nondeterminism—the lack of general substitutivity. From the fact that \( h(x) \) is deterministic (for each \( x \) has a unique value) we cannot conclude that so is \( h(t) \) for an arbitrary term \( t \). If \( t \) is nondeterministic, \( h(t) \) may have several possible results. The calculus \( \text{NEQ} \) is designed so that it appropriately restricts the substitution of terms for singular variables.

Although operations in multialgebras are set valued, their carriers are usual sets. Thus operations map individuals to sets. This is not sufficient to model plural arguments. Such arguments can be understood as sets being passed to the operation. The fact that, under plural interpretation, \( g(x) \) as defined above need not satisfy \( \phi \) results from the two occurrences of \( x \) in the body of \( g \). Each of these occurrences corresponds to a repeated application of choice from the argument set \( x \), that is, potentially, to a different value. In order to model such operations we take as the carrier of the algebra a (subset of the) power set—operations map sets to sets. In this way we obtain power algebra semantics. The extension of the semantics is reflected at the syntactic level by introduction of plural variables ranging over sets rather than over individuals. The sound and complete extension of \( \text{NEQ} \) is obtained by adding one new rule which allows for usual substitution of arbitrary terms for plural variables.

The structure of the paper is as follows. In sections 2 and 3 we introduce the language for specifying nondeterministic operations and explain the intuition behind its main features. In section 4 we define multialgebraic semantics for singular specifications and introduce a sound and complete calculus for such specifications. In section 5 the semantics is generalized to power algebras capable of modeling plural parameters, and the sound and complete extension of the calculus is obtained by introducing one additional rule. A comparison of both semantics in section 6 is guided by the similarity of the respective power algebras and power models which may serve also highlight the increased complexity problems with intuitive understanding.

Proofs of the theorems are motivated by the results from [24] where the

2. The specification language

signature \( \Sigma \) is a pair \((S,F)\) of sorts \((S)\) and result sorts \((S)\). The set of terms is denoted by \( \text{W}_\Sigma \). We always assume that \( S, S^\Sigma, \) is not empty.

\( \Sigma \) is a set of sequents of atomic formulas. The left-hand side of \( \Sigma \) is called the antecedent, and both are to be understood and multiplicity of the atomic formulas in the antecedent or consequent to be empty.

All variables occurring in a sequent occur in the whole sequent. A sequent is satisfiable if the antecedent is false or if one of \( a_1 \land \cdots \land a_n \Rightarrow e_1 \lor \cdots \lor e_m \) is valid.

For any term (formula set of \( \Sigma \)) \( \xi \) and \( \alpha \), if the variable set is not mentioned, then \( a \) is a variable.

An atomic formula in the context of \( \Sigma \) is a sequent with exactly one formula in the consequent and a Horn formula with empty antecedent.

For a given specification \( \text{SP} = (\Sigma, E) \) of signature \( \Sigma \),

the above conventions will be interpreted as nonempty intersection of term set and power model which may serve as a set of possibilities of the corresponding operation. We, on the other hand, demand facts, i.e., facts which have to hold. This is achieved by introducing the following

3. A note on the intuitive

interpretations in some framework (operations correspond to set-theory) is interpreted as a set of possibilities of the corresponding operation. We, on the other hand, demand facts, i.e., facts which have to hold. This is achieved by introducing the following

Every two syntactic occurrences of \( \text{SP} \) correspond to a repeated application of choice from the argument set \( \text{SP} \) is interpreted as a set of powers models which may serve as a set of possibilities of the corresponding operation. We, on the other hand, demand facts, i.e., facts which have to hold. This is achieved by introducing the following
else (if \( x = 0 \) then \( b \) else \( c \))" and \( \perp \) returning an arbitrary element \( a \) will satisfy the formula \( \phi \); \( g(x) \) interpretation need not satisfy this condition \( g(U \{0,1\}) \) will yield either \( a \) or \( b \) under the plural interpretation in environment both semantics would between the two semantics occurs terministic operations motivates

and the plural passing of nondeterministic ones, focusing on the associated by multialgebras, that is, algebras we correspond to the sets of possible Thus, if \( f \) is a nondeterministic is returned by \( f \) when applied to and complete with respect to this

in the language range only over describing unique results returned abstraction of the program). It gives \( \Phi(f(t)) \), which expresses something, the formula corresponding to each particular result \( x \) returned term of reasoning in the context of .

From the fact that \( h(x) \) is denot e that so is \( h(t) \) for an have several possible results. The restricts the substitution of terms

in. Their carriers are usual sets. Not sufficient to model plural arities being passed to the operation. Defined above need not satisfy \( \phi \) of \( g \). Each of these occurrences the argument set \( x \), that is, operations we take as the carrier \( x \) is map set to sets. In this way the semantics is reflected at the stage passing over sets rather than over NEQ is obtained by adding one necessary terms for plural variables.

Conventions 2 and 3 introduce the and explain the intuition behind terministic semantics for singular speciﬁcations for such speciﬁcations. In Webr is capable of modeling plural if the calculus is obtained by integrating semantics in section 6 is guided by the similarity of the respective calculi. We identify the subclasses of multimodels and power models which may serve as equivalent semantics of one speciﬁcation. We also highlight the increased complexity of the power algebra semantics reﬂecting the problems with intuitive understanding of parallel arguments.

Proofs of the theorems are merely indicated in this presentation. It reports some of the results from [24] where the full proofs and other details can be found.

2. The speciﬁcation language. A speciﬁcation is a pair \((\Sigma, \Pi)\), where the signature \(\Sigma\) is a pair \((S, F)\) of sorts \(S\) and operation symbols \(F\) (with argument and result sorts in \(S\)). The set of terms over a signature \(\Sigma\) and variable set \(X\) is denoted by \(W_{\Sigma,X}\). We always assume that, for every sort \(S\), the set of ground words of sort \(S\), \(S^{W_{\Sigma,X}}\), is not empty.\(^1\)

\(\Pi\) is a set of sequents of atomic formulas written as \(\alpha_1, \ldots, \alpha_n \Rightarrow \epsilon_1, \ldots, \epsilon_m\). The left-hand side (LHS) of \(\Rightarrow\) is called the antecedent and the right-hand side (RHS) the consequent, and both are to be understood as sets of atomic formulas (i.e., the ordering and multiplicity of the atomic formulas do not matter). In general, we allow either antecedent or consequent to be empty, though \(\emptyset\) is usually dropped in the notation. A sequent with exactly one formula in the consequent \((m = 1)\) is called a Horn formula, and a Horn formula with empty antecedent \((n = 0)\) is a simple formula (or a simple sequent).

All variables occurring in a sequent are implicitly universally quantiﬁed over the whole sequent. A sequent is satisﬁed if, for every assignment to the variables, one of the antecedents is false or one of the consequents is true (it is valid if the formula \(\alpha_1 \land \cdots \land \alpha_n \Rightarrow \epsilon_1 \lor \cdots \lor \epsilon_m\) is valid).

For any term (formula set of formulas) \(\xi\), \(\forall \xi\) will denote the set of variables in \(\xi\). If the variable set is not mentioned explicitly, we may also write \(x \in V\) to indicate that \(x\) is a variable.

An atomic formula in the consequent is either an equation, \(t = s\), or an inclusion, \(t \preceq s\), of terms \(t, s \in W_{\Sigma,X}\). An atomic formula in the antecedent, written \(t \prec s\), will be interpreted as nonempty intersection of the (result) sets corresponding to \(t\) and \(s\). For a given speciﬁcation \(SP = (\Sigma, \Pi)\), \(L(SP)\) will denote the above language over the signature \(\Sigma\).

The above conventions will be used throughout the paper. The distinction between the singular and the plural parameters (introduced in the section 5) will be reﬂected in the notation by the superscript \(*\): a plural variable will be denoted by \(x^*\), the set of plural variables in a term \(t\) by \(V^*[t]\), a speciﬁcation with plural arguments \(SP^*\), the corresponding extension of the language \(L\) by \(L^*\), etc.

3. A note on the intuitive interpretation. Multialgebraic semantics [10, 13] interprets speciﬁcations in some form of power structures where the (nondeterministic) operations correspond to set-valued functions. This means that a (ground) term is interpreted as a set of possibilities; it denotes the set of possible results of the corresponding operation. We, on the other hand, want our formulas to express necessary facts, i.e., facts which have to hold in every evaluation of a program (speciﬁcation). This is achieved by interpreting terms as applications of the respective operations. Every two syntactic occurrences of a term \(t\) will refer to possibly distinct applications of \(t\). For nondeterministic terms this means that they may denote two distinct values.

\(^1\)This restriction is motivated by the fact (pointed out in [7]) that admitting empty carriers requires additional mechanisms (explicit quantiﬁcation) in order to obtain sound logic. We conjecture that a similar solution can be applied in our case.
Typically, equality is interpreted in a multialgebra as set equality [13, 23, 12]. For instance, the formula \( \mapsto t = s \) means that the sets corresponding to all possible results of the operations \( t \) and \( s \) are equal. This gives a model which is mathematically plausible but which does not correspond to our operational intuition. The (set) equality \( \mapsto t = s \) does not guarantee that the result returned by some particular application of \( t \) will actually be equal to the result returned by an application of \( s \). It merely tells us that in principle (in all possible executions) any result produced by \( t \) can also be produced by \( s \) and vice versa.

Equality in our view should be a necessary equality which must hold in every evaluation of a program (specification). It does not correspond to set equality but to identity of one-element sets. Thus the simple formula \( \mapsto t = s \) will hold in a multistructure \( M \) if both \( t \) and \( s \) are interpreted in \( M \) as one and the same set which, in addition, has only one element. Equality is then a partial equivalence relation, and terms \( t \) for which \( \mapsto t = t \) holds are exactly the deterministic terms, denoted by \( D_{sp,x} \). This last equality indicates that arbitrary two applications of \( t \) have to return the same result.

If it is possible to produce a computation where \( t \) and \( s \) return different results—and this is possible when they are nondeterministic—then the terms are not equal but, at best, equivalent. They are equivalent if they are capable of returning the same results, i.e., if they are interpreted as the same set. This may be expressed using the inclusion relation: \( s \prec t \) holds iff the set of possible results of \( s \) is included in the set of possible results of \( t \), and \( s \prec t \) if each is included in the other.

Having introduced inclusion one might expect that a nondeterministic operation can be specified by a series of inclusions, each defining one of its possible results. However, such a specification gives only a “lower bound” on the admitted nondeterminism. Consider the following example.

**Example 3.1.**

\[
\begin{align*}
S & : \{\text{Nat}\}, \\
F & : 0: \to \text{Nat} \quad \text{(zero)} \\
& \quad s: \text{Nat} \to \text{Nat} \quad \text{(successor)} \\
& \quad \cup: \text{Nat} \times \text{Nat} \to \text{Nat} \quad \text{(binary nondeterministic choice)} \\
II & : (1) \mapsto 0 = 0 \\
& \quad (2) \mapsto s(x) = s(x) \\
& \quad (3) 1 \prec 0 \mapsto \\
& \quad (4) \mapsto 0 < 0 \lor 1 \mapsto 1 < 0 \lor 1
\end{align*}
\]

The first two axioms make zero and successor deterministic. A limited form of negation is present in \( \mathcal{L} \) in the form of sequents with empty consequent. Axiom (3) makes 0 distinct from 1. Axioms (4) make then \( \cup \) a nondeterministic choice with 0 and 1 among its possible results. This, however, ensures only that in every model both 0 and 1 can be returned by \( 0 \lor 1 \). In most models all other kinds of elements may be among its possible results as well, since no extension of the result set of \( 0 \lor 1 \) will violate the inclusions of (4). If we are satisfied with this degree of precision, we may stop here and use only the Horn formula. All the results in the rest of the paper apply to this special case. But to specify an “upper bound” of nondeterministic operations we need disjunction, the multiple formulas in the consequents. Now, if we write the axiom

\( (5) \mapsto 0 \lor 1 = 0 \lor 1 \)

the two occurrences of \( 0 \lor 1 \) return either 0 or 1; i.e., it is a nondeterministic term as referred to by binding both occurrences to \( t \).

\( (5') \mapsto x \prec 0 \lor 1 \mapsto x \)

The axiom says: whenever \( 0 \lor 1 \) returns either 0 or 1; i.e., it is a nondeterministic term as referred to by binding both occurrences to \( t \).

\( (5'') \mapsto x^* \prec 0 \lor 1 \mapsto x^* \)

would have a completely different syntax common in the literature on simply typed lambda calculus [2, 8, 11], in spite of terms for variables. Any substitution of a term for a variable would yield a unique result in the subsection on reasoning, one, for instance, to conclude 0 if \( 0 \lor 1 \) is one (though it could be obtained from \( x^* \)).

**4. The singular case:** Since the multialgebraic semantics of specification is sound and complete calculus.

**4.1. Multistructures and multihomomorphisms**

**Definition 4.2 (Multistructures).**

- **(1)** its carrier \( |M| \) is an \( S\)-multiset,
- **(2)** for every \( f: S_1 \times \cdots \times S_n \to S \), \( f^M: S_1^M \times \cdots \times S_n^M \to S^M \), a multihomomorphism from a \( S\)-multiset,
- **(H1)** for each constant symbol \( s \in S \), \( f(s^M) = s^M \),
- **(H2)** for each \( f: S_1 \times \cdots \times S_n \to S \), \( f(f^A(a_1 \cdots a_n)) \subseteq f^B(b_1 \cdots b_m) \)

If all inclusions in H1 and H2 are strict, the \( S\)-multiset is strictly loose (or just loose).

**Definition 4.3 (Multihomomorphisms).**

\( \Phi(f^A(a_1 \cdots a_n)) \subseteq f^B(b_1 \cdots b_m) \)

Since multihomomorphisms respect singletons and are \( S\)-monoidal.
The two occurrences of $0 \cup 1$ refer to two arbitrary applications and, consequently, we obtain that either any application of $0 \cup 1$ equals 0 or else it equals 1, i.e., that $\cup$ is not really nondeterministic but merely underspecified. Since axioms (4) require that both 0 and 1 be among the results of $t$, the addition of (5) will actually make the specification inconsistent.

What we are trying to say with the disjunction of (5) is that every application of $0 \cup 1$ returns either 0 or 1: i.e., we need a means of identifying two occurrences of a nondeterministic term as referring to one and the same application. This can be done by binding both occurrences to a variable. The appropriate axiom will be

$$(5') \quad x \sim 0 \cup 1 \leftrightarrow x = 0, x = 1.$$  

The axiom says: whenever $0 \cup 1$ returns $x$, then $x$ equals 0 or $x$ equals 1. Notice that such an interpretation presupposes that the variable $x$ refers to a unique, individual value. Thus bindings have the intended function only if they involve singular variables. (Plural variables, on the other hand, will refer to sets and not individuals, and so the axiom

$$(5'') \quad x^* \sim 0 \cup 1 \leftrightarrow x^* = 0, x^* = 1,$$

would have a completely different meaning.) The singular semantics is the most common in the literature on algebraic semantics of nondeterministic specification languages [2, 8, 11], in spite of the fact that it prohibits unrestricted substitution of terms for variables. Any substitution must now be guarded by the check that the substituted term yields a unique value, i.e., is deterministic. We return to this point in the subsection on reasoning, where we introduce a calculus which does not allow one, for instance, to conclude $0 \cup 1 = 0 \cup 1 \rightarrow 0 \cup 1 = 0, 0 \cup 1 = 1$ from the axiom $(5')$ (though it could be obtained from $(5'')$).

4. The singular case: Semantics and calculus. This section defines the multialgebraic semantics of specifications with singular arguments and introduces a sound and complete calculus.

4.1. Multistructures and multimodels. Let $\Sigma$ be a signature. $M$ is a $\Sigma$-multistructure if

1. its carrier $|M|$ is an $S$-sorted set,
2. for every $f: S_1 \times \cdots \times S_n \rightarrow S$ in $F$, there is a corresponding function $f^M: S_1^M \times \cdots \times S_n^M \rightarrow P^+(S^M)$.

A function $\Phi: A \rightarrow B$ (i.e., a family of functions $\Phi_S: S^A \rightarrow S^B$ for every $S \in S$) is a multihomomorphism from a $\Sigma$-multistructure $A$ to $B$ if

3. for each constant symbol $c \in F$, $\Phi(c^A) \subseteq c^B$,
4. for every $f: S_1 \times \cdots \times S_n \rightarrow S$ in $F$ and $a_1 \ldots a_n \in S_1^A \times \cdots \times S_n^A$,

$\Phi(f^A(a_1 \ldots a_n)) \subseteq f^B(\Phi(a_1) \ldots \Phi(a_n))$.

If all inclusions in H1 and H2 are (set) equalities the homomorphism is tight; otherwise it is strictly loose (or just loose).

$P^+(S)$ denotes the set of nonempty subsets of the set $S$. Operations applied to sets refer to their unique pointwise extensions. Notice that for a constant $c : \rightarrow S(2)$ indicates that $c^M$ can be a set of several elements of sort $S$.

Since multihomomorphisms are defined on individuals and not sets they preserve singletons and are $\subseteq$-monotonic. We denote the class of $\Sigma$-multistructures by
MStr(Σ). It has the distinguished word structure MWΣ defined in the obvious way, where each ground term is interpreted as a singleton set. We will treat such singleton sets as terms rather than one-element sets (i.e., we do not take special pains to distinguish MWΣ and WΣ). MWΣ is not an initial Σ-structure since it is deterministic and there can exist several homomorphisms from it to a given multistructure. We do not focus on the aspect of initiality and merely register the useful fact from [11].

LEMMA 4.3. \( M \) is a Σ-multistucture iff for every set of variables \( X \) and assignment \( β : X \rightarrow |M| \), there exists a unique function \( β[-] : W_{Σ,X} \rightarrow P^+(|M|) \) such that

1. \( β[x] = \{β(x)\} \),
2. \( β[c] = c^M \),
3. \( β[f(t_i)] = \bigcup \{f^M(y_i) \mid y_i \in β[t_i]\} \).

In particular, for \( X = \emptyset \) there is a unique interpretation function (not a multihomomorphism) \( I : W_Σ \rightarrow P^+(|M|) \) satisfying the last two points of this definition.

As a consequence of the definition of multistructures, all operations are \( Σ \)-monotonic, i.e., \( β(s) \subseteq β(t) \Rightarrow β[f(s)] \subseteq β[f(t)] \). Notice also that assignment in the lemma (and in general whenever it is an assignment of elements from a multistructure) means assignment of individuals, not sets.

Next we define the class of multimodels of a specification.

DEFINITION 4.4 (Satisfiability). A Σ-multistucture \( M \) satisfies an \( L(Σ) \) sequent \( π \)

\[ t_i \vdash s_i \Rightarrow p_j = r_j, m_k \leq n_k, \]

written \( M \models π \) iff for every \( β \) : \( X \rightarrow M \) we have

\[ \bigwedge_i β[t_i] \cap β[s_i] \neq \emptyset \Rightarrow \bigvee_j β[p_j] = β[r_j] \lor \bigvee_k β[m_k] \leq β[n_k], \]

where \( A = B \) iff \( A \) and \( B \) are the same one-element set.

An SP-multimodel is a Σ-multistucture which satisfies all the axioms of SP. We denote the class of multimodels of SP by MMod(SP).

The reason for using nonempty intersection (and not set equality) as the interpretation of \( \vdash \) in the antecedents is the same as using “elementwise” equality \( = \) in the consequents. Since we avoid set equality in the positive sense (in the consequents), the most natural negative form seems to be the one we have chosen. For deterministic terms this is the same as equality, i.e., deterministic antecedents correspond exactly to the usual (deterministic) conditions. For nondeterministic terms this reflects our interest in binding such terms: the sequent “\( \vdash t \rightarrow s \rightarrow t \) . . .” is equivalent to “\( \vdash x \rightarrow s, x \rightarrow t \rightarrow \ldots \) . . .”. A binding “\( x \rightarrow b \) . . .” is also equivalent to the more familiar “\( x \in t \ldots \rightarrow \ldots \)” so the notation \( s \vdash t \) may be read as an abbreviation for the more elaborate formula with two \( e \) and a new variable \( x \) not occurring in the rest of the sequent.

For a justification of this, as well as other choices we have made here, the reader is referred to [24].

4.2. The calculus for singular semantics. In [24] we introduced the calculus NEQ which is sound and complete with respect to the class MMod(SP). Its rules are as follows:

(R1) \( \vdash x = x, \quad x \in V \),

(R2) \( \Gamma_x \vdash \Delta_x \vdash \Gamma \vdash \Delta \),

(R3) \( \Gamma_x \vdash \Delta_x \vdash \Gamma \vdash \Delta \),

(R4) \( \vdash x \vdash y \vdash x = y \),

(R5) \( \Gamma, \Delta \vdash \Gamma, \Delta \),

(R6) \( \vdash \Delta, s \leq t \vdash \Delta' \),

(R7) \( \Gamma, x \vdash t \vdash \Delta, x \in \Gamma, \Delta \).

\( \Gamma_b \) denotes \( \Gamma \) with \( b \) substituted for \( b \) in order.

The fact that “=” is a part only to variables and is sound for (singular) variables.

(R2) is a paramodulation rule which is deterministic (in the case where \( t \vdash t \) does not hold), it allows derivation of the standard paramodulation rule for singular variables.

(R3) allows “specialization” of a term \( t \) which is included in \( t \) but not substituted for don’t occur in the consequent.

(R4) and \( R5 \) express the relation of substitution and inclusion in the consequent.

(R5) is unsound conclusion \( \vdash t \rightarrow t \) . . .

(R7) eliminates redundant bindings of \( \vdash \).

We will write \( \Pi \vdash _{CAL} π \) to indicate a derivation in CAL.

The counterpart of soundness is proved in [24].

THEOREM 4.5. NEQ is sound with respect to MMod(SP).

Proof idea. Soundness is proved by a style argument. The axiom set \( \Pi \vdash _{CAL} π \).
defined in the obvious way, a set. We will treat such singleton sets not to take special pains to dis-structure since it is deterministic to a given multistructure. We do not set equality (not a multiho-structure, all operations are \( \leq \)-mono- also that assignment in the lemma de­mension, assignment in the lemma genenents from a multistructure) means ciﬁcation.

an \( \varepsilon \)-structure \( M \) satisfies an \( \Lambda(\Sigma) \) sequent

satisfies all the axioms of \( SP \). We

Also, equality (not set equality) as the interpre-

tation function (not a multihop-t of this definition.

structures, all operations are \( \leq \)-mono-

that assignment in the lemma de-
mension, assignment in the lemma genenents from a multistructure) means ciﬁcation.

an \( \varepsilon \)-structure \( M \) satisfies an \( \Lambda(\Sigma) \) sequent

satisfies all the axioms of \( SP \). We


\[ \forall k \left( \beta[m_k] \leq \beta[n_k] \right), \]

\( \varepsilon \)-structure.

The fact that “\( = \)” is a partial equivalence relation is expressed in (R1). It applies only to variables and is sound because all assignments assign individual values to the (singular) variables.

(R2) is a paramodulation rule allowing replacement of terms which may be de-
terministic (in the case where \( t_1 = t_2 \) holds in the second assumption). In particular, it allows derivation of the standard substitution rule when the substituted terms are deterministic and prevents substitution of nondeterministic terms for variables.

(R3) allows “specialization” of a sequent by substituting for a term \( t_2 \) another term \( t_1 \) which is included in \( t_2 \). The restriction that the occurrences of \( t_2 \) which are substituted for don’t occur in the RHS of \( \prec \) is needed to prevent, for instance, the unsound conclusion \( \vDash t_1 \prec t_2 \) from the premises \( \vDash s \prec t_2 \) and \( \vDash \neg s \prec t_2 \).

(R4) and (R5) express the relation between \( \sim \) in the antecedent and the equality in the consequent. The axiom of standard sequent calculus, \( \vDash s \prec t \rightarrow e \equiv e \), (i.e., \( \vDash s \prec t \rightarrow s \leq t \)) does not hold in general here because the antecedent corresponds to nonempty intersection of the result sets while the consequent to the inclusion \( \prec \) or identity of one-element \( = \) result sets. Only for deterministic terms (in particular, variables) \( s, t \) do we have that \( \vDash s \prec t \rightarrow s = t \) holds.

(R5) allows us to cut both \( \vDash s = t \) and \( \vDash s \prec t \) with \( s \sim t \rightarrow \Delta \).

(R7) eliminates redundant bindings, namely those that bind an application of a term occurring at most once in the rest of the sequent.

We will write \( \Pi \vdash_{\text{CAL}} \pi \) to indicate that \( \pi \) is provable from \( \Pi \) with the calculus CAL.

The counterpart of soundness/completeness of the equational calculus is as follows [24].

**Theorem 4.5.** NEQ is sound and complete with respect to MMod(SP):

\[ \Pi \vdash_{\text{CAL}} \pi \iff \Pi \vdash_{\text{NEQ}} \pi. \]

**Proof idea.** Soundness is proved by induction on the length of the proof \( \Pi \vdash_{\text{NEQ}} \pi \). The proof of the completeness part is a standard, albeit rather involved, Henkin-style argument. The axiom set \( \Pi \) of SP is extended by adding all \( \Lambda(\Sigma) \) formulas \( \pi \).
which are consistent with \( \Pi \) (and the previously added formulas). If the addition of \( \pi \) leads to inconsistency, one adds the negation of \( \pi \). Since empty consequents provide only a restricted form of negation, the general negation operation is defined as a set of formulas over the original signature extended with new constants. One shows then that the construction yields a consistent specification with a deterministic basis from which a model can be constructed.

We also register an easy lemma that the set-equivalent terms \( t \sim s \) satisfy the same formulas.

\[ \text{LEMMA 4.6. } t \sim s \text{ iff, for any sequent } \pi, \Pi \vdash_{\text{NEQ}} \pi \iff \Pi \vdash_{\text{NEQ}} \pi. \quad \square \]

5. The plural case: Semantics and calculus. The singular semantics for passing non-deterministic arguments is the most common notion to be found in the literature. Nevertheless, the plural semantics has also received some attention. In the denotational tradition most approaches considered both possibilities [18, 19, 20, 22]. Engelfriet and Schmidt gave a detailed study of both—in their language, IO and "OI"—semantics based on tree languages [5] and continuous algebras of relations and power sets [6]. The unified algebras of Mosses [17] and the rewriting logic of Meseguer [15] represent other algebraic approaches distinguishing these aspects.

We will define the semantics for specifications where operations may have both singular and plural arguments. The next subsection gives the necessary extension of the calculus NEQ to handle this generalized situation.

5.1. Power structures and power models. Singular arguments (such as the variables in \( \mathcal{L} \)) have the usual algebraic property that they refer to a unique value. This reflects the fact that they are evaluated at the moment of substitution and the result is passed to the following computation. Plural arguments, on the other hand, are best understood as textual parameters. They are not passed as a single value, but every occurrence of the formal parameter denotes a distinct application of the operation.

We will allow both singular and plural parameter passing in one specification. The corresponding semantic distinction is between power set functions which are merely \( \subseteq \)-monotonic and those which also are \( \cup \)-additive.

In the language, we merely introduce a notational device for distinguishing the singular and plural arguments. We allow annotating the sorts in the profiles of the operation by a superscript, like \( S^* \), to indicate that an argument is plural.

Furthermore, we partition the set of variables into two disjoint subsets of singular \( X \) and plural \( X^* \) variables. \( x \) and \( x^* \) are to be understood as distinct symbols. We will say that an operation \( f \) is singular in the \( i \)th argument iff the \( i \)th argument (in its signature) is singular. The specification language extended with such annotations of the signatures will be referred to as \( \mathcal{L}^* \).

These are the only extensions of the language we need. We may, optionally, use superscripts \( t^* \) at any (sub)term to indicate that it is passed as a plural argument. The outermost applications, e.g., \( f \) in \( f(...) \), are always to be understood plurally, and no superscripting will be used at such places.

**DEFINITION 5.1.** Let \( \Sigma \) be a \( \mathcal{L}^* \)-signature. A is a \( \Sigma \)-power structure \( A \in PStr(\Sigma) \) iff \( A \) is a (deterministic) structure such that

1. for every sort \( S \), the carrier \( S^A \) is a (subset of the) power set \( P^+(S^-) \) of some basis set \( S^- \),
2. for every \( f : S_1 \times \cdots \times S_n \to S \) in \( \Sigma \), \( f^A \) is a \( \subseteq \)-monotonic function \( S_1^A \times \cdots \times S_n^A \to S^A \) such that if the \( i \)th argument is \( S_i \) (singular), then \( f^A \) is singular in the \( i \)th argument.

The singularity in the ith argument is merely a notion but to its semantic counterpart.

**DEFINITION 5.2.** A function \( A \) is singular in the \( i \)th argument if \( f \) is singular in the \( i \)th argument and \( x_i \in S_i^A \) and all \( x_k \in S_k^A \) for \( k \neq i \) and \( x_k \in x_k \).

Thus, the definition of plugging a function into a function is modeled by the semantic one.

Note the unorthodox point of view. Instead of using a whole power set but allow it to be modeled by a finite (or infinite) set of subsets. If all finite subsets are needed for modeling the join operation (under the set theory) union only if all sets are present necessary. Consequently, we do not allow the \( \cup \)-additive ones. Instead, give the user means of constructing them (as in choice) directly.

Let \( \Sigma \) be a signature, \( A \) and \( X^* \) a set of plural variables, and \( A = A_{X^*} \). Then \( x \in X : |\beta(x)| = 1 \). (Saying as \( A_{X^*} = A \) in \( A \).

\[ \text{LEMMA 4.6. } \text{ (R8) } \Gamma \vdash \Delta \iff \Gamma \vdash \Delta^* \cdot \]

A is a power model of the specification \( \text{PMo} \), and \( A \) satisfies all axioms from \( \text{PMo} \).

Except for the change in the rules \( \text{R8} \) and \( \text{R10} \), which is the reason for replacing \( \Pi \) with \( \Pi^* \).

5.2. The calculus for power models. The new rule (R8) expresses the fact that we can substitute an arbitrary term \( t \) for a plural variable \( x \). In particular, any \( t_i \) may be a plural argument.

\[ \text{THEOREM 5.4. } \text{For any } \mathcal{L}^*, \text{PMo} \cdot \]

The new rule (R8) expresses the fact that we can substitute an arbitrary term \( t \) for a plural variable \( x \). In particular, any \( t_i \) may be a plural argument.

The opposite is, in general, not sufficient for performing operations. The main result concerning \( \text{PMo} \) is:
The singularity in the i-th argument in this definition refers not to the syntactic notion but to its semantic counterpart.

**Definition 5.2.** A function \( f^A : S_1^A \times \cdots \times S_n^A \to S^A \) in a power structure \( A \) is singular in the i-th argument iff it is \( U \)-additive in the i-th argument, i.e., iff for all \( x_i \in S_i^A \) and all \( x_k \in S_k^A \) (for \( k \neq i \)), \( f^A(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) = \bigcup \{ f^A(x_1, \ldots, x_i = x, \ldots, x_n) \mid x \in x_i \} \).

Thus, the definition of power structures requires that syntactic singularity be modeled by the semantic one.

Note the unorthodox point in the definition: we do not require the carrier to be the whole power set but allow it to be a subset of some power set. Usually one assumes a primitive nondeterministic operation with the predefined semantics as set union. Then all finite subsets are needed for the interpretation of this primitive operator. Also, the join operation (under the set inclusion as partial order) corresponds exactly to set union only if all sets are present (see Example 6.8). None of these assumptions seem necessary. Consequently, we do not assume any predefined (choice) operation but, instead, give the user means of specifying any nondeterministic operation (including choice) directly.

Let \( \Sigma \) be a signature, \( A \) a \( \Sigma \)-power structure, \( X \) a set of singular variables and \( X^* \) a set of plural variables, and \( \beta \) an assignment \( X \cup X^* \to \{ A \} \) such that for all \( x \in X : |\beta(x)| = 1 \). (Saying assignment we will from now on mean only assignments satisfying this last condition.) Then, every term \( t(x, x^*) \in W_{\Sigma, X, X^*} \) has a unique set interpretation \( \beta[t(x, x^*)] \) in \( A \) defined as \( \beta^A(\beta(x), \beta(x^*)) \).

**Definition 5.3 (Satisfiability).** Let \( A \) be a \( \Sigma \)-power structure and \( \pi : t_i \rightarrow s_i \vdash p_j = r_j, m_k = n_k \) be a sequent over \( L^*(\Sigma, X, X^*) \). \( A \) satisfies \( \pi \), \( A \models \pi \), iff for every assignment \( \beta : X \cup X^* \to \{ A \} \), we have that

\[
\bigwedge_i \beta[t_i] \cap \beta[s_i] \neq \emptyset \rightarrow \bigvee_j \beta[p_j] = \beta[r_j] \lor \bigvee_k \beta[m_k] \leq \beta[n_k].
\]

A is a power model of the specification \( SP = (\Sigma, \Pi) \), \( A \in \text{PMod}(SP) \), iff \( A \in \text{PStr}(\Sigma) \) and \( A \) satisfies all axioms from \( \Pi \).

Except for the change in the notion of an assignment, this is identical to Definition 4.4, which is the reason for retaining the same notation for the satisfiability relation.

**5.2. The calculus for plural parameters.** The calculus \( \text{NEQ} \) is extended with one additional rule:

\[
\Gamma \vdash A \quad \Gamma' \vdash A';
\]

\[
\text{(R8)} \quad \Gamma, x \vdash A; \quad \Gamma', x \vdash A';
\]

Rules (R1)–(R7) remain unchanged, but now all terms \( t_i \) belong to \( W_{\Sigma, X, X^*} \). In particular, any \( t_i \) may be a plural variable. We let \( \text{NEQ}^* \) denote the calculus \( \text{NEQ} + \text{R8} \).

The new rule (R8) expresses the semantics of plural variables. It allows us to substitute an arbitrary term \( t \) for a plural variable \( x^* \). Taking \( t \) to be a singular variable \( x \), we can thus exchange plural variables in a provable sequent \( \pi \) with singular ones. The opposite is, in general, not possible because rule (R1) applies only to singular variables. For instance, a plural variable \( x^* \) will satisfy \( \rightarrow x^* < x^* \), but this is not sufficient for performing a general substitution for a singular variable. The main result concerning \( \text{PMod} \) and \( \text{NEQ}^* \) is as follows.

**Theorem 5.4.** For any \( L^* \)-specification \( SP \) and \( L^* \) (\( SP \)) sequent \( \pi \):

\[
\text{PMod}(SP) \models \pi \text{ iff } \Pi \vdash \text{NEQ}^* \pi.
\]
Proof idea. The proof is a straightforward extension of the proof of Theorem 4.5.

6. Comparison. Since plural and singular semantics are certainly not one and the same thing, it may seem surprising that essentially the same calculus can be used for reasoning about both. One would perhaps expect that PMod, being a richer class than MMod, will satisfy fewer formulas than the latter and that some additional restrictions of the calculus would be needed to reflect the increased generality of the model class. In this section we describe precisely the relation between the $L$ and $L^*$ specifications (section 6.1) and emphasize some points of difference (section 6.2).

6.1. The “equivalence” of both semantics. The following example illustrates a strong sense of equivalence of $L$ and $L^*$.

Example 6.1. Consider the following plural definition:

$$
\forall f(x^*) \iff x^* = x^* \text{ then } 0 \text{ else } 1.
$$

It is “equivalent” to the collection of definitions

$$
\forall f(t) \iff t = t \text{ then } 0 \text{ else } 1
$$

for all terms $t$.

In the rest of this section we will clarify the meaning of this “equivalence.”

Since the partial order of functions from a set $A$ to the power set of a set $B$ is isomorphic to the partial order of additive (and strict, if we take $P$ (all subsets) instead of $P^+$) functions from the power set of $A$ to the power set of $B$, $[A \rightarrow P(B)] \simeq [P(A) \rightarrow P(B)]$, we may consider every multistructure $A$ in a power structure $A^*$ by taking $A^* = P^+(A)$ and extending all operations in $A$ pointwise. We then have the obvious lemma.

Lemma 6.2. Let $SP$ be a singular specification (i.e., all operations are singular in all arguments), let $A \in MStr(SP)$, and let $\pi$ be a sequent in $L(SP)$. Then $A \models \pi$ iff $A^* \models \pi$, and so $A \in MMod(SP)$ iff $A^* \in PMod(SP)$.

Call an $L^*$ sequent $\pi$ p-ground (for plurally ground) if it does not contain any plural variables.

Theorem 6.3. Let $SP^* = (\Sigma^*, \Pi^*)$ be an $L^*$ specification. There exists a (usually infinite) $L$ specification $SP = (\Sigma, \Pi)$ such that

1. $W_{\Sigma, X} = W_{\Sigma^*, X}$
2. for any p-ground $\pi \in L^*(SP^*) : PMod(SP^*) \models \pi$ iff $MMod(SP) \models \pi$.

Proof. Let $\Sigma$ be $\Sigma^*$ with all “$\ast$” symbols removed. This makes (1) true. Any p-ground $\pi$ as in (2) is then a $\pi$ over the language $L(\Sigma, X)$.

The axioms $\Pi$ are obtained from $\Pi^*$ as in Example 6.1. For every $\pi^* \in \Pi^*$ with plural variables $x^*_1 \cdots x^*_n$, let $\pi = (\pi^* x^*_1 \cdots x^*_n | t_1 \cdots t_n \in W_{\Sigma, X})$. Obviously, for any $\pi \in L(SP)$ if $\Pi \models \text{NEQ } \pi$ then $\Pi^* \models \text{NEQ } \pi$. If $\Pi^* \models \text{NEQ } \pi$ then the proof can be simulated in NEQ. Let $\pi'(x^*)$ be the last sequent used in the NEQ*-proof which contains plural variables $x^*$ and the sequent $\pi'$ be the one that is used in the first branch of the diagram (R8).

Build the analogous NEQ-proof tree with all plural variables replaced by the terms which occupy their place in $\pi'$. The leaves of this tree will be instances of the $\Pi^*$ axioms with plural variables replaced by the appropriate terms, and all such axioms are in $\Pi$. Then soundness and completeness of NEQ and NEQ* imply the conclusion of the theorem. $\square$

We now ask whether, or under what conditions, MMod could be reduced to PMod (or vice versa), and if so, how. The one-way transition is trivial: obviously, any $\Pi \models \text{MMod } \Pi$.

For the other direction, we need to check several cases in the theorem is crucial: sets, undenotable, sets. Let $MMod'(SP)$ be the class of all $\Theta$-ground $\Pi$-models of $SP^*$ that $\beta(x^*) = \{m_1 \cdots m_k \cdots \}$ is an assignment equal to $\beta_1$.

Example 6.4. Let $M^* \in MMod'(SP)$ and $p_j = r_j, m_k < n_k$ with $x^* \in Y^*$, let $\beta(x^*) = \{m_1 \cdots m_k \cdots \}$ is an assignment equal to $\beta_1$.

$$
M^* \models \beta[\pi^*] \iff
$$

(a) $M^* \models \bigcup_{i \in \Theta} \beta_i[t_i] \cap \bigcup_{i \in \Sigma} \beta_i[s_i] 

(b) $M^* \models \beta[t_i] \cap \beta[s_i] 

But (b) does not necessarily imply (a). The reason is that operations in $M^*$ are defined in a way that, for all $i$,

$$
(\text{b) } M^* \models \beta[t_i] \cap \beta[s_i] 
$$

is not necessarily true. To ensure that (a) holds, we redefine the plural variables we redefine the plural variables we redefine the plural variables we redefine the plural variables we redefine the plural variables we redefine the plural variables we redefine.
SINGULAR AND PLURAL NONDETERMINISTIC PARAMETERS

We now ask whether, or under which conditions, the classes PMod and MMd are interchangeable as the models of a specification. Let SP*, SP be as in the theorem. The one-way transition is trivial. Axioms of SP are p-ground, so PMod(SP*) will satisfy all these axioms by the theorem. The subclass \( \downarrow \operatorname{PMod}(SP^*) \subseteq \operatorname{PMod}(SP^*) \), where for every \( P \in \downarrow \operatorname{PMod}(SP^*) \) all operations are singular, will yield a subclass of MMd(SP).

For the other direction, we have to observe that the restriction to p-ground sequents in the theorem is crucial because plural variables range over arbitrary, also undenotable, sets. Let MMd*(SP) denote the class of power structures obtained as in Lemma 6.2. It is not necessarily the case that MMd*(SP) \( \models \Pi^* \), as the following argument illustrates.

Example 6.4. Let \( M^* \in \text{MMd}^*(SP) \) have infinite carrier, \( \pi^* \in \Pi^* \) be \( t_i \sim s_i \mapsto p_j = r_j, m_k \sim \eta_k \) with \( x^* \in \forall[\pi^*] \), and \( \beta: X \times X^* \rightarrow [M^*] \) be an assignment such that \( \beta(x^*) = \{m_1, \ldots, m_i, \ldots\} \) is a set which is not denoted by any term in \( W_{\Sigma, X} \). Let \( \beta \) be an assignment equal to \( \beta \) except that \( \beta(x^*) = \{m_1\} \), i.e., \( \beta = \beta_1 \). Then \( M^* \models \beta[\pi^*] \) if

\[
M^* \models \beta(t_i) \cap \beta(s_i) \neq \emptyset \Rightarrow \beta(p_j) \equiv \beta(r_j) \lor \ldots \lor \beta(m_k) \leq \beta[n_k] \quad \text{iff}
\]

(a) \( M^* \models i_{\beta(t_i)} \cap i_{\beta(s_i)} \neq \emptyset \Rightarrow i_{\beta(p_j)} = i_{\beta(r_j)} \lor \ldots \lor i_{\beta(m_k)} \leq i_{\beta[n_k]} \)

since operations in \( M^* \) are defined by pointwise extension. \( M^* \in \text{MMd}^*(SP) \) implies that, for all \( l \)

(b) \( M^* \models i_{\beta(t_i)} \cap i_{\beta(s_i)} \neq \emptyset \Rightarrow i_{\beta(p_j)} = i_{\beta(r_j)} \lor \ldots \lor i_{\beta(m_k)} \leq i_{\beta[n_k]} \).

But (b) does not necessarily imply (a). In particular, even if for all \( l \), all intersections in the antecedent of (b) are empty, those in (a) may be nonempty. So we are not guaranteed that \( M^* \in \text{PMod}(SP^*) \).

Thus, the intuition that the multismodels are contained in the power models is not quite correct. To ensure that no undenotable sets from \( M^* \) can be assigned to the plural variables we redefine the lifting operator \( \ast: \text{MMd}(SP) \rightarrow \text{PMod}(SP) \) from Lemma 6.2.

Definition 6.5. Given a singular specification \( SP \) and \( M \in \text{MMd}(SP) \), we denote by \( |M| \) the following power structure:

1. (1) \( |M| \mid M \subseteq \mathcal{P}^+(|M|) \) is such that
   a. for every \( n \in |M|: \{n\} \in |M| \),
   b. for every \( m \in |M| \) there exists a \( a \in W_{\Sigma, X}, n \in |M| \) such that:
      \( t^M(n) = m \).

2. (2) The operations in \( |M| \) can be then defined by: \( f(|m|)^M = f(t(|m|))^M \).

Then, for any assignment \( \beta: X^* \rightarrow |M| \) there exists an assignment \( \theta: X^* \rightarrow W_{\Sigma, X} \) \( 1 \) and an assignment \( \alpha: X \rightarrow |M| \) \( 1 \) such that \( \beta(x^*) = \alpha \theta(x^*) \) (2), i.e., such that the diagram in Figure 1 commutes.

Since \( M \in \text{MMd}(SP) \), it satisfies all the axioms \( \Pi \) obtained from \( \Pi^* \) and the commutativity of the figure gives us the second part of the following.

Corollary 6.6. Let \( SP^* \) and \( SP \) be as in Theorem 6.3. Then

\[
\downarrow \operatorname{PMod}(SP^*) \models \Pi, \text{ i.e., } \downarrow \operatorname{PMod}(SP^*) \subseteq \operatorname{MMd}(SP) \),
\]

\[
\downarrow \operatorname{MMd}(SP) \models \Pi^* , \text{ i.e., } \downarrow \operatorname{MMd}(SP) \subseteq \operatorname{PMod}(SP^*) .
\]
The corollary makes precise the claim that the class of power models of a plural specification $SP^*$ may be seen as a class of multimodels of some singular specification $SP$ and vice versa. The reasoning about both semantics is essentially the same because the only difference concerns the (arbitrary) undenotable sets which can be referred to by plural variables.

6.2. Plural specification of choice. Plural variables provide access to arbitrary sets. In the following example we attempt to utilize this fact to give a more concise form to the specification of choice.

Example 6.7. The specification

$$S: \{ S \},$$

$$F: \{ \sqcup_-, : S^* \to S \},$$

$$II: \{ \sqcup_-, x^* \sqcup_-, \}$$

defines $\sqcup_-$ as the choice operator: for any argument $t, \sqcup_- t$ is capable of returning any element belonging to the set interpreting $t$.

The specification may seem plausible, but there are several difficulties. Obviously, such a choice operation would be redundant in any specification since the axiom makes $\sqcup_- t$ observationally equivalent to $t$, and Lemma 4.6 allows us to remove any occurrences of $\sqcup_-$ from the (derivable) formulas. Furthermore, observe how such a specification confuses the issue of nondeterministic choice. Choice is supposed to take a set as an argument and return one element from the set or, perhaps, to convert an argument of type “set” to a result of type “individual.” This is the intention behind writing the specification above. But power algebras model all operations as functions on power sets and such a “conversion” simply does not make sense. The only points where conversion of a set to an individual takes place is when a term is passed as a singular argument to another operation. If we have an operation with a singular argument $f: S \to S$, then $f(t)$ will make (implicitly) the choice from $t$.

This might be particularly confusing because one tends to think of plural arguments as sets and mix up the semantic sets (i.e., the elements of the carrier of a power algebra) and the syntactic ones (as expressed by the profiles of the operations in the

signature). As a matter of fact, we are forced to imagine the intention of choosing an element in the set $t$. By definition, choice the signature $Set(S) \to \mathcal{P}(t)$ is specified by $Set(S)$ is specified by $\mathcal{P}(t)$ to $\mathcal{P}(S)$. Assuming $\mathcal{P}$ to the power set construction, we are unable to refer to a set with a power set of a power set, and thus we cannot let the same variable stand for the choice from the set $t$.

Example 6.7 and remarks significantly complicate the meaning of plural parameters. On the other hand, plural variables provide access to arbitrary sets and may significantly complicate the model.

Example 6.8. The following signature $S$ is specified with respect to all terms. (Not just $t$) whenever $\rightarrow s < p$ and $\rightarrow s < p$ (see Figure 2). Violating our intuition shows the validity of the form $s < p \rightarrow \sqcup_- t, \sqcup_- s < p$.

Thus, in any model of the signature $\rightarrow$ $\rightarrow$ it is then natural to consider $\sqcup_-$ as the join which under nondeterministic choice would have a different, and in several cases, the same signature $\rightarrow$ $\rightarrow$ we have to rework the signature $\rightarrow$ $\rightarrow$, $\rightarrow$ of the model. For instance, the model $\rightarrow$ $\rightarrow$ $\rightarrow$ $\rightarrow$

such that $\rightarrow$ $\rightarrow$ will be a model of the specification $\rightarrow$ $\rightarrow$.

7. Conclusion. We have considered both singular (run-time-choice) and plural (run-time-choice).

The central results reported in the
class of power models of a plural specification is essentially the same because sets which can be referred to variables provide access to arbitrary elements which can be utilized this fact to give a more

Example 6.7 and remarks illustrate some of the problems with the intuitive understanding of plural parameters. Power algebras, needed for modeling such parameters, significantly complicate the model of nondeterminism as compared with multialgebras.

On the other hand, plural variables allow us to specify the "upper bound" of nondeterministic choice without using disjunction. The choice operation can be specified as the join which under the partial ordering \(<\) interpreted as set inclusion will correspond to set union (cf. [17]).

Example 6.8. The following specification makes binary choice the join operation wrt. \(<\):

\[
S: \{ \emptyset \},
F: \{ \sqcup : S \times S \to S \},
\Pi: \{ (1) \quad x^* \prec x^* \sqcup y^* \quad \iff \quad y^* \prec z^* \sqcup y^* \\
(2) \quad x^* \prec z^* \quad \text{if} \quad y^* \prec z^* \}
\]

Axiom (2) although using singular variables \(x, y\), does specify the minimality of \(\sqcup\) with respect to all terms. (Notice that the axiom \(x^* \prec z^* \quad \text{if} \quad y^* \prec z^* \) would have a different, and in this context unintended, meaning.) We can show that whenever \(t \prec p\) and \(s \prec p\) hold (for arbitrary terms) then so does \(t \sqcup s \prec p\) (see Figure 2). Violating our formalism a bit, we may say that the above proof shows the validity of the formula stating the expected minimality of join: \(t \prec p, s \prec p \implies t \sqcup s \prec p\).

Thus, in any model of the specification from Example 6.8 \(\sqcup\) will be a join. It is then natural to consider \(\sqcup\) as the basic (primitive) operation used for defining other nondeterministic operations. Observe also that in order to ensure that join is the same as set union, we have to require the presence of all (finite) subsets in the carrier of the model. For instance, the power structure \(A\) with the carrier

\[
S^A = \{ \{1\}, \{2\}, \{3\}, \{1, 2, 3\} \}
\]

will be a model of the specification although \(\sqcup^A\) is not the same as set union.

7. Conclusion. We have defined the algebraic semantics for singular (call-time-choice) and plural (run-time-choice) passing of nondeterministic parameters. One of the central results reported in the paper is soundness and completeness of two new
reasoning systems NEQ and NEQ*, respectively, for singular and plural semantics. The plural calculus NEQ* is a minimal extension of NEQ which merely allows unrestricted substitution for plural variables. This indicated a close relationship between the two semantics. We have shown that plural specifications have equivalent (modulo undenotable sets) singular formulations if one considers the plural axioms as singular axiom schemata.

Acknowledgments. We are grateful to Manfred Broy for pointing out the inadequacy of our original notation and to Peter D. Mosses for the observation that in the presence of plural variables choice may be specified as join with Horn formulas.

REFERENCES

SINGULAR AND PLURAL NONDETERMINISTIC PARAMETERS

Switzerland, 1981.


