Introduction

“Stringly typed” is a new antipattern referring to an implementation that needlessly relies on strings, when other options are available. The problem of “string typing” appears often in service-oriented architecture and microservices on the border between a service and its clients (external interfaces) due to necessity to communicate over text-based protocols (like HTTP) and collaboration with clients written in dynamically-typed languages (like JavaScript). The solution to this problem can be found with refinement types, which are used to statically (or dynamically) check compatibility of a given value and refined type by means of predicates constraining the set of possible values. Though employment of numerical refinements is well-known in programming languages, string refinements are still rare.

In this paper, we introduce a design for extending the Jolie programming language [24,3] and its type system. On top of previous extensions with choice type [27] and regular expressions, we introduce here string refinement type and we motivate the reasons for such extension. Section 2 recalls the basic of the Jolie language and its type system while Section 3 describes the open problem this paper attacks with clarifying examples. Section 4 discusses related work in the context of using SMT solvers for static typing of refinement types.

Jolie programming language

Jolie [24] is the first programming language based on the paradigm of microservices [17]: all components are autonomous services that can be deployed independently and operate by running parallel processes, programmed following the workflow approach. Microservices can be composed to obtain, in turn, other microservices. The language was originally developed in the context of a major formalization effort for workflow and services composition languages, the EU Project SENSORIA [1], which spawned many models for reasoning on the composition of services (e.g., [19,20]). Jolie comes with a formally-specified semantics [16,15,23]; on the more practical side it is inspired by standards for Service-oriented Computing such as WS-BPEL [4]. The combination of theoretical and practical aspects in Jolie enabled its usage in research on correct-by-construction software (see, e.g., [26,9,21]).

Microservices work together by exchanging messages. In Jolie, messages are structured as trees [23] (a variant of the structures that can be found in XML or JSON). Communications are type checked at runtime, when messages are sent or received. Type checking of incoming messages is especially relevant, since it mitigates the effect of ill-behaved clients. The work in [25] presents a first attempt at formalizing a static type checker for the core fragment of Jolie. However, for the time being, the language is still dynamically type checked.

Extension of Jolie Type System

Safina et al [28] extended the basic type system of Jolie with type choices. The work had been then continued with the addition of regular expression types, a special case...
of refinement types. In refinement types, types are decorated with logical predicates which further constrain the set of values described by the type and therefore represent the specification of invariant on values. Here, we extend this with the possibility of expressing invariants on string values in form of regular expressions. The integration of static and dynamic analysis allows considering “internal” services (native Jolie services) and calls from “external” services (potentially developed in other languages) in a complementary way. The first ones can be statically checked while the second ones, which could exhibit malicious behavior, still need a runtime validation.

The key idea behind service-oriented computing, and microservices in particular, is the ability to connect services developed in different programming languages and possibly running on different servers over standard communication protocols [18]. A common use case is the implementation of APIs for Web and mobile applications. In such scenarios, the de-facto standard communication protocol is HTTP(S), combined with standardized data formats (SOAP, JSON, etc.). HTTP is a text-based protocol, where all data get serialized into strings. Moreover, clients of a service (an application or another service) may have been developed in a language that does not support particular datatypes (e.g., JavaScript does not have a datatype for calendar dates or time of day), therefore relying on string representation for internal processing too. The same issue arises with key-value storage systems (e.g., Memcache and Redis), which support only string keys and string values. These factors make string handling an important part of a service application, especially at the boundary with external systems.

Not all strings are made equal. For example, GUIDs are often used to identify records in a store. GUIDs are represented as strings of hexadecimal digits with a particular structure. Currently, developers have to manually check the conformance of received values to the expected format. In such a scenario, a developer has to find her way in a narrow stream between the Scylla of forgetting to insert necessary checks and the Charybdis of inserting too many checks for data that has been already validated.

Description of the shape of expected string data (like GUID or e-mail address) is natural with regular expressions. Adding the description of this shape to the datatype definition allows the compiler to automatically insert the necessary dynamic checks (for public functions) and statically validate the conformance (for internal calls). This is the extension of refinement type to string type. The same techniques and tools used for static verification of conformance for numerical refinements [17, 12] can be used for strings. For the purposes of this paper we will use Z3 SMT solver by Microsoft Research [6], which recently got support for theory of strings and regular expressions in its development branch.

1 Jolie partially mitigates this aspect with automatic conversion of string serializations to structured data by following the interface definition of the service [23]. However, this does not solve the general problem addressed here.

2 Scylla and Charybdis are monsters of Greek mythology living on the two sides of a narrow channel so that sailors trying to avoid one would have fallen into the other.

3 Please note that in Jolie we structure the variable’s data as a tree, where the nodes contain values. Using the void type for the variable on the top of the tree, we show that it contains no data and is used as a container for its subtypes.
Introducing string refinement allows Jolie to have both dynamic and static checking for strings. In case of dynamic checking, the string is verified at runtime when passed to the receiving service. The more interesting case is static checking by means of SMT. Here we present the most essential parts of the encoding, complete example can be found in [2].

Type checking is based on proving a theorem stating that a function is correctly typed. Technically, the opposite proposition is actually stated and the SMT solver is put in charge of finding a counterexample. A failure in such an attempt leads to the conclusion that the original theorem has to be true (proof by contradiction). The Z3 solver successfully proves the well-typedness theorem for the correct implementation of all posts by user, and fails to disprove the incorrect implementation (all_posts_by_user2) due to many simplifications to the presented SMT encoding for the sake of clarity and understandability. Employment of a more sophisticated encoding for the actual implementation of refinement constraints may mitigate this situation and is left as future work.
4. Related Work

Within the context of functional languages, type-checking of refined types by employing SMT solvers is not new. In [7], the authors present the design and implementation of the F7 enhanced type-checker for the functional language F# that verifies security properties of cryptographic protocols and access control mechanisms using Z3 [10]. The SAGE language [17] employs a hybrid approach [13] that performs both static and dynamic type-checking. During compilation time, the Simplify theorem prover [11] is used to check refinement types. If Simplify is not able to decide a particular subtyping relation, a proper type cast is inserted in the code and it is checked at runtime. If the type cast fails during runtime, this particular subtyping relation is inserted in a database of known failed casts. In contrast to checking syntactic subtyping as in F7 and SAGE, the authors of [8], introduce semantic subtyping checking for a subset of the M language [5] using the Z3 SMT solver.

5. Conclusions

The Jolie language is dynamically type-checked. This paper explores the possibility of integrated dynamic and static type checking with the introduction of refinement types, verified via an SMT solver. The integration of the two aspects allows a scenario where the static verification of internal services and the dynamic verification of (potentially malicious) external services cooperates in order to reduce testing effort and enhance security. In this work, we motivate the usefulness and feasibility of string refinement types using an example. Naturally, we need to integrate this extension with an actual type-checker employing a more advanced SMT-encoding. Not only for strings but for numerical types too which is well-known and useful tool for correctness enhancement. When we have a type-checker for refinement types, an interesting empirical study would be checking of existing programs augmented with refined types to discover whether this technique can uncover bugs caused by a developer’s oversight.

References


Refinement типы для языка Jolie

Аннотация. Jolie — язык программирования для разработки микросервисов и на текущий момент является динамически проверяемым. В статье рассматривается возможность объединить динамическую и статическую проверку типов с помощью refinement типов, проверяемых SMT-решателем. Соединение этих двух аспектов делает возможным сценарий, когда статическая верификация ускользает от традиционной системы типов. Предложенное расширение целесообразно, поскольку оно не пропускает программу с ошибкой. Полноценное решение потребует доработки в части точности проверки и качества сообщений об ошибках.