Expressibility in the Kleene Algebra of Partial Predicates with the Complement Composition

Ievgen Ivanov(✉) and Mykola Nikitchenko

Taras Shevchenko National University of Kyiv,
64/13, Volodymyrska Street, Kyiv 01601, Ukraine
ivanov.eugen@gmail.com, nikitchenko@unicyb.kiev.ua

Abstract. In the paper we investigate the expressibility of partial predicates in the Kleene algebra extended with the composition of predicate complement and give a necessary and sufficient condition of this expressibility in terms of the existence of an optimal solution of an optimization problem. We also investigate the expressibility in the first-order Kleene algebra with predicate complement. The obtained results may be useful for software verification using an extension of the Floyd-Hoare logic for partial pre- and postconditions.

Keywords: Formal methods · Software verification · Partial predicate · Floyd-Hoare logic

1 Introduction

A popular approach to software verification is based on application of Floyd-Hoare logic [1,2] which allows one to derive valid assertions (triples) of the form $\{p\}f\{q\}$, where f is a program, p is a precondition, and q is a postcondition. Assertions are interpreted as follows: if an input data d of the program f satisfies the precondition p, and the program terminates on d, then the program's output satisfies the postcondition q. The classical Floyd-Hoare logic admits the case when the program f has an undefined execution result (e.g. due to nontermination). However, the pre- and postcondition predicates are assumed to have a definite truth value (true or false). In some situations the latter assumption is not convenient and it makes sense to consider pre- and postconditions expressed by partial predicates which can be undefined on some data. This can happen, e.g., if pre- and postconditions can be most easily expressed using partial operations such as division of numbers. Then one has to either reinterpret/change the meaning of classical Floyd-Hoare triples and take into account partiality of predicates, or try to eliminate the need to ever deal with undefined predicate values by performing special well-formedness checks which imply that predicates are applied only to values on which they can be guaranteed to be defined.

V. Ermolayev et al. (Eds.): ICTERI 2019, CCIS 1175, pp. 50–67, 2020.
https://doi.org/10.1007/978-3-030-39459-2_3

Both approaches lead to certain complications: the former one leads to multiple possible triple interpretations, some of which make the rules of the classical Floyd-Hoare logic unsound; the latter one complicates triple derivations by requiring definedness of predicates in all intermediate derivation steps which may be inessential to the validity of a target triple.

When explicit unrestricted partial pre- and postconditions are allowed, at least two obvious generalized interpretations of a triple $\{p\}f\{q\}$ can be given [9]:

(a) "strong triple": if the precondition p is defined and true on the program's input, and the program terminates with a result y, then the postcondition q is defined on y, and q is true on y.
(b) "weak triple": if the precondition p is defined and true on the program's input, and the program terminates with a result y, and the postcondition q is defined on y, then q is true on y.

The "weak triple" interpretation makes the rules of the classical Floyd-Hoare logic unsound [14,15], but this interpretation is attractive in the case of high-level verification of code implementing numerical algorithms in environments like Matlab or Octave and in other similar applications. In this sort of situations, during formal verification it is difficult to take into account all details of implementation of floating-point arithmetic and give precise error bounds for an algorithm implementation. Algorithm verification using the model of ideal real number/rational number arithmetic can be much more feasible and can be useful for detecting high-level flaws (unrelated to floating point arithmetic). In particular, such models are used in VerSAA [1] verifier for Matlab code and in Simulink Design Verifier. However, e.g., during high-level verification of a numerical algorithm in the model of ideal real number arithmetic in most cases it makes no sense to formally prove that zero values never appear in the denominators of division expressions in postconditions, since, anyway, the behavior of a verification model is an inexact approximation of the behavior of an actual program. So, in order to ensure validity of a triple under "strong triple" interpretation one is required to prove more (i.e. to prove a stronger statement) than what is necessary to prove the validity of a triple under "weak triple" interpretation, while the information content in the statement about triple validity relevant to the real-world decision making is essentially the same in both cases.

In the previous papers [4,5,9,11–13,16] we investigated an inference system for a variant of an extension of Floyd-Hoare logic for partial pre- and postconditions which is sound under "weak triple" interpretation. The formulation of the rules of this inference system requires the change of semantics (and, it turns out, syntax) of the logical language which is used to express the pre- and postcondition formulas. Note that the formulation of the rules of the classical Floyd-Hoare logic depends on the usual boolean compositions ($\neg$, $\wedge$) which are applied to total predicates which appear in the program's body and/or pre- and postconditions, e.g. the loop rule uses both the conjunction and negation:

$$\frac{\{r \wedge p\}\ f\ \{p\}}{\{p\}\ \textbf{while}\ r\ \textbf{do}\ f\ \textbf{end}\ \{\neg r \wedge p\}}$$

Here p represents the loop invariant.

The formulation of the rules of the mentioned extension of Floyd-Hoare logic depends on compositions of partial predicates (from program's body and/or pre- and postconditions). In this situation one needs to express and interpret compositions of predicates in terms of a certain three-valued logic, where the third truth value corresponds to the case where a predicate is undefined.

From the viewpoint of pragmatics, propositional compositions of such a logic have to be based on a finite system of functions of three-valued logic (P_3) which contains reasonable generalized versions of boolean negation and conjunction. In P_3 there exist multiple sets of functions which, arguably, fit this description. One choice is the system $\{f_T, f_F, f_U, f_\neg, f_\wedge\}$, where f_T, f_F, f_U are pairwise different constant functions (T for "true", F for "false", U for "undefined"), and $f_\neg$, $f_\wedge$ are, respectively, an unary and binary operation on a 3 element set defined in accordance with the truth tables for negation and conjunction of Kleene's strong 3-valued logic, i.e.

x	F	U	T
$f_\neg(x)$	T	U	F

x	F	U	T
$f_\wedge(x,F)$	F	F	F
$f_\wedge(x,U)$	F	U	U
$f_\wedge(x,T)$	F	U	T

This system is not functionally complete in P_3, and, it turns out, the corresponding propositional compositions of predicates are not sufficient for representing the sequence and loop rules of the inference system of [9] for "weak triple" interpretation. A functionally complete (in P_3) extension of $\{f_T, f_F, f_U, f_\neg, f_\wedge\}$ is sufficient for this purpose, but, from the results of [9] it turns out that a certain extension of $\{f_T, f_F, f_U, f_\neg, f_\wedge\}$ which is not functionally complete in P_3 is also sufficient. Such an extension can be obtained by adjoining to $\{f_T, f_F, f_U, f_\neg, f_\wedge\}$ an unary function $f_\sim$ defined as follows:

x	F	U	T
$f_\sim(x)$	U	T	U

The propositional composition of partial predicates corresponding to $f_\sim$ was called in [9] the predicate complement and denoted as $\sim$. This composition can be used to extend the signature of the Kleene algebra of partial predicates [10]. Using such an extended signature, the loop rule of an extended Floyd-Hoare logic for partial pre- and postconditions with "weak triple" interpretation can be reformulated as [9]:

$$\frac{\{r \wedge p\}\ f\ \{p\}, \{r \wedge (\sim p)\} f \{p\}}{\{p\}\ \textbf{while}\ r\ \textbf{do}\ f\ \textbf{end}\ \{\neg r \wedge p\}}$$

In this paper we investigate the question of expressibility of partial predicates in the Kleene algebra extended with the composition of predicate complement

and give a necessary and sufficient condition of this expressibility in terms of the existence of an optimal solution of a special constrained optimization problem.

This is closely related to the properties of the functional closure of $\{f_T, f_F, f_U, f_\neg, f_\wedge, f_\sim\}$. The number of n-ary functions in this closure is $2^{3^n+O(2^n)}$ (see Proposition 2 in Sect. 3), which is asymptotically lower than the cardinality of the set of all n-ary operations on a three element set (3^{3^n}), and these functions have special properties that can be useful for software verification using the above mentioned extended Floyd-Hoare logic for partial pre- and postconditions and "weak triple" interpretation. For example (see Lemma 4 in Sect. 5), when checking satisfiability of an expression $E(x_1, ..., x_n)$ over $\{f_T, f_F, f_U, f_\neg, f_\wedge, f_\sim\}$ by searching for a "true" value of E in some search space S, any evaluation of $E(x_1, ..., x_n)$ which gives the "false" value can be used to eliminate from S elements which belong a metric ball with center $(x_1, ..., x_n)$ and radius 1 in the sense of Chebyshev distance (the cardinality of which is at least 2^n).

2 Notation

Unless indicated otherwise, n will denote an integer number.

The notation $f : A \tilde{\to} B$ means that f is a partial function on a set A with values in a set B, and $f : A \to B$ means that f is a total function from A to B.

The notation $x \mapsto e(x)$, where e is some expression, denotes a function which maps x to $e(x)$. The domain of this function should be clear from the context.

For a function $f : A \tilde{\to} B$:

- $f(x)\downarrow$ means that f is defined on x;
- $f(x)\downarrow = y$ means that f is defined on x and $f(x) = y$;
- $f(x)\uparrow$ means that f is undefined on x;
- $dom(f) = \{x \in A \mid f(x)\downarrow\}$ is the domain of a function.

We will denote as $f_1(x_1) \cong f_2(x_2)$ the *strong equality*, i.e. $f_1(x_1)\downarrow$ if and only if $f_2(x_2)\downarrow$, and if $f_1(x_1)\downarrow$, then $f_1(x_1) = f_2(x_2)$.

The symbols T, F will denote the "true" and "false" values of predicates and $Bool = \{T, F\}$. The symbol $\perp$ will denote a nowhere defined partial predicate.

Depending on the context, $|\cdot|$ will denote either the cardinality of a set, or the absolute value of an (integer) number.

We will use $\circ$ to denote functional composition: $(f \circ g)(x) \cong f(g(x))$.

3 Preliminaries

Let $D \neq \emptyset$ be a set, $n \geq 1$, and P_1, ..., P_n be partial predicates on D.

The Kleene algebra of partial predicates on D with predicate complement and constants $P_1, ..., P_n$ is the algebra

$$APr_{P_1,...,P_n}(D) = (D \tilde{\to} \{T, F\}; \vee, \wedge, \neg, \sim, P_1, P_2, ..., P_n),$$

where

1. $\vee, \wedge, \neg$ are the operations of *disjunction*, *conjunction* and *negation* on partial predicates defined in accordance with Kleene's strong three-valued logic as follows:

$$(P \vee Q)(d) = \begin{cases} T, & \text{if } P(d) \downarrow = T \text{ or } Q(d) \downarrow = T; \\ F, & \text{if } P(d) \downarrow = F \text{ and } Q(d) \downarrow = F; \\ \text{undefined} & \text{in other cases.} \end{cases}$$

$$(P \wedge Q)(d) = \begin{cases} T, & \text{if } P(d) \downarrow = T \text{ and } Q(d) \downarrow = T; \\ F, & \text{if } P(d) \downarrow = F \text{ or } Q(d) \downarrow = F; \\ \text{undefined} & \text{in other cases.} \end{cases}$$

$$(\neg P)(d) = \begin{cases} T, & \text{if } P(d) \downarrow = F; \\ F, & \text{if } P(d) \downarrow = T; \\ \text{undefined} & \text{in other case.} \end{cases}$$

2. $\sim$ is the unary operation of *predicate complement*:

$$(\sim P)(d) = \begin{cases} T, & \text{if } P(d) \uparrow; \\ \text{undefined}, & \text{if } P(d) \downarrow . \end{cases}$$

Let V, W be non-empty sets, $n \geq 1$, and Q_1, ..., Q_n be partial predicates on $V \tilde{\to} W$ (i.e. the set of all partial functions on V which take values in W). The elements of V will be interpreted as *variable names*, the elements of W as *values*, and the elements of $V \tilde{\to} W$ as partial variable assignments.

Denote $QPr_W^V = (V \tilde{\to} W) \tilde{\to} \{T, F\}$. We will call the elements of the set QPr_W^V *partial quasiary predicates* over V and W. For a fixed finite V, such elements can be considered as continuations of partial n-ary predicates on W for $n = |V|$ to the cases when some arguments are undefined with the possibility of having a defined ("true" or "false") value when some arguments are undefined, e.g. if $Q \in QPr_W^V$, $Q(d)$ may take the "true" value when d is nowhere defined on V (empty variable assignment).

An *existential quantification composition* $\exists v$ (with parameter $v \in V$) is an unary operation on QPr_W^V such that for each $Q \in QPr_W^V$:

$$(\exists v(Q))(d) = \begin{cases} T, & \text{if } Q(d\nabla^v a) \downarrow = T \text{ for some } a \in W; \\ F, & \text{if } Q(d\nabla^v a) \downarrow = F \text{ for all } a \in W; \\ \text{undefined} & \text{in other cases,} \end{cases}$$

where $d\nabla^v a$ denotes the element of $V \tilde{\to} W$ with the graph

$$\{(v, a)\} \cup \{((v', d(v')) \mid v' \in V \backslash \{v\}, d(v') \downarrow\}.$$

When one restricts attention to total predicates and total variable assignments over a fixed finite V, $\exists v$ has the meaning corresponding to the meaning of the existential quantifier in the classical first order logic.

Similarly, a *universal quantification composition* $\forall v$ (with parameter $v \in V$) is an unary operation on QPr^V_W such that for each $Q \in QPr^V_W$:

$$(\forall v(Q))(d) = \begin{cases} T, & \text{if } Q(d\nabla^v a) \downarrow = T \text{ for all } a \in W; \\ F, & \text{if } Q(d\nabla^v a) \downarrow = F \text{ for some } a \in W; \\ \text{undefined} & \text{in other cases.} \end{cases}$$

A *renomination (variable renaming) composition* $R^{\bar{u}}_{\bar{v}}$ with parameters $\bar{u} = (u_1, ..., u_n) \in V^n$ and $\bar{v} = (v_1, ..., v_n) \in V^n$ (where $n \geq 1$) such that $u_1, u_2, ..., u_n$ are pairwise different, is an unary operation on QPr^V_W such that for each $Q \in QPr^V_W$ and $d \in {}^V W$:

$$R^{\bar{u}}_{\bar{v}}(Q)(d) \cong Q(r^{\bar{u}}_{\bar{v}}(d)),$$

where $r^{\bar{u}}_{\bar{v}}(d) = d \circ rn^{\bar{u}}_{\bar{v}}$ and $rn^{\bar{u}}_{\bar{v}} : V \to V$ is the function with the graph $\{(u_1, v_1), ..., (u_n, v_n)\} \cup \{(u, u) \mid u \in V \backslash \{u_1, ..., u_n\}\}$.

The first-order Kleene algebra of partial predicates over the set of variable names V and values W with predicate complement and constants $Q_1, ..., Q_n$ is the algebra

$$\begin{aligned} &AQPr_{Q_1,...,Q_n}(V, W) \\ &\quad = (QPr^V_W; \vee, \wedge, \neg, \sim, \{R^{\bar{u}}_{\bar{v}}\}_{n' \geq 1, \bar{u} \in V^{n'}_{\neq}, \bar{v} \in V^{n'}}, \{\exists v\}_{v \in V}, \{\forall v\}_{v \in V}, Q_1, ..., Q_n), \end{aligned}$$

where $\vee, \wedge, \neg, \sim$ are defined as above for $D = V \tilde{\to} W$, and $V^{n'}_{\neq}$ is the set of tuples $(v_1, ..., v_{n'}) \in V^{n'}$ such that $v_i \neq v_j$ for all $i, j \in \{1, 2, ..., n'\}$ such that $i \neq j$.

Note that for a finite V the signature of $AQPr_{Q_1,...,Q_n}(V, W)$ contains only finitely many unary operation symbols.

We will also use the following algebra which we call the renominative Kleene algebra of partial predicates with predicate complement and constants $Q_1, ..., Q_n$:

$$ARPr_{Q_1,...,Q_n}(V, W) = (QPr^V_W; \vee, \wedge, \neg, \sim, \{R^{\bar{u}}_{\bar{v}}\}_{n' \geq 1, \bar{u} \in V^{n'}_{\neq}, \bar{v} \in V^{n'}}, Q_1, ..., Q_n).$$

We will say that a variable name $v \in V$ is unessential for a quasiary predicate $Q : (V \tilde{\to} W) \tilde{\to} Bool$, if $Q(d|_{V \backslash \{v\}}) \cong Q(d)$ for all $d \in V \tilde{\to} W$.

Let $X = \{-1, 0, 1\}$ and $F^{(n)}$ be the set of all n-ary functions (operations) $f : X^n \to X$. The elements of $F^{(n)}$ will represent functions of 3-valued logic P_3 (where 1 corresponds to the "true" value and -1 corresponds to the "false" value, and 0 is an intermediate truth value).

Let $F = \bigcup_{n \geq 0} F^{(n)}$.

We will denote as $\bar{x} = (x_1, x_2, ..., x_n)$ a tuple of values $x_i \in X$.

Consider X^n as a metric space with Chebyshev distance:

$$\rho_n((x_1, ..., x_n), (y_1, ..., y_n)) = \max_{i=1}^{n} |x_i - y_i|.$$

Proposition 1. *For $n \geq 1$, the equilateral metric dimension*[1] *of the metric space (X^n, ρ_n) is 2^n.*

Proof. Let us show by induction on n that $|A| \leq 2^n$ for any set $A \subseteq X^n$ such that $\rho_n(\bar{x}, \bar{y}) = \rho_n(\bar{x}', \bar{y}')$ for all $\bar{x}, \bar{y}, \bar{x}', \bar{y}' \in A$ such that $\bar{x} \neq \bar{y}$ and $\bar{x}' \neq \bar{y}'$ (equidistant subset).

Induction base ($n = 1$). The set $\{-1, 0, 1\}$ is not an equidistant subset, so $|A| \leq 2$ for any equidistant subset $A \subseteq X$.

Induction step. Assume that for $n \geq 1$ it holds that $|A| \leq 2^n$ for any equidistant subset A in (X^n, ρ_n). Let A' be an equidistant subset in (X^{n+1}, ρ_{n+1}). Let $A_j = \{(x_1, ..., x_n) \mid (x_1, ..., x_n, j) \in A'\}$ for $j \in \{-1, 0, 1\}$.

For each $j \in \{-1, 1\}$, $\bar{x} = (x_1, ..., x_n) \in A_0 \cup A_j$, and $\bar{y} = (y_1, ..., y_n) \in A_0 \cup A_j$ such that $\bar{x} \neq \bar{y}$ we have:

1. there exist $k, l \in \{0, j\}$ such that $\bar{x} \in A_k$ and $\bar{y} \in A_l$ and $|k - l| \leq 1$.
2. moreover, $\rho_n(\bar{x}, \bar{y}) = \max_{i=1}^n |x_i - y_i| = \max(\max_{i=1}^n |x_i - y_i|, |k - l|)$ $= \rho_{n+1}((x_1, ..., x_n, k), (y_1, ..., y_n, l))$, where $(x_1, ..., x_n, k)$ and $(y_1, ..., y_n, l)$ are distinct elements of A'.

Since A' is an equidistant subset, we have that $A_0 \cup A_{-1}$ and $A_0 \cup A_1$ are equidistant subsets in (X^n, ρ_n). By induction hypothesis, $|A_0 \cup A_j| \leq 2^n$ for $j \in \{-1, 1\}$.

Also note that $A_{-1} \cap A_0 \cap A_1 = \emptyset$, because otherwise, there exists a tuple $(x_1, ..., x_n) \in X^n$ such that $(x_1, ..., x_n, j) \in A'$ for each $j \in \{-1, 0, 1\}$, which contradicts the assumption that A' is an equidistant subset.

Then $|A'| = |A_{-1}| + |A_0| + |A_1| = |A_{-1} \cup A_0| + |A_{-1} \cap A_0| + |A_1|$
$= |A_{-1} \cup A_0| + |(A_{-1} \cap A_0) \cup A_1| + |A_{-1} \cap A_0 \cap A_1|$
$\leq |A_{-1} \cap A_0| + |A_0 \cup A_1| \leq 2 \cdot 2^n = 2^{n+1}$.

We conclude that $|A| \leq 2^n$ for each $n \geq 1$ and each equidistant subset A in (X^n, ρ_n).

On the other hand, for each $n \geq 1$ we have $|\{0, 1\}^n| = 2^n$ and $\{0, 1\}^n$ is an equidistant subset in (X^n, ρ_n), since $\rho_n(\bar{x}, \bar{y}) = \max_{i=1}^n |x_i - y_i| = 1$ for each $\bar{x} = (x_1, ..., x_n) \in \{0, 1\}^n$ and $\bar{y} = (y_1, ..., y_n) \in \{0, 1\}^n$ such that $\bar{x} \neq \bar{y}$.

Thus for $n \geq 1$ the equilateral metric dimension of (X^n, ρ_n) is 2^n. □

We will say that a function $f \in F^{(n)}$ is *short*, if it is a short map, i.e. if for all $\bar{x}$, $\bar{y}$ we have

$$|f(\bar{x}) - f(\bar{y})| \leq \rho_n(\bar{x}, \bar{y}).$$

Let $M^{(n)}$ be the set of all short functions from $F^{(n)}$.

Proposition 2. $|M^{(n)}| = 2^{3^n + O(2^n)}$

[1] The maximum cardinality of a subset such that any two of its distinct points are at the same distance.

Proof. Since X^n has 2^{3^n} subsets, it is sufficient to show that for any $n \geq 1$ and $Z \subseteq X^n$ the number of distinct functions from $M^{(n)}$ which have the set of zeros Z belongs to $\{1, 2, 3, ..., 2^{2^n}\}$.

Let $n \geq 1$ and $Z \subseteq X^n$. Denote $M_Z^{(n)} = \{f \in M^{(n)} \mid f^{-1}(\{0\}) = Z\}$.

Let $f_Z \in F^{(n)}$ be a function such that $f_Z(\bar{x}) = 1$ for $\bar{x} \in X^n \backslash Z$ and $f_Z(\bar{x}) = 0$ for $\bar{x} \in Z$. Then for each $\bar{x}, \bar{y} \in X^n$ such that $\bar{x} \neq \bar{y}$ we have $|f_Z(\bar{x}) - f_Z(\bar{y})| \leq 1 \leq \leq \rho_n(\bar{x}, \bar{y})$. This and the definition of f_Z imply that $f_Z \in M_Z^{(n)}$. Then $|M_Z^{(n)}| \geq 1$.

If $Z = X^n$, then $|M_Z^{(n)}| = 1 \in \{1, 2, ..., 2^{2^n}\}$.

Now assume that $Z \neq X^n$.

Let $G = (X^n, E)$ be the $\{1\}$-distance graph of the metric space (X^n, ρ_n), i.e. vertices $\bar{x},\ \bar{y} \in X^n$ are connected by an edge in E if and only if $\rho_n(\bar{x}, \bar{y}) = 1$, and let G_Z be a subgraph induced in G by the set of vertices $X^n \backslash Z \neq \emptyset$. Each $f \in M_Z^{(n)}$ is a graph homomorphism from G_Z to the graph $(\{-1, 1\}, \{\{-1\}, \{1\}\})$ ($\{a\}$ denotes a loop), because for each $\bar{x}, \bar{y} \in X^n \backslash Z$ such that $\rho_n(\bar{x}, \bar{y}) = 1$ we have $|f(\bar{x}) - f(\bar{y})| \leq 1$, $f(\bar{x}) \neq 0$, and $f(\bar{y}) \neq 0$, whence $f(\bar{x}) = f(\bar{y})$. Hence f is constant on the vertex set of each connected component of G_Z.

Denote as C_Z the set of connected components of G_Z. There exists a choice function $c : C_Z \to X^n$ which selects a vertex from each element of C_Z. Then for each $f_1, f_2 \in M_Z^{(n)}$, $f_1 \circ c = f_2 \circ c$ implies $f_1|_{X^n \backslash Z} = f_2|_{X^n \backslash Z}$ and $f_1|_Z = f_2|_Z$, whence $f_1 = f_2$. Then the map $f \mapsto f \circ c$ is injective on $M_Z^{(n)}$ and takes values in $\{-1, 1\}^{C_Z}$. Then $|M_Z^{(n)}| \leq |\{-1, 1\}^{C_Z}| = 2^{|C_Z|}$.

Denote as $c(C_Z)$ the image of C_Z under c. We have $|C_Z| = |c(C_Z)|$, since the sets of vertices of connected components are pairwise disjoint and c in injective. Moreover, $c(C_Z)$ is an equidistant subset in the metric space (X^n, ρ_n), because distinct elements $\bar{x}, \bar{y} \in c(C_Z)$ belong to different connected components of G_Z and are not connected by an edge in E, and this implies $\rho_n(\bar{x}, \bar{y}) = 2$. Then Proposition 1 implies that $|c(C_Z)| \leq 2^n$. Hence $|M_Z^{(n)}| \leq 2^{|C_Z|} \leq 2^{2^n}$.

Thus the number of distinct functions from $M^{(n)}$ which have the set of zeros Z belongs to $\{1, 2, 3, ..., 2^{2^n}\}$ and we conclude that $|M^{(n)}| = 2^{3^n + O(2^n)}$. □

4 Expressibility in Kleene Algebra

As before, let $X = \{-1, 0, 1\}$.

For any set D and a partial predicate $P : D \tilde{\to} \{T, F\}$ denote by $\Phi(P)$ a function from $D \to X$ such that for all $d \in D$:

$$\Phi(P)(d) = \begin{cases} 1, & \text{if } P(d) \downarrow = T, \\ 0, & \text{if } P(d) \uparrow, \\ -1, & \text{if } P(d) \downarrow = F. \end{cases}$$

Note that Φ is a bijection between $D \tilde{\to} \{T, F\}$ and $D \to X$.

Let $D \neq \emptyset$ be a fixed set, $P_0, P_1, ..., P_n : D \tilde{\to} \{T, F\}$ be partial predicates, and $p_i = \Phi(P_i)$ for $i = 0, 1, 2, ..., n$.

Denote $||f|| = \sum_{\bar{x} \in X^n} |f(\bar{x})|$ for $f \in F^{(n)}$ and consider the following (constrained) optimization problem[2]:

$$||f|| \to \min \tag{1}$$

$$f(p_1(d), p_2(d), ..., p_n(d)) = p_0(d), \quad d \in D \tag{2}$$

The following theorem characterizes expressibility in the Kleene algebra of partial predicates with predicate complement.

Theorem 1. *If $n \geq 1$, a predicate P_0 is expressible in the algebra $APr_{P_1,...,P_n}(D)$ if and only if on the set $F^{(n)}$ the problem (1)–(2) has an optimal solution which is a short function.*

The proof of this theorem is given in the next section.

$APr_{P_1,...,P_n}(D)$ induces the following pseudo-metric $\tilde{\rho}_{P_1,...,P_n}$ on D:

$$\tilde{\rho}_{P_1,...,P_n}(d, d') = \rho_n((p_1(d), ..., p_n(d)), (p_1(d'), ..., p_n(d'))).$$

Note that the sum of $\tilde{\rho}_{P_1,...,P_n}$ and any metric on D is a metric on D.

A predicate P_0 is called short with respect to (w.r.t.) $P_1, ..., P_n$, if p_0 is a short map between the pseudo-metric space $(D, \rho_{P_1,...,P_n})$ and (X, ρ_1).

Theorem 2. *If $n \geq 1$, P_0 is expressible in the algebra $APr_{P_1,...,P_n}(D)$ if and only if P_0 is short with respect to $P_1, P_2, ..., P_n$.*

Proof. "If": Assume that P_0 is short w.r.t. $P_1, P_2, ..., P_n$. Then for all $d, d' \in D$:

$$|p_0(d) - p_0(d')| \leq \tilde{\rho}_{P_1,...,P_n}(d, d') = \rho_n((p_1(d), ..., p_n(d)), (p_1(d'), ..., p_n(d'))).$$

For each $\bar{x} = (x_1, ..., x_n) \in X$ let $F(\bar{x}) = \{p_0(d) \mid d \in D \wedge \bigwedge_{i=1}^{n} p_i(d) = x_i\}$ and $f : X^n \to X$ be a function such that $f(\bar{x}) \in F(\bar{x})$, if $F(\bar{x}) \neq \emptyset$, and $f(\bar{x}) = 0$, if $F(\bar{x}) = \emptyset$. Since p_0 is a short map, $F(\bar{x})$ is a singleton set whenever $F(\bar{x}) \neq \emptyset$. Then $f(p_1(d), p_2(d), ..., p_n(d)) = p_0(d)$ for all $d \in D$.

Let $\bar{x} = (x_1, ..., x_n) \in X^n$, $\bar{y} = (y_1, ..., y_n) \in X^n$. Assume that $\bar{x} \neq \bar{y}$. If $F(\bar{x}) = \emptyset$ or $F(\bar{y}) = \emptyset$, then $f(\bar{x}) = 0$ or $f(\bar{y}) = 0$, whence $|f(\bar{x}) - f(\bar{y})| \leq 1 \leq \rho_n(\bar{x}, \bar{y})$. Otherwise, $F(\bar{x}) \neq \emptyset$ and $F(\bar{y}) \neq \emptyset$, so $f(\bar{x}) = p_0(d_x)$ and $f(\bar{y}) = p_0(d_y)$ for some $d_x, d_y \in D$ such that $p_i(d_x) = x_i$ and $p_i(d_y) = y_i$ for $i = 1, 2, ..., n$. Then $|f(\bar{x}) - f(\bar{y})| = |p_0(d_x) - p_0(d_y)| \leq \rho_n(\bar{x}, \bar{y})$. We conclude that $f \in M^{(n)}$.

Let $g \in F^{(n)}$ be a function such that $g(p_1(d), ..., p_n(d)) = p_0(d)$ for all $d \in D$, Then $f(\bar{x}) = g(\bar{x})$ whenever $F(\bar{x}) \neq \emptyset$. Then $||f|| \leq ||g||$, since $f(\bar{x}) = 0$ when $F(\bar{x}) = \emptyset$. Thus on the set $F^{(n)}$ the problem (1)–(2) has an optimal solution which is a short function. Then by Theorem 1, P_0 is expressible in $APr_{P_1,...,P_n}(D)$.

"Only if": Assume that P_0 is expressible in $APr_{P_1,...,P_n}(D)$. Then by Theorem 1, there exists $f \in M^{(n)}$ such that $f(p_1(d), p_2(d), ..., p_n(d)) = p_0(d)$ for all

[2] If one interprets partiality in terms as possibility, minimization of $||f||$ may be related to the principle of minimum specificity of D. Dubois et al. from possibility theory, or other similar principles.

$d \in D$. Then for all $d, d' \in D$:

$$|p_0(d) - p_0(d')| \leq |f(p_1(d), ..., p_n(d)) - f(p_1(d'), ..., p_n(d'))| \leq \tilde{\rho}_{P_1,...,P_n}(d, d').$$

□

Let $V \neq \emptyset$, $W \neq \emptyset$ be fixed sets, $Q_0, Q_1, ..., Q_n : (V \tilde{\to} W) \tilde{\to} \{T, F\}$ be partial quasiary predicates, and $q_i = \Phi(Q_i)$ for $i = 0, 1, 2, ..., n$.

If $k \geq 0$ and $m \in [0, 2^k - 1]$ are integers, and $\bar{v} = (v_1, ..., v_k) \in V^k$ (we assume V^0 consists of the single empty tuple), denote by $\mathfrak{Q}^k_{m,\bar{v}}(P)$, where P is a partial predicate, the k-th element of the finite sequence of predicates T_j, $j = 0, 1, ..., k$ such that $T_0 = P$ and for all $j = 1, 2, ..., k$:

$$T_{j+1} = \begin{cases} \exists v_j(T_j), & b_j = 0; \\ \forall v_j(T_j), & b_j = 1, \end{cases}$$

where (b_j) is the j-th digit in the binary expansion of m (starting from the least significant digit).

The following theorem characterizes expressibility in the first-order Kleene algebra of partial predicates with predicate complement.

Theorem 3. *Assume that $n \geq 1$ and there exists an infinite set $V' \subseteq V$ such that each name in V' is unessential for each predicate in $\{Q_0, Q_1, ..., Q_n\}$. Then Q_0 is expressible in the algebra $AQPr_{Q_1,...,Q_n}(V, W)$ if and only if there exist*

- *integers $l \geq 1$, $k \geq 0$, $m \in [0, 2^k - 1]$,*
- *a tuple $\bar{v} \in V^k$,*
- *finite sequences of integers $k_j \geq 1$ and $n_j \in [1, n]$ for $j = 1, 2, ..., l$,*
- *finite sequences of tuples $\bar{u}_j \in V^{k_j}_{\neq}$, $\bar{v}_j \in V^{k_j}$ for $j = 1, 2, ..., l$,*
- *and a partial predicate P on $V \tilde{\to} W$, short w.r.t. $R^{\bar{u}_j}_{\bar{v}_j}(Q_{n_j})$ for $j = 1, 2, ..., l$,*

such that $Q_0 = \mathfrak{Q}^k_{m,\bar{v}}(P)$.

We will give a proof of this theorem in Sect. 6.

5 Proof of Theorem 1

In order to prove Theorem 1, first let us formulate and prove a number of auxiliary lemmas.

Denote for all $x, y \in X$:

$$\neg x = -x$$

$$\sim x = 1 - |x|$$

$$x^{[y]} = \begin{cases} x, & \text{if } y = 1 \\ \sim x, & \text{if } y = 0 \\ \neg x, & \text{if } y = -1 \end{cases}$$

Lemma 1. *$\rho_n(\bar{x}, \bar{y}) = 1 - \min_{i=1}^{n} x_i^{[y_i]}$ for every $n \geq 1$ and $\bar{x}, \bar{y} \in X^n$.*

Proof. It is easy to see that for all $x, y \in X$:

$$x^{[y]} = 1 - |x - y|$$

Then $\rho_n(\bar{x}, \bar{y}) = \max_{i=1}^{n} |x_i - y_i| = \max_{i=1}^{n}(1 - x_i^{[y_i]}) = 1 - \min_{i=1}^{n} x_i^{[y_i]}$. □

Consider X as a lattice with operations:

$$x \vee y = \max(x, y);$$

$$x \wedge y = \min(x, y).$$

Below we will assume that in expressions involving operations on X the operation $x^{[y]}$ has the highest priority, and is followed (by priority) by the unary operations $\neg$, $\sim$, which are followed by the binary operations $\wedge$ and $\vee$. As usual, among $\wedge, \vee$, the operation $\wedge$ has higher priority.

Lemma 2. *For each short function $f \in F^{(n)}$ and $\bar{x} \in X^n$:*

$$f(\bar{x}) = \hat{f}(\bar{x}) \wedge f_{\neq 0}(\bar{x}) \vee \neg f_{\neq 0}(\bar{x})$$

where

$$\hat{f}(\bar{x}) = \begin{cases} \bigvee_{\bar{y}: f(\bar{y})=1} \bigwedge_{i=1}^{n} x_i^{[y_i]}, & \text{if } \exists \bar{y}\ f(\bar{y}) = 1 \\ -1, & \text{otherwise} \end{cases}$$

$$f_{\neq 0}(\bar{x}) = \begin{cases} \bigvee_{\bar{y}: f(\bar{y}) \neq 0} \bigwedge_{i=1}^{n} \sim (x_i^{[y_i]} \wedge \sim x_i^{[y_i]}) \wedge \sim\sim x_i^{[y_i]}, & \text{if } \exists \bar{y}\ f(\bar{y}) \neq 0 \\ 0, & \text{otherwise.} \end{cases}.$$

Proof. It is easy to see that for each $x, y \in X$:

$$\sim (x^{[y]} \wedge \sim x^{[y]}) \wedge \sim\sim x^{[y]} = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{if } x \neq y. \end{cases}$$

Then

$$f_{\neq 0}(\bar{x}) = \begin{cases} 1, & \text{if } f(\bar{x}) \neq 0 \\ 0, & \text{if } f(\bar{x}) = 0. \end{cases}$$

By Lemma 1,

$$\hat{f}(\bar{x}) = \begin{cases} \bigvee_{\bar{y}: f(\bar{y})=1} (1 - \rho_n(\bar{x}, \bar{y})), & \text{if } \exists \bar{y}\ f(\bar{y}) = 1, \\ -1, & \text{otherwise.} \end{cases}$$

If $f(\bar{x}) = 1$, then $\hat{f}(\bar{x}) = 1$ and $f_{\neq 0}(\bar{x}) = 1$, so $\hat{f}(\bar{x}) \wedge f_{\neq 0}(\bar{x}) \vee \neg f_{\neq 0}(\bar{x}) = 1$.
If $f(\bar{x}) = 0$, then $f_{\neq 0}(\bar{x}) = 0$, so
$\hat{f}(\bar{x}) \wedge f_{\neq 0}(\bar{x}) \vee \neg f_{\neq 0}(\bar{x}) = (\hat{f}(\bar{x}) \wedge 0) \vee 0 = 0$.

If $f(\bar{x}) = -1$, then for each $\bar{y}$ such that $f(\bar{y}) = 1$ we have $\rho_n(\bar{x}, \bar{y}) \geq |f(\bar{x}) - f(\bar{y})| = 2$ which implies that $1 - \rho_n(\bar{x}, \bar{y}) = -1$. Then $\hat{f}(\bar{x}) = -1$ and $f_{\neq 0}(\bar{x}) = 1$, so $\hat{f}(\bar{x}) \wedge f_{\neq 0}(\bar{x}) \vee \neg f_{\neq 0}(\bar{x}) = -1$.

Thus

$$f(\bar{x}) = \hat{f}(\bar{x}) \wedge f_{\neq 0}(\bar{x}) \vee \neg f_{\neq 0}(\bar{x}).$$

□

Lemma 3. *The set of all short functions from F is a precomplete class in F and is the functional closure of the set $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\}$, where $f_U \in F^{(0)}$, $f_\neg, f_\sim \in F^{(1)}$, $f_\vee, f_\wedge \in F^{(2)}$, $f_U = 0$, $f_\neg(x) = -x$, $f_\sim(x) = 1 - |x|$, $f_\vee(x, y) = \max(x, y)$, $f_\wedge(x, y) = \min(x, y)$.*

Proof. Denote by S the set of all short functions from F. In accordance with its definition, a short function from F can be alternatively characterized as a function $X^n \to X$ $(n \geq 0)$ which does not change sign on each of the sets $\prod_{i=1}^n \{0, a_i\}$, where $a_1, ..., a_n \in \{-1, 1\}^n$. In the terminology of [19], such functions correspond to the precomplete class $T^3_{\mathcal{E}_1,1}$ of functions for which the image of the product of sets, 1-equivalent to $\mathcal{E}_1$ is a subset of a set, 1-equivalent to $\mathcal{E}_1$, where two sets are 1-equivalent, if their symmetric difference has no more than 1 element. Thus S is a precomplete class in F. Obviously, $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\} \subseteq S$. On the other hand, since the constant function with value -1 is expressible as $f_\neg \circ f_\sim \circ f_U$, from Lemma 2 and the definition of $x^{[y]}$ it follows that each $f \in S$ can be expressed as a composition of elements of $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\}$ and of projections $\pi^n_k(x_1, ..., x_n) = x_k$ $(n \geq 1,\ k = 1, 2, ..., n)$. Thus S is the functional closure of $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\}$. □

Lemma 4. *The set of all short functions from F is the functional closure of the set $\{f_T, f_F, f_U, f_\neg, f_\wedge, f_\sim\}$, where $f_F, f_U, f_T \in F^{(0)}$, $f_\neg, f_\sim \in F^{(1)}$, $f_\wedge \in F^{(2)}$, $f_F = -1$, $f_U = 0$, $f_T = 1$, $f_\neg(x) = -x$, $f_\sim(x) = 1 - |x|$, $f_\wedge(x, y) = \min(x, y)$.*

Proof. From the equalities $f_\sim(0) = 1$, $f_\neg(f_\sim(0)) = -1$ and the De-Morgan law it follows that the set $\{f_T, f_F, f_U, f_\neg, f_\wedge, f_\sim\}$ has the same functional closure as the set $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\}$ (where $f_\vee(x, y) = \max(x, y)$), which is the set of all short functions from F by Lemma 3. □

Lemma 5. *For each $P, Q : D \xrightarrow{\sim} \{T, F\}$ and $d \in D$ we have:*

$$\Phi(\bot)(d) = 0$$
$$\Phi(\neg P)(d) = -(\Phi(P)(d))$$
$$\Phi(\sim P)(d) = 1 - |\Phi(P)(d)|$$
$$\Phi(P \vee Q)(d) = \max(\Phi(P)(d), \Phi(Q)(d))$$
$$\Phi(P \wedge Q)(d) = \min(\Phi(P)(d), \Phi(Q)(d))$$

Proof. Follows immediately from the definition Φ and operations $\neg, \sim, \vee, \wedge$ on partial predicates. □

Lemma 6. *The problem (1)–(2) has an optimal solution on $F^{(n)}$ if and only if p_0 is continuous in the initial topology on D induced by $p_1, ..., p_n$ (where the codomain of p_i, i.e. X, is considered as a discrete space).*

Proof. "If": assume that p_0 is continuous in the initial topology on D induced by $p_1, ..., p_n$. Then there exists $f \in F^{(n)}$ such that $p_0(d) = f(p_1(d), ..., p_n(d))$ for all $d \in D$. Then since the set $F^{(n)}$ is finite, the problem (1)–(2) has an optimal solution on $F^{(n)}$.

"Only if": assume that the problem (1)–(2) has an optimal solution $f \in F^{(n)}$. Then $p_0(d) = f(p_1(d), ..., p_n(d))$ for all $d \in D$, so p_0 is continuous in the initial topology on D induced by $p_1, ..., p_n$. □

Lemma 7. *If the problem (1)–(2) has an optimal solution on $F^{(n)}$, then this solution is unique.*

Proof. Assume that the problem (1)–(2) has optimal solutions $f, g \in F^{(n)}$. Then $||f|| = ||g||$ and $f(p_1(d), ..., p_n(d)) = p_0(d) = g(p_1(d), ..., p_n(d))$ for all $d \in D$.

Suppose that $f \neq g$. Then there exists $\bar{x}^* = (x_1^*, ..., x_n^*) \in X^n$ such that $f(\bar{x}^*) \neq g(\bar{x}^*)$.

Consider the case when $f(\bar{x}^*) \neq 0$. Let us define a function $h \in F^{(n)}$ as follows: $h(\bar{x}) = f(\bar{x})$, if $\bar{x} \neq \bar{x}^*$, and $h(\bar{x}) = 0$, if $\bar{x} = \bar{x}^*$. Then for all $d \in D$, $(p_1(d), ..., p_n(d)) \neq \bar{x}^*$, so $h(p_1(d), ..., p_n(d)) = p_0(d)$. Moreover, $||h|| = ||f|| - |f(\bar{x}^*)| = ||f|| - 1 < ||f||$ which contradicts the assumption that f is an optimal solution of (1)–(2).

Consider the case when $f(\bar{x}^*) = 0$. Then $|g(\bar{x}^*)| = 1$. Let us define a function $h \in F^{(n)}$ as follows: $h(\bar{x}) = g(\bar{x})$, if $\bar{x} \neq \bar{x}^*$, and $h(\bar{x}) = 0$, if $\bar{x} = \bar{x}^*$. Then for all $d \in D$, $(p_1(d), ..., p_n(d)) \neq \bar{x}^*$, so $h(p_1(d), ..., p_n(d)) = p_0(d)$. Moreover, $||h|| = ||g|| - |g(\bar{x}^*)| = ||g|| - 1 < ||g||$ which contradicts the assumption that g is an optimal solution of (1)–(2).

Thus $f = g$. So if the problem (1)–(2) has an optimal solution on $F^{(n)}$, then this solution is unique. □

Lemma 8. *Let $f \in M^{(n)}$, $g \in F^{(n)}$ and $g(\bar{x}) \in \{f(\bar{x}), 0\}$ for each $\bar{x} \in X^n$. Then $g \in M^{(n)}$.*

Proof. Let $\bar{x}, \bar{y} \in X^n$. Consider the following cases.

(1) $g(\bar{x}) = f(\bar{x}), g(\bar{y}) = f(\bar{y})$. Then $|g(\bar{x}) - g(\bar{y})| = |f(\bar{x}) - f(\bar{y})| \leq \rho(\bar{x}, \bar{y})$.
(2) $g(\bar{x}) = f(\bar{x}), g(\bar{y}) = 0$. Then $|g(\bar{x}) - g(\bar{y})| = |f(\bar{x})| \leq \rho(\bar{x}, \bar{y})$, if $\bar{x} \neq \bar{y}$, and $|g(\bar{x}) - g(\bar{y})| = 0 \leq \rho(\bar{x}, \bar{y})$, if $\bar{x} = \bar{y}$.
(3) $g(\bar{x}) = 0, g(\bar{y}) = f(\bar{y})$. Then $|g(\bar{x}) - g(\bar{y})| = |f(\bar{y})| \leq \rho(\bar{x}, \bar{y})$, if $\bar{x} \neq \bar{y}$, and $|g(\bar{x}) - g(\bar{y})| = 0 \leq \rho(\bar{x}, \bar{y})$, if $\bar{x} = \bar{y}$.
(4) $g(\bar{x}) = 0$, $g(\bar{y}) = 0$. Then $|g(\bar{x}) - g(\bar{y})| \leq \rho(\bar{x}, \bar{y})$.

Thus $g \in M^{(n)}$. □

Lemma 9. *The problem (1)–(2) has an optimal solution on $M^{(n)}$ if and only if it has an optimal solution on $F^{(n)}$ which belongs to $M^{(n)}$.*

Proof. "If": assume that the problem (1)–(2) has an optimal solution $f \in F^{(n)}$ which belongs to $M^{(n)}$. Then $f(p_1(d), p_2(d), ..., p_n(d)) = p_0(d)$ for all $d \in D$.

Moreover, for each $g \in M^{(n)}$ such that $g(p_1(d), p_2(d), ..., p_n(d)) = p_0(d)$ for all $d \in D$, we have $g \in F^{(n)}$, so $||f|| \leq ||g||$. So f is an optimal solution of (1)–(2) on $M^{(n)}$.

"Only if": assume that the problem (1)–(2) has an optimal solution f on $M^{(n)}$. Then $f(p_1(d), p_2(d), ..., p_n(d)) = p_0(d)$ for all $d \in D$. Then since $F^{(n)}$ is finite, the problem (1)–(2) has an optimal solution on $F^{(n)}$. By Lemma 7, the problem (1)–(2) has a unique optimal solution of $F^{(n)}$. Denote it as g. Then $g(p_1(d), p_2(d), ..., p_n(d)) = p_0(d)$ for all $d \in D$ and $||g|| \leq ||f||$. Let us define a function $h \in F^{(n)}$ as follows: for each $\bar{x} \in X^n$, $h(\bar{x}) = f(\bar{x})$, if $g(\bar{x}) \neq 0$, and $h(\bar{x}) = g(\bar{x})$, if $g(\bar{x}) = 0$. Then for all $d \in D$, $h(p_1(d), ..., p_n(d)) = p_0(d)$. Moreover, $h \in M^{(n)}$ by Lemma 8. Then $||h|| = ||f||$, so for each $\bar{x}$ such that $g(\bar{x}) = 0$ we have $f(\bar{x}) = 0$. Then $||f|| \leq ||g||$. Since $||g|| \leq ||f||$ as mentioned above, we have $||f|| = ||g||$. The f is an optimal solution of (1)–(2) on $F^{(n)}$ and f belongs to $M^{(n)}$. □

Now we can give a proof of Theorem 1.

Proof (of Theorem 1). "If": assume that the problem (1)–(2) has an optimal solution on the set $F^{(n)}$ which is a short function. Denote by f such a solution. Then we have $p_0(d) = f(p_1(d), p_2(d), ..., p_n(d))$ for all $d \in D$. By Lemma 3, f belongs to the functional closure of $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\}$, where the functions $f_.$ are defined as in Lemma 3. From Lemma 5 it follows that $p_0(d) = \Phi(P)(d)$ for all $d \in D$ for some predicate $P : D \tilde{\to} \{T, F\}$ expressible in the algebra $(D \tilde{\to} \{T, F\}; \vee, \wedge, \neg, \sim, \bot, P_1, P_2, ..., P_n)$. Since $n \geq 1$ and the predicate $\bot$ can be expressed as $\sim P_1 \wedge \sim\sim P_1$, we conclude that P is expressible in the algebra $APr_{P_1,...,P_n}(D)$. Then $\Phi(P_0)(d) = \Phi(P)(d)$ for all $d \in D$. Then the definition of Φ implies that $P_0 = P$, so P_0 is expressible in $APr_{P_1,...,P_n}(D)$.

"Only if": assume that a predicate P_0 is expressible in algebra $APr_{P_1,...,P_n}(D)$. Then Lemma 5 implies that $\Phi(P_0)(d) = f(\Phi(P_1)(d), \Phi(P_2)(d), ..., \Phi(P_n)(d))$ for all $d \in D$ for some function $f \in F^{(n)}$ which belongs to the functional closure of $\{f_U, f_\neg, f_\sim, f_\vee, f_\wedge\}$, where the functions $f_.$ are defined as in Lemma 3. Then by Lemma 3, f is a short function and $p_0(d) = f(p_1(d), ..., p_n(d))$ for all $d \in D$. Then since $M^{(n)} \subseteq F^{(n)}$ is a finite set, the problem (1)–(2) has an optimal solution on the set $M^{(n)}$. Then Lemma 9 implies that the problem (1)–(2) has an optimal solution on $F^{(n)}$ which is a short function. □

Note that the problem (1)–(2) has the following addition property.

Lemma 10. *If the problem (1)–(2) has an optimal solution on $M^{(n)}$, then this solution is unique.*

Proof. Assume that f, g are optimal solutions of (1)–(2) on $M^{(n)}$. Then by Lemma 9, (1)–(2) has an optimal solution on $F^{(n)}$ which belongs to $M^{(n)}$. By Lemma 7 this solution is unique. Denote it as h. Then $||h|| \leq ||f||$ and $||h|| \leq ||g||$. Then h is an optimal solution of (1)–(2) on $M^{(n)}$ and $||h|| = ||f|| = ||g||$. Then f, g are optimal solutions of (1)–(2) on $F^{(n)}$. Then by Lemma 7, $f = g$. □

6 Proof of Theorem 3

First, let us prove auxiliary lemmas.

Lemma 11. *Let V and $W \neq \emptyset$ be sets, $Q \in QPr_W^V$, and $v \in V$. Then*

$$\sim (\exists v\ Q) = (\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee \neg Q)).$$

Proof. Let us fix $d \in V \tilde{\to} W$ and consider the following cases.

1. Assume that $(\sim (\exists vQ))(d) \downarrow = T$. Then $(\exists vQ)(d) \uparrow$, so there exists $a \in W$ such that $Q(d\nabla^v a) \uparrow$ and there is no $b \in W$ such that $Q(d\nabla^v b) \downarrow = T$. Then $(\sim Q)(d\nabla^v a) \downarrow = T$, so $(\exists v(\sim Q))(d) \downarrow = T$. Moreover, for each $b \in W$, either $Q(d\nabla^v b) \uparrow$, or $Q(d\nabla^v b) \downarrow = F$, so either $(\sim Q)(d\nabla^v b) \downarrow = T$, or $(\neg Q)(d\nabla^v b) \downarrow = T$, whence $(\sim Q \vee \neg Q)(d\nabla^v b) \downarrow = T$. Hence $(\forall v(\sim Q \vee \neg Q))(d) \downarrow = T$. Thus $((\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee \neg Q)))(d) \downarrow = T$.
2. Assume that $(\sim (\exists vQ))(d) \uparrow$. Then $(\exists vQ)(d) \downarrow$. Then either there exists $a \in W$ such that $Q(d\nabla^v a) \downarrow = T$, or $Q(d\nabla^v b) \downarrow = F$ for all $b \in W$.
   2.1. Consider the case when there exists $a \in W$ such that $Q(d\nabla^v a) \downarrow = T$. Then $(\sim Q)(d\nabla^v a) \uparrow$ and $(\sim Q \vee \neg Q)(d\nabla^u a) \uparrow$. Note that $(\sim Q \vee \neg Q)(d\nabla^u b)$ is not false for any $b \in W$, since $(\sim Q)(d\nabla^u b)$ cannot be false. Then $(\forall v(\sim Q \vee \neg Q))(d) \uparrow$. Besides, $(\exists v(\sim Q))(d)$ is not false, since $(\sim Q)(d\nabla^v a) \uparrow$. Then $((\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee \neg Q)))(d) \uparrow$.
   2.2. Consider the case when $Q(d\nabla^v b) \downarrow = F$ for all $b \in W$. Then $(\exists v(\sim Q))(d) \uparrow$ (since $W \neq \emptyset$). Moreover, $(\sim Q \vee \neg Q)(d\nabla^u b) \downarrow = T$ for all $b \in W$. Then $(\forall v(\sim Q \vee \neg Q))(d) \downarrow = T$. Hence $((\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee \neg Q)))(d) \uparrow$.

Since $(\sim (\exists vQ))(d)$ cannot be false for any d, we conclude that $(\sim (\exists vQ))(d) \cong ((\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee \neg Q)))(d)$ for all $d \in V \tilde{\to} W$.
Thus $\sim (\exists vQ) = (\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee \neg Q))$. □

Corollary 1. *Let V and $W \neq \emptyset$ be sets, $Q \in QPr_W^V$, $u, v \in V$, $u \neq v$, and u is unessential for Q. Then $\sim (\exists v\ Q) = \forall u \exists v(\sim Q \wedge (\sim R_v^u(Q) \vee \neg R_v^u(Q)))$.*

The proof follows immediately from Lemma 11 by renaming the right-most bound variable v to u.

Lemma 12. *Let V and $W \neq \emptyset$ be sets, $Q \in QPr_W^V$, and $v \in V$. Then*

$$\sim (\forall v\ Q) = (\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee Q)).$$

Proof. By taking into account Lemma 11 and that $\forall v\ Q = \neg \exists v(\neg Q)$, $\neg\neg Q = Q$, and $\sim (\neg Q) = \ \sim Q$, we have:

$$\sim (\forall v\ Q) = \sim (\neg \exists v\ (\neg Q)) = \sim (\exists v\ (\neg Q))$$

$$= (\exists v(\sim (\neg Q))) \wedge (\forall v(\sim (\neg Q) \vee \neg\neg Q)) = (\exists v(\sim Q)) \wedge (\forall v(\sim Q \vee Q)).$$

□

Corollary 2. *Let V and $W \neq \emptyset$ be sets, $Q \in QPr_W^V$, $u, v \in V$, $u \neq v$, and u is unessential for Q. Then* $\sim (\forall v\ Q) = \forall u \exists v (\sim Q \wedge (\sim R_v^u(Q) \vee R_v^u(Q)))$.

The proof follows immediately from Lemma 12 by renaming the right-most bound variable v to u.

Proof (Of Theorem 3). "If": By Theorem 2, P is expressible in the algebra $APr_{P_1,...,P_l}(V \tilde{\to} W)$, where $P_j = R_{\bar{v}_j}^{\bar{u}_j}(Q_{n_j})$ for $j = 1, 2, ..., l$. Then it is easy to see that $\mathfrak{Q}_{m,\bar{v}}^k(P)$ is expressible in $AQPr_{Q_1,...,Q_n}(V, W)$. Thus Q_0 is expressible in $AQPr_{Q_1,...,Q_n}(V, W)$.

"Only if": Assume that Q_0 is expressible in the algebra $AQPr_{Q_1,...,Q_n}(V, W)$. From Corollary 1 and Corollary 2 given above, and elementary properties of $\neg$, $\vee$, $\wedge$, $\exists u$, $\forall u$ and renomination [20], it is easy to see (by using a process analogous to the process of construction of the prenex normal form in the classical first-order logic) that there exists a predicate P expressible in $ARPr_{Q_1,...,Q_n}(V, W)$ such that $Q_0 = \mathfrak{Q}_{m,\bar{v}}^k(P)$ for some integers $k \geq 0$, $m \in [0, 2^k - 1]$ and a tuple $\bar{v} \in V^k$. Since renomination distributes with $\vee$, $\wedge$, $\neg$, and $\sim$ [20] (e.g. $R_{\bar{v}}^{\bar{u}}(P_1 \vee P_2) = R_{\bar{v}}^{\bar{u}}(P_1) \vee R_{\bar{v}}^{\bar{u}}(P_2)$), and the composition of renominations is again a renomination (i.e. $R_{\bar{v}}^{\bar{u}}(R_{\bar{v}'}^{\bar{u}'}(P))$ is equal to $R_{\bar{v}''}^{\bar{u}''}(P)$ for some $\bar{u}'', \bar{v}''$), there exists an integer $l \geq 1$, finite sequences of integers $k_j \geq 1$ and $n_j \in [1, n]$ for $j = 1, 2, ..., l$, and finite sequences of tuples $\bar{u}_j \in V_{\neq}^{k_j}$, $\bar{v}_j \in V^{k_j}$ for $j = 1, 2, ..., l$ such that P is expressible in $APr_{Q^1,...,Q^l}(V \tilde{\to} W)$, where $Q^j = R_{\bar{v}_j}^{\bar{u}_j}(Q_{n_j})$ for $j = 1, 2, ..., l$. Then by Theorem 2, P is short w.r.t. $R_{\bar{v}_j}^{\bar{u}_j}(Q_{n_j})$ for $j = 1, 2, ..., l$. □

7 Conclusion

We have investigated the expressibility of partial predicates in the Kleene algebra with predicate complement and have given a necessary and sufficient condition of this expressibility in terms of the existence of an optimal solution of an optimization problem. We have also investigated expressibility in the first-order Kleene algebra with predicate complement. The obtained results may be useful for software verification using an extension of the Floyd-Hoare logic for partial pre- and postconditions and "weak triple" interpretation.

References

1. Wiik, J., Boström, P.: Contract-based verification of MATLAB and simulink matrix-manipulating code. In: Merz, S., Pang, J. (eds.) ICFEM 2014. LNCS, vol. 8829, pp. 396–412. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11737-9_26
2. Floyd, R.: Assigning meanings to programs. Math. Aspects Comput. Sci. **19**, 19–32 (1967)
3. Hoare, C.: An axiomatic basis for computer programming. Commun. ACM **12**(10), 576–580 (1969)

4. Ivanov, I., Korniłowicz, A., Nikitchenko, M.: Implementation of the composition-nominative approach to program formalization in Mizar. Comput. Sci. J. Moldova **26**, 59–76 (2018)
5. Ivanov, I., Korniłowicz, A., Nikitchenko, M.: Formalization of nominative data in Mizar. In: Proceedings of TAAPSD 2015, 23–26 December 2015, pp. 82–85. Taras Shevchenko National University of Kyiv, Ukraine (2015)
6. Ivanov, I.: An abstract block formalism for engineering systems. In: Ermolayev, V., et al. (eds.) Proceedings of the 9th International Conference on ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer, Kherson, Ukraine, June 19–22, 2013. CEUR Workshop Proceedings, vol. 1000, pp. 448–463. CEUR-WS.org (2013)
7. Ivanov, I.: On existence of total input-output pairs of abstract time systems. In: Ermolayev, V., Mayr, H.C., Nikitchenko, M., Spivakovsky, A., Zholtkevych, G. (eds.) ICTERI 2013. CCIS, vol. 412, pp. 308–331. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03998-5_16
8. Ivanov, I.: On representations of abstract systems with partial inputs and outputs. In: Gopal, T.V., Agrawal, M., Li, A., Cooper, S.B. (eds.) TAMC 2014. LNCS, vol. 8402, pp. 104–123. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-06089-7_8
9. Ivanov, I., Nikitchenko, M.: Inference rules for the partial floyd-hoare logic based on composition of predicate complement. In: Ermolayev, V., Suárez-Figueroa, M.C., Yakovyna, V., Mayr, H.C., Nikitchenko, M., Spivakovsky, A. (eds.) ICTERI 2018. CCIS, vol. 1007, pp. 71–88. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-13929-2_4
10. Korniłowicz, A., Ivanov, I., Nikitchenko, M.: Kleene algebra of partial predicates. Formalized Math. **26**, 11–20 (2018)
11. Korniłowicz, A., Kryvolap, A., Nikitchenko, M., Ivanov, I.: An approach to formalization of an extension of Floyd-Hoare logic. In: Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017, pp. 504–523 (2017)
12. Kornilowicz, A., Kryvolap, A., Nikitchenko, M., Ivanov, I.: Formalization of the algebra of nominative data in Mizar. In: Ganzha, M., Maciaszek, L.A., Paprzycki, M. (eds.) Proceedings of the 2017 Federated Conference on Computer Science and Information Systems. ACSIS, vol. 11, pp. 237–244 (2017)
13. Korniłowicz, A., Kryvolap, A., Nikitchenko, M., Ivanov, I.: Formalization of the nominative algorithmic algebra in Mizar. In: Świątek, J., Borzemski, L., Wilimowska, Z. (eds.) ISAT 2017. AISC, vol. 656, pp. 176–186. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-67229-8_16
14. Kryvolap, A., Nikitchenko, M., Schreiner, W.: Extending floyd-hoare logic for partial pre- and postconditions. In: Ermolayev, V., Mayr, H.C., Nikitchenko, M., Spivakovsky, A., Zholtkevych, G. (eds.) ICTERI 2013. CCIS, vol. 412, pp. 355–378. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03998-5_18
15. Nikitchenko, M., Kryvolap, A.: Properties of inference systems for Floyd-Hoare logic with partial predicates. Acta Electrotechnica et Informatica **13**(4), 70–78 (2013)
16. Nikitchenko, M., Ivanov, I., Korniłowicz, A., Kryvolap, A.: Extended floyd-hoare logic over relational nominative data. In: Bassiliades, N., et al. (eds.) ICTERI 2017. CCIS, vol. 826, pp. 41–64. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76168-8_3

17. Nikitchenko, N.S.: A composition nominative approach to program semantics. Technical report, IT-TR 1998–020, Technical University of Denmark (1998)
18. Skobelev, V., Nikitchenko, M., Ivanov, I.: On algebraic properties of nominative data and functions. In: Ermolayev, V., Mayr, H., Nikitchenko, M., Spivakovsky, A., Zholtkevych, G. (eds.) ICTERI 2014. CCIS, vol. 469, pp. 117–138. Springer, Cham (2014)
19. Yablonskii, S.: Functional constructions in a k-valued logic. Trudy Mat. Inst. Steklov. **51**, 5–142 (1958)
20. Nikitchenko, M., Shkilniak, O., Shkilniak, S., Mamedov, T.: Completeness of the logic of partial quasiary predicates with the complement composition. In: Proceedings of the Conference on Mathematical Foundations of Informatics MFOI 2019, July 3–6, 2019, Iasi, Romania (2019)