Safe Compositional Network Sketches: The Formal Framework

Azer Bestavros* best@cs.bu.edu
Assaf Kfoury* kfoury@cs.bu.edu
Andrei Lapets* lapets@cs.bu.edu
Michael Ocean† mocean@endicott.edu

October 30, 2009

Abstract

NetSketch is a tool for the specification of constrained-flow applications and the certification of desirable safety properties imposed thereon. NetSketch is conceived to assist system integrators in two types of activities: modeling and design. As a modeling tool, it enables the abstraction of an existing system while retaining sufficient information about it to carry out future analysis of safety properties. As a design tool, NetSketch enables the exploration of alternative safe designs as well as the identification of minimal requirements for outsourced subsystems. NetSketch embodies a lightweight formal verification philosophy, whereby the power (but not the heavy machinery) of a rigorous formalism is made accessible to users via a friendly interface. NetSketch does so by exposing tradeoffs between exactness of analysis and scalability, and by combining traditional whole-system analysis with a more flexible compositional analysis. The compositional analysis is based on a strongly-typed Domain-Specific Language (DSL) for describing and reasoning about constrained-flow networks at various levels of sketchiness along with invariants that need to be enforced thereupon. In this paper, we define the formal system underlying the operation of NetSketch, in particular the DSL behind NetSketch's user-interface when used in "sketch mode", and prove its soundness relative to appropriately-defined notions of validity. In a companion paper [6], we overview NetSketch, highlight its salient features, and illustrate how it could be used in two applications: the management/shaping of traffic flows in a vehicular network (as a proxy for CPS applications) and in a streaming media network (as a proxy for Internet applications).

1 Introduction

Constrained-Flow Networks: Many large-scale, safety-critical systems can be viewed as interconnections of subsystems, or modules, each of which is a producer, consumer, or regulator of *flows*. These flows are characterized by a set of variables and a set of constraints thereof, reflecting *inherent* or *assumed* properties or rules governing how the modules operate (and what constitutes safe operation). Our notion of flow encompasses streams of physical entities (*e.g.*, vehicles on a road, fluid in a pipe), data objects (*e.g.*, sensor network packets or video frames), or consumable resources (*e.g.*, electric energy or compute cycles).

Traditionally, the design and implementation of such *constrained-flow networks* follow a bottom-up approach, enabling system designers and builders to certify (assert and assess) desirable safety invariants of the system as a whole. While justifiable in some instances, this vertical approach does not lend itself well to current practices in the assembly of complex, large-scale systems – namely, the integration of various subsystems into a whole by "system integrators" who may not possess the requisite expertise or knowledge of the internals of the subsystems on which they rely. This can be viewed as an alternative *horizontal* approach, and it has significant merits with respect to scalability and modularity. However, it also poses significant challenges with respect to aspects of trustworthiness – namely, certifying that the system as a whole will satisfy specific safety invariants.

The NetSketch Tool: In recongnition of this challenge, we have developed NetSketch – a tool that assists system integrators in two types of activities: modeling and design.

This work is supported in part by NSF awards CNS-0952145, CCF-0820138, CSR-0720604, and EFRI-0735974.
*Computer Science Department, Boston University, Boston MA 02215.
†Computer Science Department, Endicott College, Beverly, MA 09195.

As a modeling tool, NetSketch enables the abstraction of an existing (flow network) system while retaining sufficient information about it to carry out future analysis of safety properties. The level of abstraction, or sketchiness (and hence the amount of information to be retained) is the result of two different processes that NetSketch offers to its users. The first process is the identification of boundaries of the subsystems to be sketched. At the extreme of finest granurality, these boundaries are precisely those of the interconnected modules that make up the system – *i.e.*, the constituent subsystems are the modules. At the other extreme, these boundaries would enclose the entire system. The second process is the control of the level of precision of information retained for the specification of a given subsystem, which are expressed as constraints defined over flow variables at the boundaries of that subsystem. By making conservative assumptions (*e.g.*, restricting the set of permissible inputs to a subsystem or extending the set of possible outputs from a subsystem), it is possible to reduce the complexity of these constraints.

As a design tool, NetSketch enables the exploration of alternative safe designs as well as the identification of minimal requirements for missing subsystems in partial designs. Alternative designs are the result of having multiple possible subsystem designs. NetSketch enables its users to check whether any (or which) one of their alternative designs is safe (thus allowing the exploration of "what if" scenarios and tradeoffs), or whether every one of a set of possible deployments would be safe (thus establishing the safety of a system design subject to uncertainties regarding various settings in which the system may be deployed). Partial designs are the result of missing (*e.g.*, outsourced, or yet-to-be acquired) subsystems. These missing subsystems constitute "holes" in the system design. NetSketch enables its users to infer the minimal requirements to be expected of (or to be imposed on) such holes. This enables the design of a system to proceed based only on promised functionality of missing parts thereof.

Formal analysis is at the heart of both of the above modeling and design activities. For example, in conjunction with a modeling activity in which the user identifies the boundaries of an interconnected set of modules that need to be encapsulated into a single subsystem, NetSketch must infer (through analysis) an appropriate set of constraints (*i.e.*, a typing) of that encapsulated subsystem. Similarly, in conjunction with a design activity in which the user specifies a subsystem as a set of alternative designs (or else as a hole), NetSketch must perform type checking (or type inference) to establish the safety of the design (or the minimal requirements to be expected of any subsystem that would fill the hole).

In a companion paper [6], we presented NetSketch from an operational perspective in support of modeling and design activities, by overviewing the processes it entails and by illustrating its use in two applications: the management/shaping of traffic flows in a vehicular network (as a proxy for CPS applications) and in a streaming media network (as a proxy for Internet applications). In this paper, we focus on the more fundamental aspects of NetSketch – namely the formal system underlying its operation.

The NetSketch Formalism: Support for safety analysis in design and/or development tools such as NetSketch must be based on sound formalisms that are not specific to (and do not require expertise in) particular domains.[1] Not only should such formalisms be domain-agnostic, but also they must act as a unifying glue across multiple theories and calculi, allowing system integrators to combine (compose) exact results obtained through esoteric domain-specific techniques (*e.g.*, using network calculus to obtain worst-case delay envelopes, using scheduling theory to derive upper bounds on resource utilizations, or using control theory to infer convergence-preserving settings). This sort of approach lowers the bar for the expertise required to take full advantage of such domain-specific results at the small (sub-system) scale, while at the same time enabling scalability of safety analysis at the large (system) scale.

As we alluded before, NetSketch enables the composition of exact analyses of small subsystems by adopting a constrained-flow network formalism that exposes the tradeoffs between exactness of analysis and scalability of analysis. This is done using a strongly-typed Domain-Specific Language (DSL) for describing and reasoning about constrained-flow networks at various levels of "sketchiness" along with invariants that need to be enforced thereupon. In this paper, we formally define NetSketch's DSL and prove its soundness relative to appropriately-defined notions of validity.

[1] While acceptable and perhaps expected for vertically-designed and smaller-scale (sub-)systems, deep domain expertise cannot be assumed for designers of horizontally-integrated, large-scale systems.

A Motivating Example: Before delving into precise definitions and formal arguments, we outline the essential concepts that constitute our formalism for compositional analysis of problems involving constrainted-flow networks. We do so by considering (at a very high level) an example flow network systems problem in which compositional analysis of properties plays a role. Our goal is to identify essential aspects of these systems that we will later model precisely, and motivate their inclusion within the formalism. This example is considered in more precise detail in Section 7, and is also examined more extensively in a companion paper [6].

A software engineer in charge of developing a CPS vehicular traffic control application for a large metropolitan authority is faced with the following problem. Her city lies on a river bank across from the suburbs, and every morning hundreds of thousands of motorists drive across only a few bridges to get to work in the city center. Each bridge has a fixed number of lanes, but they are all reversible, enabling the application to determine how many lanes are available to inbound and outbound traffic during different times of the day. During morning rush hour, the goal of the system is to maximize the amount of traffic that can get into the city, subject to an overriding safety consideration – that no backups occur in the city center.

Modules and Networks: The city street grid is a network of a large number of only a few distinct kinds of traffic junctions (*e.g.*, forks, merges, and crossing junctions). Because the network is composed of many instances of a few modular components, if any analysis of the network is desired, it may be possible to take advantage of this modularity by analyzing the components individually in a more precise manner, and then composing the results to analyze the entire network. To this end, as detailed in Sections 2 and 3, our formalism provides means for defining *modules* (small network components) and assembling them into larger *networks* (graphs).

Constraints: Within our framework, analyses are represented using a language of *constraints*. If the engineer views traffic as a flow across a network of modules, the relevant *parameters* describing this flow (*e.g.*, the number of open lanes, the density of traffic in the morning) can be mathematically constrained for each instance of a module. These constraints can model both the limitations of modules as well as the problem the engineer must solve. For example, a module corresponding to a merge junction may have two incoming lanes $1, 2$ and one outgoing lane 3, and the density of traffic travelling across the outgoing lane must be equivalent to the total traffic density travelling across the incoming lanes

$$d_1 + d_2 = d_3.$$

Likewise, constraints can model the problem to be solved. The engineer can find appropriate constraints for each of the three junction types that will ensure that no backups occur locally within that junction. For example, it may be the case for a junction that if the total density of entering traffic exceeds a “jam density” that makes the two entering traffics block each other, there will be backups. Thus, the engineer may choose to introduce a constraint such as

$$d_1 + d_2 \leqslant 10.$$

More complicated situations requiring the enforcement of additional desirable properties may introduce non-linear constraints. Once the local requirements are specified, a compositional analysis can answer interesting questions about the entire network, such as whether a configuration of lanes ensuring no backups is possible, or what the range of viable configurations may be.

Semantics and Soundness: So far, we have motivated the need for two intertwined languages: a language for describing networks composed of modules, and a language for describing constraints governing flows across the network components. But what precisely do the expressions in these languages mean, and how can we provide useful functionalities to the engineer, such as the ability to verify that constraints can be satisfied, to find solution ranges for these constraints, and to compose these analyses on modules to support analyses of entire networks? In order to ensure that our system works correctly “under the hood”, it is necessary to define a precise *semantics* for these languages, along with a rigorous notion of what it means for an analysis of a network to be “correct”. Only once these are defined is it possible to provide a guarantee that the system is indeed safe to use. To this end, we define a precise semantics for constraint sets and relationships between them, as well as network flows. The proof of soundness for our formalism is given in full in Section 8.

2 Modules: Untyped and Typed

We introduce several preliminary notions formally.

Definition 1 (*Syntax of Constraints*)**.** We denote by $\mathbb{N}$ the set of natural numbers. The countably infinite set of *parameters* is $\mathcal{X} = \{x_0, x_1, x_2, \ldots\}$. The set of *constraints over* $\mathbb{N}$ *and* $\mathcal{X}$ can be defined in extended BNF style, where we use metavariables n and x to range over $\mathbb{N}$ and $\mathcal{X}$, respectively:

$$
\begin{aligned}
e \in \textsc{Exp} \quad &::= \; n \mid x \mid e_1 * e_2 \mid e_1 + e_2 \mid e_1 - e_2 \mid \; \ldots \\
c \in \textsc{Const} \quad &::= \; e_1 = e_2 \mid e_1 < e_2 \mid e_1 \leqslant e_2 \mid \; \ldots
\end{aligned}
$$

We include in Const at least equalities and orderings of expressions. Our examination can be extended to more general constraints, indicated by the ellipses "…", but the preceding give us enough to consider and to present our main ideas on compositional analysis. Possible extensions of Const include conditional constraints, negated constraints, time-dependent constraints, and others.

A special case of the constraints are the *linear constraints*, obtained by restricting the rule for Exp and Const:

$$
\begin{aligned}
e \in \textsc{LinExp} \quad &::= \; n \mid x \mid n * x \mid e_1 + e_2 \\
c \in \textsc{LinConst} \quad &::= \; e_1 = e_2 \mid e_1 < e_2 \mid e_1 \leqslant e_2
\end{aligned}
$$

In what follows, constraints in Const are part of a *given* flow network abstraction and may be arbitrarily complex; constraints in LinConst are to be *inferred* and/or *checked* against the given constraints. Constraints in LinConst are hopefully simple enough so that their manipulation does not incur a prohibitive cost, but expressive enough so that their satisfaction guarantee desirable properties of the flow network under exmination. □

Depending on the application, the set $\mathcal{X}$ of parameters may be n-sorted for some finite $n \geqslant 1$. For example, in relation to vehicular traffic networks, we may choose $\mathcal{X}$ to be 2-sorted, one sort for *velocity parameters* and one sort for *density parameters*.

When there are several sorts, dimensionality restrictions must be heeded. For traffic networks with two sorts, the velocity dimension is *unit distance/unit time*, *e.g.*, *kilometer/hour*, and the density dimension is *unit mass/unit distance*, *e.g.*, *ton/kilometer*. Thus, multiplying a velocity v by a density d produces a quantity $v * d$, namely a *flow*, which is measured in *unit mass/unit time*, *e.g.*, *ton/hour*. If we add two expressions e_1 and e_2, or subtract them, or compare them, then e_1 and e_2 must have the same dimension, otherwise the resulting expression is meaningless.

In the abstract setting of our examination below we do not need to worry about such restrictions on expressions: they will be implicitly satisfied by our constraints if they correctly model the behavior of whatever networks are under consideration.

Definition 2 (*Untyped Modules*)**.** We specify an untyped module $\mathcal{A}$ by a four-tuple: $(\mathcal{A}, \mathsf{In}, \mathsf{Out}, \mathsf{Con})$ where:

$$
\begin{aligned}
\mathcal{A} \; &= \; \text{name of the module} \\
\mathsf{In} \; &= \; \text{finite set of input parameters} \\
\mathsf{Out} \; &= \; \text{finite set of output parameters} \\
\mathsf{Con} \; &= \; \text{finite set of constraints over } \mathbb{N} \text{ and } \mathcal{X}
\end{aligned}
$$

where $\mathsf{In} \cap \mathsf{Out} = \varnothing$ and $\mathsf{In} \cup \mathsf{Out} \; \subseteq \; \mathsf{parameters}(\mathsf{Con})$, where $\mathsf{parameters}(\mathsf{Con})$ is the set of parameters occurring in Con.

We are careful in adding the name of the module, $\mathcal{A}$, to its specification; in the formal setup of Section 3, we want to be able to refer to the module by its name without the overhead of the rest of its specification. By a slight abuse of notation, we may write informally: $\mathcal{A} \; = \; (\mathcal{A}, \mathsf{In}, \mathsf{Out}, \mathsf{Con})$. Thus, "$\mathcal{A}$" may refer to the full specification of the module or may be just its name.

We use upper-case calligraphic letters to refer to modules and networks – from the early alphabet ($\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$) for modules and from the middle alphabet ($\mathcal{M}, \mathcal{N}$ and $\mathcal{P}$) for networks. □

$$\textsc{Hole}\qquad \frac{(X, \mathsf{In}, \mathsf{Out}) \;\in\; \Gamma}{\Gamma \,\vdash\, (X, \mathsf{In}, \mathsf{Out}, \{\ \})}$$

$$\textsc{Module}\qquad \frac{(\mathcal{A}, \mathsf{In}, \mathsf{Out}, \mathsf{Con}) \ \ \text{module}}{\Gamma \,\vdash\, (\mathcal{B}, I, O, \{C\})} \qquad (\mathcal{B}, I, O, C) = \ '(\mathcal{A}, \mathsf{In}, \mathsf{Out}, \mathsf{Con})$$

$$\textsc{Connect}\qquad \frac{\Gamma \,\vdash\, (\mathcal{M}, I_1, O_1, \mathcal{C}_1) \qquad \Gamma \,\vdash\, (\mathcal{N}, I_2, O_2, \mathcal{C}_2)}{\Gamma \,\vdash\, (\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}), I, O, \mathcal{C})} \quad \begin{array}{l} \theta \subseteq_{\text{1-1}} O_1 \times I_2,\ I = I_1 \cup (I_2 - \mathsf{range}(\theta)),\ O = (O_1 - \mathsf{domain}(\theta)) \cup O_2, \\ \qquad \mathcal{C} = \{C_1 \cup C_2 \cup \{\, p = q \mid (p, q) \in \theta \,\} \mid C_1 \in \mathcal{C}_1, C_2 \in \mathcal{C}_2\} \end{array}$$

$$\textsc{Loop}\qquad \frac{\Gamma \,\vdash\, (\mathcal{M}, I_1, O_1, \mathcal{C}_1)}{\Gamma \,\vdash\, (\mathbf{loop}(\theta, \mathcal{M}), I, O, \mathcal{C})} \qquad \begin{array}{l} \theta \subseteq_{\text{1-1}} O_1 \times I_1,\ I = I_1 - \mathsf{range}(\theta),\ O = O_1 - \mathsf{domain}(\theta), \\ \quad \mathcal{C} = \ \{C_1 \cup \{\, p = q \mid (p, q) \in \theta \,\} \mid C_1 \in \mathcal{C}_1\} \end{array}$$

$$\textsc{Let}\qquad \frac{\Gamma \,\vdash\, (\mathcal{M}_k, I_k, O_k, \mathcal{C}_k) \quad \text{for } 1 \leqslant k \leqslant n \qquad \Gamma \cup \{(X, \mathsf{In}, \mathsf{Out})\} \,\vdash\, (\mathcal{N}, I, O, \mathcal{C})}{\Gamma \,\vdash\, \big(\ \mathbf{let}\ X \in \{\mathcal{M}_1, \ldots, \mathcal{M}_n\}\ \mathbf{in}\ \mathcal{N}\ , I, O, \mathcal{C}'\ \big)}$$

$$\mathcal{C}' = \Big\{ C \cup \hat{C} \cup \{\, p = \varphi(p) \mid p \in I_k \,\} \cup \{\, p = \psi(p) \mid p \in O_k \,\} \Big|\, 1 \leqslant k \leqslant n,\ C \in \mathcal{C},\ \hat{C} \in \mathcal{C}_k,\ \varphi : I_k \to \mathsf{In},\ \psi : O_k \to \mathsf{Out} \Big\}$$

Figure 1: Rules for Untyped Network Sketches.

Definition 3 (*Typed Modules*)**.** Consider a module $\mathcal{A}$ as specified in Definition 2. A *typing judgment*, or a *typed specification*, or just a *typing*, for $\mathcal{A}$ is an expression of the form $(\mathcal{A} : \mathsf{Con}^*)$, where Con^* is a finite set of *linear* constraints over $\mathsf{In} \cup \mathsf{Out}$. As it stands, a typing judgment $(\mathcal{A} : \mathsf{Con}^*)$ may or may not be valid. The validity of judgments presumes a formal definition of the semantics of modules, which we introduce in Section 4.

To distinguish between a constraint in Con, which is arbitrarily complex, and a constraint in Con^*, which is always linear, we refer to the former as "given" or "internal" and to the latter as a "type". □

3 Network Sketches: Untyped

We define a specification language to assemble modules together, also allowing for the presence of network holes. This is a strongly-typed *d*omain-*s*pecific *l*anguage (DSL), which can be used in two modes, with and without the types inserted. Our presentation is in two parts, the first without types and the second with types. In this section, we present the first part, when our DSL is used to construct networks without types inserted. In Section 6, we re-define our DSL with types inserted. This two-part presentation allows us to precisely define the difference between "untyped specification" and "typed specification" of a flow network.

"Network holes" are place-holders. We later attach some attributes to network holes (they are not totally unspecified), in Definitions 6 and 13. We use X, Y, and Z, possibly decorated, to denote network holes.

An untyped network sketch is written as $(\mathcal{M}, I, O, \mathcal{C})$, where I and O are the sets of input and output parameters, and $\mathcal{C}$ is a finite set of finite constraint sets. $\mathcal{M}$ is *not* a name but an expression built up from: (1) module names, (2) hole names, and (3) the constructors **conn**, **loop** and **let-in**. Nevertheless, we may refer to such a sketch by just writing the expression $\mathcal{M}$, and by a slight abuse of notation we may also write: $\mathcal{M} = (\mathcal{M}, I, O, \mathcal{C})$. For such an untyped network $\mathcal{M}$, we define $\mathsf{In}(\mathcal{M})$ as I (the set of input parameters) and $\mathsf{Out}(\mathcal{M})$ as O (the set of output parameters).

Definition 4 (*Syntax of Raw Network Sketches*)**.** In extended BNF style:

$$
\begin{array}{lll}
\mathcal{A},\mathcal{B},\mathcal{C} & \in \textsc{ModuleNames} & \\
X,Y,Z & \in \textsc{HoleNames} & \\
\mathcal{M},\mathcal{N},\mathcal{P} & \in \textsc{RawSketches} \ ::= & \\
 & \quad \mathcal{A} & \\
 & \mid X & \\
 & \mid \textbf{conn}(\theta,\mathcal{M},\mathcal{N}) & \theta \subseteq_{\text{1-1}} \mathsf{Out}(\mathcal{M}) \times \mathsf{In}(\mathcal{N}) \\
 & \mid \textbf{loop}(\theta,\mathcal{M}) & \theta \subseteq_{\text{1-1}} \mathsf{Out}(\mathcal{M}) \times \mathsf{In}(\mathcal{M}) \\
 & \mid \textbf{let}\ X \in \{\mathcal{M}_1,\ldots,\mathcal{M}_n\}\ \textbf{in}\ \mathcal{N} & X \text{ occurs once in } \mathcal{N}
\end{array}
$$

We write $\theta \subseteq_{\text{1-1}} \mathsf{Out}(\mathcal{M}) \times \mathsf{In}(\mathcal{N})$ to denote a partial one-one map from $\mathsf{Out}(\mathcal{M})$ to $\mathsf{In}(\mathcal{N})$. (If the set of parameters is sorted with more than one sort – for example, *velocity* and *density* – then θ must respect sorts, *i.e.*, if $(x, y) \in \theta$ then x and y are either both velocity parameters or both density parameters.)

The formal expressions written according to the preceding BNF are said to be "raw" because they do not specify how the internal constraints of a network sketch are assembled together from those of its subcomponents. This is what the rules in Figure 1 do precisely.

In an expression "**let** $X \in \{\mathcal{M}_1,\ldots,\mathcal{M}_n\}$ **in** $\mathcal{N}$", we call "$X \in \{\mathcal{M}_1,\ldots,\mathcal{M}_n\}$" a *binding* for the hole X and "$\mathcal{N}$" the *scope* of this binding. Informally, the idea is that all of the network sketches in $\{\mathcal{M}_1,\ldots,\mathcal{M}_n\}$ can be interchangeably placed in the hole X, depending on changing conditions of operation in the network as a whole. If a hole X occurs in a network sketch $\mathcal{M}$ outside the scope of any **let**-binding, we say X is *free* in $\mathcal{M}$. If there are no free occurrences of holes in $\mathcal{M}$, we say that $\mathcal{M}$ is *closed*.

Note carefully that $\mathcal{M},\mathcal{N}$ and $\mathcal{P}$ are *metavariables*, ranging over expressions in RawSketches; they do not appear as formal symbols in such expressions written in full. By contrast, $\mathcal{A},\mathcal{B}$ and $\mathcal{C}$ are *names* of modules and can occur as formal symbols in expressions of RawSketches. $\mathcal{A},\mathcal{B}$ and $\mathcal{C}$ are like names of "prim ops" in well-formed phrases of a programming language. □

In the examination to follow, we want each occurrence of the same module or the same hole in a specification to have its own private set of names, which we achieve using isomorphic renaming.

Definition 5 (*Fresh Isomorphic Renaming*)**.** Let A be an object defined over parameters. Typically, A is a module or a network sketch. Suppose the parameters in A are called $\{x_1, x_2, \ldots\}$. We write $'A$ to denote the same object A, whose name is also $'A$ and with all parameter names freshly renamed to $\{'x_1, 'x_2, \ldots\}$. We want these new names to be fresh, *i.e.*, nowhere else used and private to $'A$. Thus, A and $'A$ are isomorphic but distinct objects.

Sometimes we need two or more isomorphic copies of A in the same context. We may therefore consider $'A$ and $''A$. If there are more than two copies, it is more convenient to write ^1A, ^2A, ^3A, etc.

We also need to stipulate that, given any of the isomorphic copies of object A, say ^nA, we can retrieve the original A, along with all of its original names, from ^nA. □

There are other useful constructs in the DSL of Definition 4. But these will be either special cases of the basic three constructs – **conn**, **loop**, and **let-in** – or macros which can be "de-sugared" into expressions only involving the basic three. One important macro is the **let-in** construct where the hole occurs several times in the scope, instead of just once:

$$\textbf{let}^*\ X \in \{\mathcal{M}_1,\ldots,\mathcal{M}_n\}\ \textbf{in}\ \mathcal{N} \qquad X \text{ occurs } q \geqslant 1 \text{ times in } \mathcal{N}$$

To analyze the preceding expression, using the typing rules in this section, we de-sugar in a particular way:

$$
\begin{array}{l}
\textbf{let}\ \ {}^1X \in \{{}^1\mathcal{M}_1,\ldots,{}^1\mathcal{M}_n\}\ \ \textbf{in} \\
\textbf{let}\ \ {}^2X \in \{{}^2\mathcal{M}_1,\ldots,{}^2\mathcal{M}_n\}\ \ \textbf{in} \\
\cdots \\
\textbf{let}\ \ {}^qX \in \{{}^q\mathcal{M}_1,\ldots,{}^q\mathcal{M}_n\}\ \ \textbf{in}\ \ \mathcal{N}[X^{(1)} := {}^1X,\ldots,X^{(q)} := {}^qX]
\end{array}
$$

where $X^{(1)}, \ldots, X^{(q)}$ denote the q occurrences of X in $\mathcal{N}$ (the superscripts are not part of the syntax, just bookkeeping notation for this explanation), ${}^1X, \ldots, {}^qX$ are fresh distinct hole names, and $\{{}^p\mathcal{M}_1, \ldots, {}^p\mathcal{M}_n\}$ is a fresh isomorphic copy of $\{\mathcal{M}_1, \ldots, \mathcal{M}_n\}$ for every $1 \leqslant p \leqslant q$.

Definition 6 (*Untyped Network Holes*)**.** An untyped network hole is a triple: $(X, \mathsf{In}, \mathsf{Out})$ where X is the name of the hole, In is a finite set of input parameters, and Out is a finite set of output parameters. As usual, for the sake of brevity we sometimes write: $X = (X, \mathsf{In}, \mathsf{Out})$. □

There are 5 inference rules: Module, Hole, Connect, Loop, and Let, one for each of the 5 cases in the BNF in Definition 4. These are shown in Figure 1.

The renaming in rule Module is to insure that each occurrence of the same module has its own private names of paramaters. In rule Hole we do not need to rename, because there will be exactly one occurrence of each hole, whether bound or free, each with its own private set of names.

Rule Connect takes two network sketches, $\mathcal{M}$ and $\mathcal{N}$, and returns a network sketch $\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N})$ where some of the output parameters in $\mathcal{M}$ are unified with some of the input parameters in $\mathcal{N}$, according to what θ prescribes.

Rule Loop takes one network sketch, $\mathcal{M}$, and returns a new network sketch $\mathbf{loop}(\theta, \mathcal{M})$ where some of the output parameters in $\mathcal{M}$ are identified with some of the input parameters in $\mathcal{M}$ according to θ.

Rule Let is a little more involved than the preceding rules. The complication is in the way we define the collection $\mathcal{C}'$ of constraint sets in the conclusion of the rule. Suppose $\mathcal{C}_k = \{C_{k,1}, C_{k,2}, \ldots, C_{k,s(k)}\}$, *i.e.*, the flow through $\mathcal{M}_k$ can be regulated according to $s(k)$ different constraint sets, for every $1 \leqslant k \leqslant n$. The definition of the new collection $\mathcal{C}'$ of constraint sets should be read as follows: For every $\mathcal{M}_k$, for every possible way to regulate the flow through $\mathcal{M}_k$ (*i.e.*, for every possible $r \in \{1, \ldots, s(k)\}$), for every way of placing network $\mathcal{M}_k$ in hole X (*i.e.*, every isomorphism (φ, ψ) from (I_k, O_k) to $(\mathsf{In}, \mathsf{Out})$), add the corresponding constraint set to the collection $\mathcal{C}'$.

In the side-condition of rule Let, the maps φ and ψ are isomorphisms. If parameters are multi-sorted, then φ and ψ must respect sorts, *i.e.*, if $\varphi(x) = y$ then both x and y must be of the same sort, *e.g.*, both velocity parameters, or both density parameters, etc., and similarly for ψ.

In particular applications, we may want the placing of $\mathcal{M}_k$ in hole X to be uniquely defined for every $1 \leqslant k \leqslant n$, rather than multiply-defined in as many ways as there are isomorphism pairs from (I_k, O_k) to $(\mathsf{In}, \mathsf{Out})$. For this, we may introduce structured parameters, *i.e.*, finite sequences of parameters, and also restrict the network hole X to have one (structured) input parameter and one (structured) output parameter. This requires the introduction of selectors, which allow the retrieval of individual parameters from a sequence of parameters.

4 Semantics of Network Typings

A network typing, as later defined in Section 6, is specified by an expression of the form $(\mathcal{M}, I, O, \mathcal{C}) : C^*$ where $(\mathcal{M}, I, O, \mathcal{C})$ is an untyped network and C^* a finite set of linear constraints such that $\mathsf{parameters}(C^*) \subseteq I \cup O$.

Definition 7 (*Satisfaction of Constraints*)**.** Let $\mathcal{Y} \subseteq \mathcal{X}$, a subset of parameters. Let $\textsc{val}$ be a *valuation for* $\mathcal{Y}$, *i.e.*, $\textsc{val}$ is a map from $\mathcal{Y}$ to $\mathbb{N}$. Suppose all expressions and constraints are written over parameters in $\mathcal{Y}$. We use "$\models$" to denote the satisfaction relation.

The interpretation of an expression relative to $\textsc{val}$ is by induction on $e \in \textsc{Exp}$:

$$\textsc{val}(e) = \begin{cases} n & \text{if } e = n, \\ \textsc{val}(x) & \text{if } e = x \in \mathcal{Y}, \\ p & \text{if } e = e_1 * e_2 \ \&\ p = \textsc{val}(e_1) * \textsc{val}(e_2), \\ q & \text{if } e = e_1 + e_2 \ \&\ q = \textsc{val}(e_1) + \textsc{val}(e_2), \\ r & \text{if } e = e_1 - e_2 \ \&\ r = \textsc{val}(e_1) - \textsc{val}(e_2), \end{cases}$$

Satisfaction of a constraint by VAL is by cases of $c \in \text{CONST}$:

$$\begin{aligned}
\text{VAL} &\models e_1 = e_2 \quad \text{iff} \quad \text{VAL}(e_1) = \text{VAL}(e_2) \\
\text{VAL} &\models e_1 < e_2 \quad \text{iff} \quad \text{VAL}(e_1) < \text{VAL}(e_2) \\
\text{VAL} &\models e_1 \leqslant e_2 \quad \text{iff} \quad \text{VAL}(e_1) \leqslant \text{VAL}(e_2)
\end{aligned}$$

Satisfaction of a set of constraint relative to VAL:

$$\text{VAL} \models \{c_1, \ldots, c_p\} \quad \text{iff} \quad \text{VAL} \models c_1 \text{ and } \ldots \text{ and } \text{VAL} \models c_p$$

□

Definition 8 (*Closure of Constraint Sets*)**.** Let $\mathcal{Y} \subseteq \mathcal{X}$. Let C and C' be constraint sets over $\mathbb{N}$ and $\mathcal{Y}$. We say C *implies* C' just in case for every valuation $\text{VAL} : \mathcal{Y} \to \mathbb{N}$,

$$\text{VAL} \models C \quad \text{implies} \quad \text{VAL} \models C'.$$

If C implies C', we write $C \Rightarrow C'$. For a finite constraint set C, its *closure* is the set of all constraints implied by C, namely, $\mathsf{closure}(C) = \{c \in \text{CONST} \mid C \Rightarrow \{c\}\}$.

In general, $\mathsf{closure}(C)$ is an infinite set. We only consider infinite constraint sets that are the closures of finite sets of linear constraints. Following standard terminology, such an infinite constraint set is said to have a *finite basis*.[2] In actual applications, we are interested in "minimal" finite bases that do not contain "redundant" constraints. It is reasonable to define a "minimal finite basis" for a constraint set if it smallest in size. The problem is that minimal bases in this sense are not uniquely defined. How to compute minimal finite bases, and how to uniquely select a canonical one among them, are issues that are addressed by an implementation. □

Let C be a constraint set and A a set of parameters. We define two restrictions of C relative to A:

$$\begin{aligned}
C \upharpoonright A &= \{ c \in C \mid \mathsf{parameters}(c) \subseteq A \}, \\
C \downharpoonright A &= \{ c \in C \mid \mathsf{parameters}(c) \cap A \neq \varnothing \}.
\end{aligned}$$

That is, $(C \upharpoonright A)$ is the set of constraints in C where only parameters from A occur, and $(C \downharpoonright A)$ is the set of constraints in C with at least one occurrence of a parameter from A.

We introduce two different semantics, corresponding to what we call "weak satisfaction" and "strong satisfaction" of typing judgements. Both semantics are meaningful, corresponding to whether or not network nodes act as "autonomous systems", *i.e.*, whether or not each node coordinates its action with its neighbors or according to instructions from a network administrator.

Definition 9 (*Weak and Strong Satisfaction*)**.** Let $\mathcal{M} = (\mathcal{M}, I, O, \mathcal{C})$ be an untyped network sketch and $(\mathcal{M} : C^*)$ a typing for $\mathcal{M}$. Recall that $\mathsf{parameters}(C^*) \subseteq I \cup O$. We partition $\mathsf{closure}(C^*)$ into two subsets as follows:

$$\begin{aligned}
\mathsf{pre}(C^*) &= \mathsf{closure}(C^*) \upharpoonright I \\
\mathsf{post}(C^*) &= \mathsf{closure}(C^*) - \mathsf{pre}(C^*) = \mathsf{closure}(C^*) \downharpoonright O
\end{aligned}$$

The "$\mathsf{pre}(\ )$" is for "pre-conditions" and the "$\mathsf{post}(\ )$" is for "post-conditions". While the parameters of $\mathsf{pre}(C^*)$ are all in I, the parameters of $\mathsf{post}(C^*)$ are not necessarily all in O, because some constraints in C^* may contain both input and output parameters.[3]

The definitions of "weak satisfaction" and "strong satisfaction" below are very similar except that the first involves an *existential quantification* and the second a *universal quantification*. We use "$\models_{\text{w}}$" and "$\models_{\text{s}}$" to denote weak and strong satisfaction. For the rest of this definition, let VAL be a fixed valuation of the input parameters of $\mathcal{M}$, $\text{VAL} : I \to \mathbb{N}$.

We say VAL ***weakly satisfies*** the judgement $(\mathcal{M} : C^*)$ and write: $\text{VAL} \models_{\text{w}} (\mathcal{M} : C^*)$ to mean that if

[2] If we set up a logical system of inference for our linear constraints, using some kind of equational reasoning, then an infinite constraint set has a "finite basis" iff it is "finitely axiomatizable".

[3] Both $\mathsf{pre}(C^*)$ and $\mathsf{post}(C^*)$ are infinite sets. In the abstract setting of this report, this is not a problem. In an actual implementation, we need an efficient method for computing "minimal finite bases" for $\mathsf{pre}(C^*)$ and $\mathsf{post}(C^*)$, or devise an efficient algorithm to decide whether a constraint is in one of these sets.

- $\text{VAL} \models \mathsf{pre}(C^*)$

then for every $C \in \mathcal{C}$ ***there is a valuation*** $\text{VAL}' \supseteq \text{VAL}$ such that both of the following conditions are true:

- $\text{VAL}' \models C$
- $\text{VAL}' \models \mathsf{post}(C^*)$

Informally, VAL weakly satisfies $(\mathcal{M} : C^*)$ just in case, **if** VAL satisfies $\mathsf{pre}(C^*)$, **then** there is an extension VAL' of VAL satisfying the internal constraints of $\mathcal{M}$ **and** $\mathsf{post}(C^*)$.

We say VAL ***strongly satisfies*** $(\mathcal{M} : C^*)$ and write: $\text{VAL} \models_{\text{s}} (\mathcal{M} : C^*)$ to mean that if

- $\text{VAL} \models \mathsf{pre}(C^*)$

then for every $C \in \mathcal{C}$ and ***every valuation*** $\text{VAL}' \supseteq \text{VAL}$, if

- $\text{VAL}' \models C$

then the following condition is true:

- $\text{VAL}' \models \mathsf{post}(C^*)$

Informally, VAL strongly satisfies $(\mathcal{M} : C^*)$ in case, **if** VAL satisfies $\mathsf{pre}(C^*)$ **and** VAL' is an extension of VAL satisfying the internal constraints of $\mathcal{M}$, **then** VAL' satisfies $\mathsf{post}(C^*)$. □

Definition 10 (*Weak and Strong Validity of Typings*)**.** Let $(\mathcal{M} : C^*)$ be a typing for network $\mathcal{M} = (\mathcal{M}, I, O, \mathcal{C})$. We say $(\mathcal{M} : C^*)$ is *weakly valid* – resp. *strongly valid* – iff, for every valuation $\text{VAL} : \mathsf{parameters}(\mathsf{pre}(C^*)) \to \mathbb{N}$, it holds that $\text{VAL} \models_{\text{w}} (\mathcal{M} : C^*)$ – resp. $\text{VAL} \models_{\text{s}} (\mathcal{M} : C^*)$. If $(\mathcal{M} : C^*)$ is weakly valid, we write $\text{VAL} \models_{\text{w}} (\mathcal{M} : C^*)$, and if strongly valid, we write $\text{VAL} \models_{\text{s}} (\mathcal{M} : C^*)$.

Informally, $(\mathcal{M} : C^*)$ is *weakly valid* iff, for every network flow satisfying $\mathsf{pre}(C^*)$, ***there is a way*** of channelling the flow through $\mathcal{M}$, consistent with its internal constraints, so that $\mathsf{post}(C^*)$ is satisfied. $(\mathcal{M} : C^*)$ is *strongly valid* iff, for every network flow satisfying $\mathsf{pre}(C^*)$ and ***for every way*** of channelling the flow through $\mathcal{M}$, consistent with its internal constraints, $\mathsf{post}(C^*)$ is satisfied. □

5 Ordering of Network Typings

We define a precise way of deciding that a typing is "stronger" (or "more informative") or "weaker" (or "less informative") than another typing.

Definition 11 (*Comparing Typings*)**.** Let $\mathcal{M} = (\mathcal{M}, I, O, \mathcal{C})$ be a untyped network sketch and let $(\mathcal{M} : C^*)$ a typing for $\mathcal{M}$. We use again the notions of "preconditions" and "postconditions" from Definition 9, but to make explicit that these relate to $\mathcal{M}$, we write $\mathsf{pre}(\mathcal{M} : C^*)$ instead of $\mathsf{pre}(C^*)$ and $\mathsf{post}(\mathcal{M} : C^*)$ instead of $\mathsf{post}(C^*)$, resp.

Let $(\mathcal{M} : C_1^*)$ and $(\mathcal{M} : C_2^*)$ be two typings for the same network sketch $\mathcal{M}$. We say $(\mathcal{M} : C_1^*)$ *implies* – or *is more precise than* – $(\mathcal{M} : C_2^*)$ and we write: $(\mathcal{M} : C_1^*) \Rightarrow (\mathcal{M} : C_2^*)$ just in case the two following conditions hold:

1. $\mathsf{pre}(\mathcal{M} : C_1^*) \Leftarrow \mathsf{pre}(\mathcal{M} : C_2^*)$, *i.e.*, the precondition of $(\mathcal{M} : C_1^*)$ is weaker than that of $(\mathcal{M} : C_2^*)$.
2. $\mathsf{post}(\mathcal{M} : C_1^*) \Rightarrow \mathsf{post}(\mathcal{M} : C_2^*)$, *i.e.*, the postcondition of $(\mathcal{M} : C_1^*)$ is stronger than that of $(\mathcal{M} : C_2^*)$.

We say $(\mathcal{M} : C_1^*)$ and $(\mathcal{M} : C_2^*)$ are *equivalent*, and write: $(\mathcal{M} : C_1^*) \Leftrightarrow (\mathcal{M} : C_2^*)$ in case $(\mathcal{M} : C_1^*) \Rightarrow (\mathcal{M} : C_2^*)$ *and* $(\mathcal{M} : C_1^*) \Leftarrow (\mathcal{M} : C_2^*)$. If $(\mathcal{M} : C_1^*) \Leftrightarrow (\mathcal{M} : C_2^*)$, it does not necessarily follow that $C_1^* = C_2^*$, because constraints implying each other are not necessarily identical. □

$$\textsc{Hole}\quad \frac{(X,\mathsf{In},\mathsf{Out}):\ \mathsf{Con}^*\ \in\ \Gamma}{\Gamma\ \vdash\ (X,\mathsf{In},\mathsf{Out},\{\ \}):\mathsf{Con}^*}$$

$$\textsc{Module}\quad \frac{(\mathcal{A},\mathsf{In},\mathsf{Out},\mathsf{Con}):\ \mathsf{Con}^*\ \ \text{typed module}}{\Gamma\ \vdash\ (\mathcal{B},I,O,\{C\}):C^*}\qquad ((\mathcal{B},I,O,C):C^*)=\ '((\mathcal{A},\mathsf{In},\mathsf{Out},\mathsf{Con}):\mathsf{Con}^*)$$

$$\textsc{Connect}\quad \frac{\Gamma\vdash(\mathcal{M},I_1,O_1,\mathcal{C}_1):C_1^*\qquad \Gamma\vdash(\mathcal{N},I_2,O_2,\mathcal{C}_2):C_2^*}{\Gamma\ \vdash\ (\mathbf{conn}(\theta,\mathcal{M},\mathcal{N}),I,O,\mathcal{C}):C^*}\quad \begin{array}{l}\theta\subseteq_{\text{1-1}} O_1\times I_2, I=I_1\cup(I_2-\mathsf{range}(\theta)), O=(O_1-\mathsf{domain}(\theta))\cup O_2,\\ C^*=(C_1^*\cup C_2^*)\restriction(I\cup O),\end{array}$$

$$(\mathrm{Ct})\quad \boxed{\begin{array}{l}\mathsf{post}(\mathcal{M}:C_1^*)\Rightarrow\\ \{x=y\,|\,(x,y)\in\theta\}\cup(\mathsf{pre}(\mathcal{N}:C_2^*)\downharpoonleft\mathsf{range}(\theta))\end{array}}$$

$$\textsc{Loop}\quad \frac{\Gamma\ \vdash\ (\mathcal{M},I_1,O_1,\mathcal{C}_1):C_1^*}{\Gamma\ \vdash\ (\mathbf{loop}(\theta,\mathcal{M}),I,O,\mathcal{C}):C^*}\quad \begin{array}{l}\theta\ \subseteq_{\text{1-1}} O_1\times I_1,\ \ I=I_1-\mathsf{range}(\theta),\ \ O=O_1-\mathsf{domain}(\theta),\\ C^*=C_1^*\restriction(I\cup O),\end{array}$$

$$(\mathrm{Lp})\quad \boxed{\begin{array}{l}\mathsf{post}(\mathcal{M}:C_1^*)\Rightarrow\{x=y\,|\,(x,y)\in\theta\}\cup(\mathsf{pre}(\mathcal{M}:C_1^*)\downharpoonleft\mathsf{range}(\theta))\\ \text{and}\quad(\mathsf{pre}(\mathcal{M}:C_1^*)\downharpoonleft I)\Rightarrow(\mathsf{pre}(\mathcal{M}:C_1^*)\downharpoonleft\mathsf{range}(\theta))\end{array}}$$

$$\textsc{Let}\quad \frac{\Gamma\ \vdash\ (\mathcal{M}_k,I_k,O_k,\mathcal{C}_k):C_k^*\quad\text{for } 1\leqslant k\leqslant n\qquad \Gamma\cup\{(X,\mathsf{In},\mathsf{Out}):\mathsf{Con}^*\}\ \vdash\ (\mathcal{N},I,O,\mathcal{C}):C^*}{\Gamma\ \vdash\ \big(\,\mathbf{let}\ X\!\in\{\mathcal{M}_1,\ldots,\mathcal{M}_n\}\ \mathbf{in}\,\mathcal{N}\ ,I,O,\mathcal{C}'\,\big):C^*}$$

for every $1\leqslant k\leqslant n$ and every isomorphism pair $(\varphi,\psi):(I_k,O_k)\to(\mathsf{In},\mathsf{Out})$:

$$(\mathrm{Lt})\quad \boxed{\begin{array}{l}\mathsf{pre}(\mathcal{M}_k:C_k^*)\ \Leftrightarrow\ \{\,x=\varphi(x)\,|\,x\in I_k\,\}\ \cup\ \mathsf{pre}(X:\mathsf{Con}^*)\quad\text{and}\\ \mathsf{post}(\mathcal{M}_k:C_k^*)\ \Leftrightarrow\ \{\,x=\varphi(x)\,|\,x\in I_k\,\}\ \cup\ \{\,x=\psi(x)\,|\,x\in O_k\,\}\ \cup\ \mathsf{post}(X:\mathsf{Con}^*)\end{array}}$$

$$\textsc{Weaken}\quad \frac{\Gamma\ \vdash\ (\mathcal{M},I,O,\mathcal{C}):C_1^*}{\Gamma\ \vdash\ (\mathcal{M},I,O,\mathcal{C}):C^*}\qquad(\mathrm{Wn})\quad \boxed{\mathsf{pre}(\mathcal{M}:C_1^*)\ \Leftarrow\ \mathsf{pre}(\mathcal{M}:C^*)\quad\text{and}\quad\mathsf{post}(\mathcal{M}:C_1^*)\ \Rightarrow\ \mathsf{post}(\mathcal{M}:C^*)}$$

Figure 2: Rules for Typed Network Sketches.

Normally we are interested in deriving "optimal" network typings, which are the most informative about the flows that the network can safely handle. We can also call them "minimal" rather than "optimal" because we think of them as being "at the bottom" of a partial ordering on typings. This is analogous to the *principal* (or *most general*) type of a function in a strongly-typed functional programming language; the principal type is the bottom element in the lattice of valid types for the function. This analogy shouldn't be pushed too far, however; a principal type is usually unique, whereas optimal typings are usually multiple.

Definition 12 (*Optimal Typings*)**.** Let $(\mathcal{M}:C_1^*)$ be a typing for a network sketch $\mathcal{M}$. We say $(\mathcal{M}:C_1^*)$ is an *optimal weakly-valid typing* just in case:

- $(\mathcal{M}:C_1^*)$ is a weakly-valid typing.
- For every weakly-valid typing $(\mathcal{M}:C_2^*)$,
  if $(\mathcal{M}:C_2^*)\ \Rightarrow\ (\mathcal{M}:C_1^*)$ then $(\mathcal{M}:C_2^*)\ \Leftrightarrow\ (\mathcal{M}:C_1^*)$.

Define *optimal strongly-valid typing* similarly, with "strongly" substituted for "weakly" in the two preceding bullet points. □

6 Network Sketches: Typed

We define typed specifications by the same inference rules we already used to derive untyped specifications in Section 3, but now augmented with type information.

Definition 13 (*Typed Network Holes*)**.** This continues Definition 6. The network hole $(X,\mathsf{In},\mathsf{Out})$ is *typed* if it is supplied with a finite set of *linear* constraints Con^* – *i.e.*, a type – written over $\mathsf{In}\cup\mathsf{Out}$. A fully specified *typed network hole* is written as "$(X,\mathsf{In},\mathsf{Out})\ :\ \mathsf{Con}^*$".

For simplicity, we may refer to $(X,\mathsf{In},\mathsf{Out})$ by its name X and write $(X\ :\ \mathsf{Con}^*)$ instead of $(X,\mathsf{In},\mathsf{Out})\ :\ \mathsf{Con}^*$ with the understanding that the omitted attributes can be uniquely retrieved by reference to the name X of the hole. □

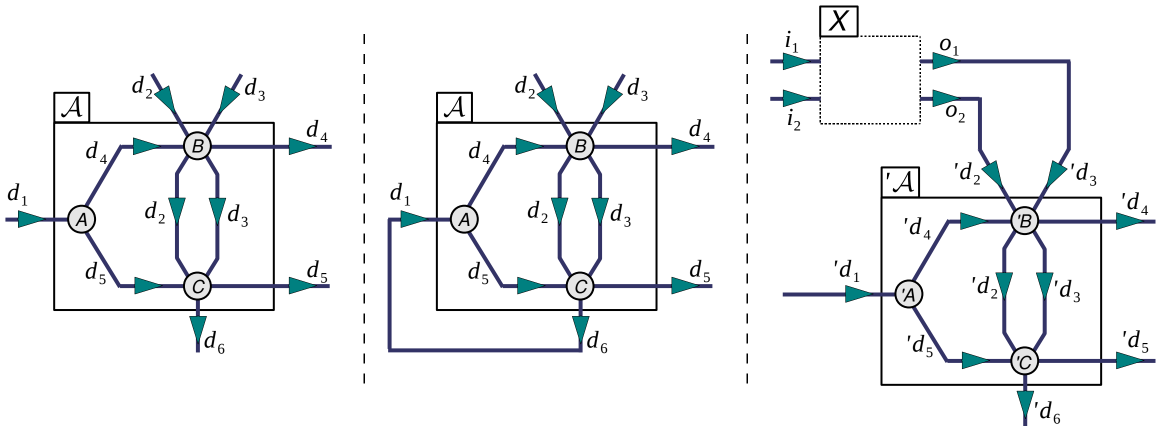

Figure 3: Graphic representation of module $\mathcal{A}$, network sketch $\mathcal{M} = \textsf{\textbf{loop}}(\{(d_6, d_1)\}, \mathcal{A})$, and network sketch $\mathcal{N} = \textsf{\textbf{conn}}(\{(o_1, 'd_3), (o_2, 'd_2)\}, X, '\mathcal{A})$. We omit a graphic representation of $\mathcal{P} = \textsf{\textbf{let}}\ X \in \{\mathcal{M}\}\ \textsf{\textbf{in}}\ \mathcal{N}$.

We repeat the rules Module, Hole, Connect, Loop, and Let, with the type information inserted. As they elaborate the previous rules, we omit some of the side conditions; we mention only the parts that are necessary for inserting the typing. The rules are shown in Figure 2.

In each of the rules, we highlight the crucial side-condition by placing it in a framed box; this condition expresses a relationship that must be satisfied by the "derived types" (linear constraints) in the premises of the rule. For later reference, we call this side-condition (Ct) in Connect, (Lp) in Loop, and (Lt) in Let.

There are different versions of rule Let depending on the side condition (Lt) – the weaker the side condition, the more powerful the rule, *i.e.*, the more network sketches for which it can derive a typing. The simplest way of formulating Let, as shown in Figure 2, makes the side condition most restrictive.

However, if we introduce the rule Weaken, the last shown in Figure 2, the side condition (Lt) is far less restrictive than it appears; it allows to adjust the derived types and constraints of the networks in $\{\mathcal{M}_1, \ldots, \mathcal{M}_n\}$ in order to satisfy (Lt), if possible by weakening them. (The rule Weaken plays the same role as a *subtyping* rule in the type system of an object-oriented programming language.)

7 An Extended Example

The purpose of this section is threefold. **First**, we show how constraints arising in use cases in practice can be formulated according to conventions laid out in this report. For this, we resort to an example from one of the use cases (vehicular traffic) we presented in our companion report [6] and discussed at a high level in the introduction. We now leave aside any of the practical justifications about vehicular traffic networks and focus on theoretical issues an implementation has to tackle.

Second, we want to show that several of our key notions are not vacuous. In particular, we want to illustrate the differences between "weakly valid" and "strongly valid" typings, between "optimal" and "non optimal" typings, and several of the relationships between these notions.

Third, we illustrate some of the limitations when we switch from "base mode" to "sketch mode"; specifically, when we abandon whole-system analysis and resort to compositional analysis using the rules of Section 6. This is done last in this section.

We consider a module $\mathcal{A}$ whose untyped specification is defined by a set $\textsf{Con}$ of internal constraints over input parameters $\{d_1, d_2, d_3\}$ and output parameters $\{d_4, d_5, d_6\}$. In this particular module $\mathcal{A}$, there are no purely internal parameters, *i.e.*, all are either input or output parameters. Con consists of:

(a)	$2 \leqslant d_1, d_4, d_5, d_6 \leqslant 8$	bounds on d_1, d_4, d_5 and d_6
(b)	$0 \leqslant d_2, d_3 \leqslant 6$	bounds on d_2 and d_3
(c)	$d_2 + d_3 + d_4 \leqslant 10$	constraint at node B
(d)	$d_2 + d_3 + d_5 \leqslant 10$	constraint at node C
(e)	$d_1 = d_4 + d_5$	constraint at node A
(f)	$d_2 + d_3 = d_6$	constraint at node C

In this simple example, all the constraints in Con are linear. Nevertheless, many of the issues and complications we need to handle with non-linear internal constraints already arise here. When we switch to sketch mode later in this section, we consider three networks – $\mathcal{M}$, $\mathcal{N}$, and $\mathcal{P}$ – assembled from the module $\mathcal{A}$ and a network hole X. Suppose X is assigned two input parameters $\{i_1, i_2\}$ and two output parameters $\{o_1, o_2\}$:

$$
\begin{aligned}
\mathcal{M} &= \textsf{\textbf{loop}}\Big(\{(d_6, d_1)\}, \mathcal{A}\Big) && \text{connect } d_6 \text{ to } d_1 \\
\mathcal{N} &= \textsf{\textbf{conn}}\Big(\{(o_1, {}'d_3), (o_2, {}'d_2)\}, X, {}'\mathcal{A}\Big) && \text{connect } o_1 \text{ to } {}'d_3\text{, and } o_2 \text{ to } {}'d_2 \\
\mathcal{P} &= \textsf{\textbf{let}}\ X \in \Big\{\mathcal{M}\Big\}\ \textsf{\textbf{in}}\ \mathcal{N} && \text{place } \mathcal{M} \text{ in hole } X \text{ of } \mathcal{N} \\
&= \textsf{\textbf{let}}\ X \in \Big\{\textsf{\textbf{loop}}(\{(d_6, d_1)\}, \mathcal{A})\Big\}\ \textsf{\textbf{in}}\ \textsf{\textbf{conn}}\Big(\{(o_1, {}'d_3), (o_2, {}'d_2)\}, X, {}'\mathcal{A}\Big)
\end{aligned}
$$

${}'\mathcal{A}$ is an isomorphic copy of $\mathcal{A}$ with its own fresh set of parameters $\{{}'d_1, {}'d_2, {}'d_3, {}'d_4, {}'d_5, {}'d_6\}$. Graphic representations of $\mathcal{A}$ (from [6]), $\mathcal{M}$ and $\mathcal{N}$ – but not $\mathcal{P}$ – are shown in Figure 3.

Note, in network $\mathcal{P}$, there are four possible ways of placing $\mathcal{M}$ in the hole X of $\mathcal{N}$, because there are two possible isomorphisms φ between the input parameters and two possible isomorphisms ψ between the output parameters, for a total of 4 possible isomorphism pairs

$$(\varphi, \psi) : (\{d_2, d_3\}, \{d_4, d_5\}) \to (\{i_1, i_2\}, \{o_1, o_2\})$$

See the side condition of rule Let in Figures 1 and 2.

We cannot just set $C^* = \mathsf{Con}$ – or, in general, set C^* to include all of the *linear* constraints in Con – in order to infer a valid typing $(\mathcal{A} : C^*)$ for module $\mathcal{A}$. In general, such a typing $(\mathcal{A} : C^*)$ is not guaranteed to be valid. For the present example, if $C^* = \mathsf{Con}$, then

$$
\begin{aligned}
\mathsf{pre}(C^*) &= \mathsf{closure}(C^*) \upharpoonright \{d_1, d_2, d_3\} \\
&\supseteq \{d_1 : [4, 8],\ d_2 : [0, 6],\ d_3 : [0, 6],\ d_2 + d_3 : [2, 8]\} \\
\mathsf{post}(C^*) &= \mathsf{closure}(C^*) \downharpoonleft \{d_4, d_5, d_6\} \\
&\supseteq \{d_4 : [2, 8],\ d_5 : [2, 8],\ d_6 : [2, 8],\ d_4 + d_5 : [4, 8],\ d_2 + d_3 + d_4 : [4, 10],\ d_2 + d_3 + d_5 : [4, 10],\ \text{(e)},\ \text{(f)}\}
\end{aligned}
$$

We write an interval constraint as "$d : [a, b]$" instead of "$a \leqslant d \leqslant b$", for some $a, b \in \mathbb{N}$, in order to save space. $\mathsf{pre}(C^*)$ and $\mathsf{post}(C^*)$ are supersets – note the "$\supseteq$" – of the listed constraints; constraints implied by those listed are omitted. The listed constraints from the two sets, $\mathsf{pre}(C^*)$ and $\mathsf{post}(C^*)$, are a finite basis for the full set.[4]

To show that $(\mathcal{A} : C^*)$ is not a valid typing, consider a valuation V such that $V(d_1) = 8$ and $V(d_2) = V(d_3) = 4$. It is easy to check that $V \models \mathsf{pre}(C^*)$. However, there is no extension $V' \supseteq V$ such that $V \models \mathsf{post}(C^*)$. Hence, $(\mathcal{A} : C^*)$ is not a valid *weak* typing, let alone a valid *strong* typing. Easy verification of these assertions are left to the reader. We need therefore to apply some extra care in order to infer valid typings.

The problem of *checking* typings for their validity is easier than *inferring* them, . We first examine theoretical issues underlying type checking and related aspects before tackling type inference.

[4]How to select a finite basis for an infinite set of linear constraints, assuming one exists, is an issue we ignore in this report – although the efficiency of an implementation very much depends on it.

Checking Weak Typings

Suppose we are given the typing $(\mathcal{A} : C_1^*)$ for module $\mathcal{A}$ where:

$$\boxed{C_1^* = \{\ d_1 : [4,8],\ d_2 : [1,3],\ d_3 : [1,3],\ d_4 : [2,4],\ d_5 : [2,4],\ d_6 : [2,6]\ \}}$$

We want to check that $(\mathcal{A} : C_1^*)$ is weakly valid. We compute finite bases D_1 and E_1 for $\mathsf{pre}(C_1^*)$ and $\mathsf{post}(C_1^*)$:

$$\begin{aligned} \mathsf{pre}(C_1^*) &\supseteq D_1 &= \{d_1 : [4,8],\ d_2 : [1,3],\ d_3 : [1,3]\} \\ \mathsf{post}(C_1^*) &\supseteq E_1 &= \{d_4 : [2,4],\ d_5 : [2,4],\ d_6 : [2,6]\} \end{aligned}$$

The size of the interval $[4,8]$ is 5 and that of the interval $[1,3]$ is 3, implying there is a total of $5\cdot3\cdot3 = 45$ distinct valuations V of $\{d_1, d_2, d_3\}$ that satisfy D_1. For each of these valuations V we have to check whether there is a valuation $V' \supseteq V$ of $\{d_4, d_5, d_6\}$ that satisfies both Con and E_1. The size of the interval $[2,4]$ is 3 and that of the interval $[2,6]$ is 5, implying there is a total of $3\cdot3\cdot5 = 45$ distinct such valuations $V' \supseteq V$. Hence, in the *worst case*, the space of valuations we have to search contains $45 \cdot 45 = 2025$ members – namely, for each of the 45 valuations V, we have to check each of the 45 extensions $V' \supseteq V$ for its satisfaction of Con and E_1. In the *best case*, we search and check only 45 of these 2025 valuations; this happens when the first $V' \supseteq V$ we check, for each of the 45 possible V, turns out to satisfy Con and E_1 – in which case we do not need to check any of the remaining 44 valuations V'.

In principle, the search and checking just described can be carried out exhaustively, but it is onerous and error-prone (if carried out by hand). Instead, we can take advantage of the *linearity* of the constraints in Con. For each of the 45 valuations V of $\{d_1, d_2, d_3\}$, we first compute $V(\mathsf{Con} \cup E_1)$, which is a finite set of linear constraints.[5] We can then check whether each such $V(\mathsf{Con} \cup E_1)$ is solvable using standard packages for linear programming and solving finite sets of linear equations – or, if the constraint set is small enough (as it is in this case), we can check its solvability by hand. But this is still expensive, with 45 distinct cases to consider!

A better approach, also based on the linearity of Con, is to first transform $\mathsf{Con} \cup E_1$ into an equivalent and simpler constraint set. We rewrite the constraints so that on the left-hand side are the non-input parameters (here d_4, d_5, d_6) which we want to express in terms of the input parameters on the right-hand side (here d_1, d_2, d_3). This produces the following constraints, ignoring the interval constraints (a) and (b) which involve only input parameters or are implied by (k), (ℓ) and (m) below:

(g)	$d_4 \leqslant 10 - (d_2 + d_3)$	from (c)
(h)	$d_5 \leqslant 10 - (d_2 + d_3)$	from (d)
(i)	$d_4 + d_5 = d_1$	same as (e)
(j)	$d_6 = d_2 + d_3$	same as (f)
(k)	$2 \leqslant d_4 \leqslant 4$	because $d_4 : [2,4]$ in E_1
(ℓ)	$2 \leqslant d_5 \leqslant 4$	because $d_5 : [2,4]$ in E_1
(m)	$2 \leqslant d_6 \leqslant 6$	because $d_6 : [2,6]$ in E_1

With $d_2, d_3 : [1,3]$, the largest possible value of $d_2 + d_3$ is 6, so that the smallest possible value on the right-hand side of (g) and (h) is 4. Hence, (g) and (h) are implied by (k) and (ℓ), respectively, and can be eliminated from consideration. Moreover, because the smallest possible value of $d_2 + d_3$ is 2 and its largest possible value is 6, (m) is implied by (j). Hence, $\mathsf{Con} \cup E_1$ is equivalent to the simpler $\{(i), (j), (k), (\ell)\}$ – under the assumption that $(d_2 + d_3) : [2,6]$. With the additional assumption that $d_1 : [4,8]$, it is easy to see that the set $\{(i), (j), (k), (\ell)\}$ is always solvable.[6]

[5] If e is an expression such that $\mathsf{parameters}(e) \not\subseteq \mathsf{domain}(V)$, we write $V(e)$ for the expression obtained from e by replacing every $d \in \mathsf{parameters}(e) \cap \mathsf{domain}(V)$ by $V(d)$. We define similarly $V(C)$ for a set C of constraints such that $\mathsf{parameters}(C) \not\subseteq \mathsf{domain}(V)$.

[6] In general, we may try to apply the algrebraic manipulation just described to constraint sets associated with other networks. But these can become quite difficult, if not impossible, to carry out by hand, especially if they include non-linear constraints. At a minumum, one will need an automated verification system to check equivalence of constraints over large finite domains.

The preceding shows that $(\mathcal{A} : C_1^*)$ is a weak typing. But it is not strong typing; for example, if we choose the following valuation V of $\{d_1, d_2, d_3\}$ that satisfies D_1:

$$V = \{d_1 \mapsto 8,\ d_2 \mapsto 1,\ d_3 \mapsto 1\}$$

and consider the extension $V' \supseteq V$ such that

$$V' = \{d_1 \mapsto 8,\ d_2 \mapsto 1,\ d_3 \mapsto 1,\ d_4 \mapsto 6,\ d_5 \mapsto 2,\ d_6 \mapsto 2\}$$

then $V' \models \mathsf{Con}$ but $V' \not\models E_1$.

A typing more complicated than $(\mathcal{A} : C_1^*)$ will include non-interval linear constraints. Suppose, for example, we want to check whether the typing $(\mathcal{A} : C_2^*)$ is weakly valid, where:

$$\boxed{C_2^* = \ \{\ d_1 : [4,8],\ d_2 : [2,4],\ d_3 : [1,2],\ d_4 : [2,4],\ d_5 : [2,4],\ d_6 : [3,6],\ d_1 = 2 \cdot d_2,\ d_4 = d_5\ \}}$$

We first compute finite bases D_2 and E_2 for $\mathsf{pre}(C_2^*)$ and $\mathsf{post}(C_2^*)$:

$$\begin{aligned} \mathsf{pre}(C_2^*) &\supseteq D_2 = \{d_1 : [4,8],\ d_2 : [2,4],\ d_3 : [1,2],\ d_1 = 2 \cdot d_2\ \} \\ \mathsf{post}(C_2^*) &\supseteq E_2 = \{d_4 : [2,4],\ d_5 : [2,4],\ d_6 : [3,6],\ d_4 = d_5\ \} \end{aligned}$$

To check the weak validity of $(\mathcal{A} : C_2^*)$, just as that of the earlier $(\mathcal{A} : C_1^*)$, we can try an exhaustive approach and/or a algebraic preprocessing of $\mathsf{Con} \cup E_2$ in order to simplify it.

$(\mathcal{A} : C_2^*)$ is not a strong typing. For example, if we choose the following valuation V of $\{d_1, d_2, d_3\}$ that satisfies D_2:

$$V = \{d_1 \mapsto 6,\ d_2 \mapsto 3,\ d_3 \mapsto 1\}$$

and consider the extension $V' \supseteq V$ such that

$$V' = \{d_1 \mapsto 6,\ d_2 \mapsto 3,\ d_3 \mapsto 1,\ d_4 \mapsto 4,\ d_5 \mapsto 2,\ d_6 \mapsto 4\}$$

then $V' \models \mathsf{Con}$ but $V' \not\models E_2$.

Checking Strong Typings

Suppose we are given the typing $(\mathcal{A} : C_3^*)$ for module $\mathcal{A}$ where:

$$\boxed{C_3^* = \ \{\ d_1 : [4,8],\ d_2 : [1,2],\ d_3 : [1,2],\ d_4 : [2,6],\ d_5 : [2,6],\ d_6 : [2,4]\ \}}$$

We want to check that $(\mathcal{A} : C_3^*)$ is strongly valid. We start by computing finite bases D_3 and E_3 for $\mathsf{pre}(C_3^*)$ and $\mathsf{post}(C_3^*)$:

$$\begin{aligned} \mathsf{pre}(C_3^*) &\supseteq D_3 = \{d_1 : [4,8],\ d_2 : [1,2],\ d_3 : [1,2]\} \\ \mathsf{post}(C_3^*) &\supseteq E_3 = \{d_4 : [2,6],\ d_5 : [2,6],\ d_6 : [2,4]\} \end{aligned}$$

We can try an exhaustive approach, very similar to that used for checking weak typings. The size of the interval $[4,8]$ is 5 and that of $[1,2]$ is 2. There are therefore $5 \cdot 2 \cdot 2 = 20$ distinct valuations V of $\{d_1, d_2, d_3\}$ which satisfy D_3. For each of these 20 valuations V, we have to check that, for *every* valuation $V' \supseteq V$ of $\{d_4, d_5, d_6\}$ satisfying Con, it holds that V' satisfies E_3. There is a large number of such valuations V', but because some of the constraints in Con are not intervals, this number is not readily computed. In any case, this is a tedious process, too expensive to carry out by hand.

There is a more efficient approach, more subtle than what we tried for checking weak typings. We assume we are given a valuation V of $\{d_1, d_2, d_3\}$ which satisfy D_3. Then we show that, for every valuation $V' \supseteq V$ of

$\{d_4, d_5, d_6\}$, if V' does *not* satisfy E_3 then V' does *not* satisfy Con. And more, since it is easier to deal with constraints that are intervals for a single parameter, we consider valuations V' which do not satisfy E_3 but do satisfy the single-parameter interval constraints in Con – constraints (a) here, not (b) whose satisfaction is implied by D_3 – and then show they cannot simultaneously satisfy all of the non-interval constraints in Con – constraints (c), (d), (e) and (f) here.

Hence, it suffices to show that if $d_4 : [2,8]-[2,6] = [7,8]$ *or* $d_5 : [2,8]-[2,6] = [7,8]$ *or* $d_6 : [2,8]-[2,4] = [5,8]$, then (c), (d), (e) and (f) cannot be all satisfied. This is indeed the case. If $d_4 : [7,8]$ (and $d_5 : [2,6]$), or $d_5 : [7,8]$ (and $d_4 : [2,6]$), or both $d_4, d_5 : [7,8]$, then (e) is violated, because $d_1 : [4,8]$. And if $d_6 : [5,8]$, then (f) is violated, because $d_2, d_3 : [1,2]$. This shows that $(\mathcal{A} : C_3^*)$ is a strong typing.

From Weak Typings To Strong Typings

By definition, every strong typing is a weak typing. The converse is not true. There is nevertheless an important relationship between weak and strong typings.

Given a weak typing which is not strong – such as $(\mathcal{A} : C_1^*)$ above – we can always *weaken the post-condition* or *strengthen the pre-condition* so that the resulting typing is strong. We define two strong typings $(\mathcal{A} : C_4^*)$ and $(\mathcal{A} : C_5^*)$ such that

$$(\mathcal{A} : C_1^*) \Rightarrow (\mathcal{A} : C_4^*) \quad \text{and} \quad (\mathcal{A} : C_1^*) \Rightarrow (\mathcal{A} : C_5^*)$$

where $(\mathcal{A} : C_4^*)$ is obtained by *weakening the post-condition* and $(\mathcal{A} : C_5^*)$ by *strengthening the pre-condition*.

This is always possible, but not interesting if carried out without restriction, because we want to find the *strongest* – i.e., the most informative – such typing $(\mathcal{A} : C_4^*)$ and $(\mathcal{A} : C_5^*)$.

Warning: Even though $(\mathcal{A} : C_1^*)$ is *stronger* than both $(\mathcal{A} : C_4^*)$ and $(\mathcal{A} : C_5^*)$ in the ordering of typings, $(\mathcal{A} : C_1^*)$ is a *weak typing* while $(\mathcal{A} : C_4^*)$ and $(\mathcal{A} : C_5^*)$ are *strong typings*. This is perhaps a little unsettling, since the ordering in the direction of weakening the typings (the direction of "⇒") is also the direction of going from weak typings to to strong typings, but this is another case of a contravariant relation.

We consider how to compute $(\mathcal{A} : C_4^*)$ from $(\mathcal{A} : C_1^*)$ by weakening the post-condition of the latter. For such $(\mathcal{A} : C_4^*)$ we set $\mathsf{pre}(C_4^*) = \mathsf{pre}(C_1^*)$ and compute the strongest $\mathsf{post}(C_4^*)$ such that $\mathsf{post}(C_1^*) \Rightarrow \mathsf{post}(C_4^*)$:

$$\begin{aligned} \mathsf{pre}(C_4^*) &\supseteq D_4 &&= \{d_1 : [4,8],\ d_2 : [1,3],\ d_3 : [1,3]\} \\ \mathsf{post}(C_4^*) &\supseteq E_4 &&= \{d_4 : [a_4,b_4],\ d_5 : [a_5,b_5],\ d_6 : [a_6,b_6]\} \end{aligned}$$

for some $a_4, b_4, a_5, b_5, a_6, b_6 \in \mathbb{N}$ yet to be determined, and D_4 and E_4 are finite bases for $\mathsf{pre}(C_4^*)$ and $\mathsf{post}(C_4^*)$. To determine the intervals $[a_4,b_4]$, $[a_5,b_5]$ and $[a_6,b_6]$, we can follow an exhaustive approach: Exhaustively find the most precise such intervals (*i.e.*, narrowest, at the post-condition) such that:

$$[2,4] \subseteq [a_4,b_4] \quad \text{and} \quad [2,4] \subseteq [a_5,b_5] \quad \text{and} \quad [2,6] \subseteq [a_6,b_6]$$

which make $(\mathcal{A} : C_4^*)$ a strong typing. However, the example is sufficiently simple so that, by inspection, it is easy to check that the desired intervals are:

$$[a_4,b_4] = [a_5,b_5] = [a_6,b_6] = [2,6]$$

Hence, the desired strong typing is $(\mathcal{A} : C_4^*)$ where:

$$\boxed{C_4^* = \{\ d_1 : [4,8],\ d_2 : [1,3],\ d_3 : [1,3],\ d_4 : [2,6],\ d_5 : [2,6],\ d_6 : [2,6]\ \}}$$

We next consider how to compute $(\mathcal{A} : C_5^*)$ from $(\mathcal{A} : C_1^*)$ by strenghening the pre-condition of the latter. For such $(\mathcal{A} : C_5^*)$ we set $\mathsf{post}(C_5^*) = \mathsf{post}(C_1^*)$ and compute the weakest $\mathsf{pre}(C_5^*)$ such that $\mathsf{pre}(C_5^*) \Rightarrow \mathsf{pre}(C_1^*)$:

$$\begin{aligned} \mathsf{pre}(C_5^*) &\supseteq D_5 &&= \{d_1 : [a_1,b_1],\ d_2 : [a_2,b_2],\ d_3 : [a_3,b_3]\} \\ \mathsf{post}(C_5^*) &\supseteq E_5 &&= \{d_4 : [2,4],\ d_5 : [2,4],\ d_6 : [2,6]\} \end{aligned}$$

for some $a_1, b_1, a_2, b_2, a_3, b_3 \in \mathbb{N}$ yet to be determined, and D_5 and E_5 are finite bases for $\mathsf{pre}(C_5^*)$ and $\mathsf{post}(C_5^*)$. We want the most precise intervals (*i.e.*, widest, at the pre-condition) such that:

$$[a_1, b_1] \subseteq [4, 8] \quad \text{and} \quad [a_2, b_2] \subseteq [1, 3] \quad \text{and} \quad [a_3, b_3] \subseteq [1, 3]$$

which make $(\mathcal{A} : C_5^*)$ a strong typing. We avoid an exhaustive search of such intervals $[a_1, b_1]$, $[a_2, b_2]$ and $[a_3, b_3]$, because the example here is simple enough. By inspection, it is easy to see that the desired intervals are:

$$[a_1, b_1] = [4, 6] \quad \text{and} \quad [a_2, b_2] = [a_3, b_3] = [1, 3]$$

Hence, the desired strong typing is $(\mathcal{A} : C_5^*)$ where:

$$\boxed{C_5^* = \{\ d_1 : [4,6],\ d_2 : [1,3],\ d_3 : [1,3],\ d_4 : [2,4],\ d_5 : [2,4],\ d_6 : [2,6]\ \}}$$

Non-Optimal Typings vs. Optimal Typings

By Definition 12, a typing is optimal if its pre-condition cannot be weakened *and* its post-condition cannot be strengthened without violating its validity, be it weak or strong. None of the typings considered earlier in this section is optimal: $(\mathcal{A} : C_1^*)$ and $(\mathcal{A} : C_2^*)$ as weak typings, and $(\mathcal{A} : C_3^*), (\mathcal{A} : C_4^*)$ and $(\mathcal{A} : C_5^*)$ as strong typings.

While the pre-condition of each of these 5 typings cannot be weakened, its post-condition can be strengthened. In particular, none of these specifies in its post-condition that the total flow at the input parameters $\{d_1, d_2, d_3\}$ must equal the total flow at the output parameters $\{d_4, d_5, d_6\}$. That this conservation of flow holds for $\mathcal{A}$ is readily seen by inspecting constraints (e) and (f) in the given Con. We therefore define the set $\widehat{C}$ consisting of constraints (e) and (f):

$$\widehat{C} \;=\; \{(e), (f)\} \;=\; \{d_1 = d_4 + d_5,\ d_2 + d_3 = d_6\}$$

The two constraints in $\widehat{C}$ involve non-input parameters of $\mathcal{A}$. Hence, if we add $\widehat{C}$ to a typing of $\mathcal{A}$ it will appear in the post-condition of the typing. It turns out that each of the typings $(\mathcal{A} : C_1^* \cup \widehat{C}), \ldots, (\mathcal{A} : C_5^* \cup \hat{C})$ is in fact optimal. We omit the verification of this claim to the reader.

Comparing Typings

Among the 5 valid typings of $\mathcal{A}$, weak or strong, so far considered, the only pairwise comparisons that hold are:

$$(\mathcal{A} : C_1^*) \Rightarrow (\mathcal{A} : C_4^*) \quad \text{and} \quad (\mathcal{A} : C_1^*) \Rightarrow (\mathcal{A} : C_5^*)$$

as already argued. We leave to the reader the straightforward check that all other pairwise comparisons do not hold. Adding $\widehat{C} = \{(e), (f)\}$ to the post-condition of these three typings, we also obtain:

$$(\mathcal{A} : C_1^* \cup \widehat{C}) \Rightarrow (\mathcal{A} : C_4^* \cup \widehat{C}) \quad \text{and} \quad (\mathcal{A} : C_1^* \cup \widehat{C}) \Rightarrow (\mathcal{A} : C_5^* \cup \widehat{C})$$

Putting these comparisons in a single diagram, we get:

$$\begin{tikzcd}
\text{optimal} & \text{non optimal} & \\
(\mathcal{A} : C_4^* \cup \widehat{C}) \arrow[r, Rightarrow] & (\mathcal{A} : C_4^*) & \text{strong typings} \\
(\mathcal{A} : C_1^* \cup \widehat{C}) \arrow[r, Rightarrow] \arrow[u, Rightarrow] \arrow[d, Rightarrow] & (\mathcal{A} : C_1^*) \arrow[u, Rightarrow] \arrow[d, Rightarrow] & \text{weak typings} \\
(\mathcal{A} : C_5^* \cup \widehat{C}) \arrow[r, Rightarrow] & (\mathcal{A} : C_5^*) & \text{strong typings}
\end{tikzcd}$$

No other pairwise comparison, other than those shown in the diagram, holds between any two of the typings discussed earlier in this section. In the diagram, the typings in the top and bottom rows are strong, and the typings in the middle row are weak; the typings in the left column are optimal, and the typings in the right column are not optimal.

Adding Objective Functions to Optimal Typings

Optimal typings are not unique, as there are typically several distinct optimal typings for the same network, whether weak or strong. (By "distinct" we mean "not equivalent" rather than "syntactically different", because we can always pad a typing with redundant constraints that make it syntactically different from the original.) A useful way of preferring and choosing between different optimal typings is relative to *objective functions*. For example, an objective function may be to *maximize* the total flow allowed at the inputs, which means to maximize the sum of the upper-bounds on the input parameters $\{d_1, d_2, d_3\}$ modulo any restriction imposed by the pre-condition (if any). Relative to this objective function:

- $(\mathcal{A} : C_1^* \cup \widehat{C})$ and $(\mathcal{A} : C_2^* \cup \widehat{C})$ are equally good, among the weak typings of $\mathcal{A}$, because the maximum input flow for both of these typings is 14.
- $(\mathcal{A} : C_4^* \cup \widehat{C})$ is to be preferred to both $(\mathcal{A} : C_3^* \cup \widehat{C})$ and $(\mathcal{A} : C_5^* \cup \widehat{C})$, among the strong typings of $\mathcal{A}$, The maximum input flows for these three typings are 14, 12, and 12, respectively.

Another objective function may be to maximize the sum of the input-interval sizes, rather than their upper-bounds. Another is to *minimize* the sum of the output-interval sizes, perhaps for purposes of safe connection with another network downstream. Other objective functions can be defined by giving priority to some of the input parameters over others, or to some of the output parameters over others – and there are many other meaningful ones depending on the application.

Type Inference vs. Type Checking

A situation we have not considered so far is to *infer* a typing for $\mathcal{A}$. We start from the constraint set Con and infer an optimal typing, possibly relative to some objective function involving the input and/or output parameters. Depending on the application, we may want to infer a weak or strong typing.

To take a specific example, suppose we want to *infer an optimal weak typing for $\mathcal{A}$ satisfying the objective* $\{d_5 - 2 \leqslant d_4 < d_5\}$. As it involves output parameters d_4 and d_5, this objective will be in the post-condition. Because we want the typing to be optimal, we need to find a *weakest pre-condition* satisfying the objective. Starting from $\{d_5 - 2 \leqslant d_4 < d_5\}$ and working backwards through the constraint set Con, we can infer two weak typings $(\mathcal{A} : C_6^*)$ and $(\mathcal{A} : C_7^*)$ where – we omit the justification:

$$\boxed{C_6^* \;=\; \{\ d_1 : [5,8],\ d_2 : [1,2],\ d_3 : [1,3],\ d_4 : [2,3],\ d_5 : [3,5],\ d_6 : [2,5],\ d_5 - 2 \leqslant d_4 < d_5\ \}}$$

$$\boxed{C_7^* \;=\; \{\ d_1 : [5,8],\ d_2 : [1,3],\ d_3 : [1,2],\ d_4 : [2,3],\ d_5 : [3,5],\ d_6 : [2,5],\ d_5 - 2 \leqslant d_4 < d_5\ \}}$$

We obtain C_6^* and C_7^* by inferring the widest possible interval for each of the parameters $d_1, \ldots, d_6$, given the requirement $\{d_5 - 2 \leqslant d_4 < d_5\}$. Neither $(\mathcal{A} : C_6^*)$ nor $(\mathcal{A} : C_7^*)$ is yet optimal: We need to add the constraints $\widehat{C}$ expressing conservation of flow through $\mathcal{A}$. The desired *optimal* weak typings are $(\mathcal{A} : C_6^* \cup \widehat{C})$ and $(\mathcal{A} : C_7^* \cup \widehat{C})$.

Warning: If we keep the constraint $\{d_5 - 2 \leqslant d_4 < d_5\}$ in the post-condition, then it is impossible to obtain *strong* typings by *weakening* the other constraints in the post-condition, here by widening any of the intervals for the output parameters $\{d_4, d_5, d_6\}$. Although it is possible to *strengthen* $\mathsf{pre}(C_6^*)$ and $\mathsf{pre}(C_7^*)$ to obtain *strong* typings, it must be by making the pre-condition inconsistent – *e.g.*, by narrowing the interval for d_1 down to $d_1 : [\ ]$ – and the resulting typings trivially valid. But this is not interesting. More generally, *if we require $\{d_5 - 2 \leqslant d_4 < d_5\}$ to be part of the post-condition, there are no (interesting) strong typings for $\mathcal{A}$, only weak typings.*

We consider one more example of type inference, which we use again below. Suppose we want to *infer an optimal weak typing for $\mathcal{A}$ whose post-condition includes the constraint $d_1 = d_6$*. Again here, working backwards from the desired post-condition, we can infer the following weak typing $(\mathcal{A} : C_8^*)$ and $(\mathcal{A} : C_9^*)$ where:

$$\boxed{C_8^* \;=\; \{\ d_1 : [4,6],\ d_2 : [2,3],\ d_3 : [2,3],\ d_4 : [2,3],\ d_5 : [2,3],\ d_6 : [4,6],\ d_1 = d_6\ \}}$$

$$\boxed{C_9^* \;=\; \{\ d_1 : [4,6],\ d_2 : [2,4],\ d_3 : [2,2],\ d_4 : [2,4],\ d_5 : [2,2],\ d_6 : [4,6],\ d_1 = d_6\ \}}$$

There are several other weak typings satisfying the post-condition $d_1 = d_6$ obtained from C_8^* and C_9^*, by switching the intervals for d_2 and d_3 and/or switching the intervals for d_4 and d_5. $(\mathcal{A} : C_8^*)$ and $(\mathcal{A} : C_9^*)$ are incomparable, and neither is comparable with any of the earlier typings for $\mathcal{A}$. To make these two typings optimal, we add the constraints $\widehat{C}$ for conservation of flow, and thus obtain $(\mathcal{A} : C_8^* \cup \widehat{C})$ and $(\mathcal{A} : C_9^* \cup \widehat{C})$.

Using Rule Loop

We connect output parameter d_6 to input parameter d_1 in module $\mathcal{A}$ to obtain network $\mathcal{M}$ described earlier in this section. Rule Loop produces a weak (resp. strong) typing for $\mathcal{M}$ from a weak (resp. strong) typing for $\mathcal{A}$, provided the side condition (Lp) is satisfied.

Of all the typings for $\mathcal{A}$ considered so far, only the four last – $(\mathcal{A} : C_8^*)$ and $(\mathcal{A} : C_9^*)$ and their subtypings $(\mathcal{A} : C_8^* \cup \widehat{C})$ and $(\mathcal{A} : C_9^* \cup \widehat{C})$ – will satisfy (Lp). For definiteness, consider $(\mathcal{A} : C_8^* \cup \widehat{C})$, for which we have:

$$\begin{aligned}
\mathsf{pre}(C_8^* \cup \widehat{C}) \;&\supseteq D_8 \;= \{d_1 : [4,6], d_2 : [2,3], d_3 : [2,3], d_1 = d_2 + d_3\} \\
\mathsf{post}(C_8^* \cup \widehat{C}) \;&\supseteq E_8 \;= \{d_4 : [2,3], d_5 : [2,3], d_6 : [4,6], d_1 = d_6, d_1 = d_4 + d_5, d_6 = d_2 + d_3\}
\end{aligned}$$

where D_8 and E_8 are finite bases for $\mathsf{pre}(C_8^*)$ and $\mathsf{post}(C_8^*)$. From D_8, we define D_8' and D_8'' as follows:

$$\begin{aligned}
D_8' &= (D_8 \downharpoonleft \{d_1\}) &&= \{d_1 : [4,6], d_1 = d_2 + d_3\} \\
D_8'' &= (D_8 \downharpoonleft \{d_2, d_3\}) &&= \{d_2 : [2,3], d_3 : [2,3], d_1 = d_2 + d_3\}
\end{aligned}$$

It is easy to see that $E_8 \Rightarrow \{d_1 = d_6\} \cup D_8'$ and $D_8'' \Rightarrow D_8'$, as required by the two parts of side-condition (Lp). The resulting typing is $(\mathcal{M} : C_{10}^*)$ where:

$$\boxed{C_{10}^* \;=\; (C_8^* \cup \widehat{C}) \upharpoonright \{d_2, d_3, d_4, d_5\} \;=\; \{\ d_2 : [2,3],\ d_3 : [2,3],\ d_4 : [2,3],\ d_5 : [2,3]\ \}}$$

Note that $(\mathcal{M} : C_{10}^*)$ is not an optimal typing for $\mathcal{M}$. To turn it into an optimal typing, it suffices to include the constraint $\{d_2 + d_3 = d_4 + d_5\}$ to C_{10}^*, which expresses conservation of flow across $\mathcal{M}$. Our formulation of the typing rules in Figure 2 preserve validity, both weak and strong, but not optimality.

Using Rule Connect

That $(\mathcal{A} : C_1^*)$ is a weak typing for $\mathcal{A}$ implies that $('\mathcal{A} : 'C_1^*)$ is a weak typing for its isomorphic copy $'\mathcal{A}$. Suppose we assign to hole X the the typing $(X : C_{11}^*)$ where:

$$C_{11}^* \;=\; \{\ i_1 : [2,3],\ i_2 : [2,3],\ o_1 : [2,3],\ o_2 : [2,3]\ \}$$

Connecting output parameters o_1 and o_2 in X to input parameters $'d_3$ and $'d_2$ in $'\mathcal{A}$, respectively, it is easy to check that side-condition (Ct) is satisfied. The resulting typing is $(\mathcal{N} : C_{12}^*)$ where:

$$\boxed{C_{12}^* = ('C_1^* \cup C_{11}^*) \upharpoonright \{i_1, i_2, 'd_1, 'd_4, 'd_5, 'd_6\} = \{i_1 : [2,3], i_2 : [2,3], 'd_1 : [4,8], 'd_4 : [2,4], 'd_5 : [2,4], 'd_6 : [2,6]\}}$$

Note that $(\mathcal{N} : C_{12}^*)$ is not optimal for $\mathcal{N}$; *e.g.*, the output constraint $'d_6 : [2,6]$ can be strengthened to $'d_6 : [4,6]$ without violating the weak validity of the typing.

Using Rule Let

The typings $(\mathcal{M} : C^*_{10})$ and $(X : C^*_{11})$ are such that, under any of the 4 isomorphism pairs (φ, ψ):

$$(\varphi, \psi) : (\{d_2, d_3\}, \{d_4, d_5\}) \to (\{i_1, i_2\}, \{o_1, o_2\})$$

the side-condition (Lt) is satisfied. Hence, by rule Let, $(\mathcal{P} : C^*_{12})$ is a weak typing for $\mathcal{P}$.

8 Soundness

The inference rules for typed network sketches presented in Figure 2 are sound with respect to both strong and weak versions of validity. We present an argument that the inference rules are sound with respect to both the strong and weak versions of validity. We note within the proof any differences that arise between the proof for the two notions. These differences occur exclusively when specifying the quantifier governing the valuations V' and V'', the extensions of V that satisfy certain constraint sets.

This claim is stated formally in Theorem 16. The theorem is proven by an inductive argument for which there exist two base cases, which we state below.

Axiom 14 (Module)**.** *If we have by the inference rule* Module *that* $\Gamma \vdash (\mathcal{A}, \mathsf{In}, \mathsf{Out}, \mathcal{C}) : C^*_0$ *then it is the case that* $V \models (\mathcal{A}, \mathsf{In}, \mathsf{Out}, \mathcal{C}) : C^*_0$*.*

Axiom 15 (Hole)**.** *If we have by the inference rule* Hole *that* $\Gamma \vdash (X, \mathsf{In}, \mathsf{Out}, \{\}) : C^*_0$ *then it is the case that* $V \models (X, \mathsf{In}, \mathsf{Out}, \{\}) : C^*_0$*.*

Modules and holes are the basis of our inductive proof. While it is possible to construct a module $\mathcal{A}$ for which $V \not\models \mathcal{A} : C^*_0$ and holes for which $V \not\models X : C^*_0$, it is unreasonable to expect any network with such modules or holes to have a valid valuation. Thus, we assume that all modules and holes trivially satisfy our theorem.

Theorem 16 (Soundness)**.** *If* $\Gamma \vdash \mathcal{N} : C^*$ *can be derived by the inference rules then for any* V*,* $V \models \mathcal{N} : C^*$*.*

Proof. The theorem holds by induction over the structure of the derivation $\Gamma \vdash \mathcal{N} : C^*$. Axioms 14 and 15 are the two base cases, and Propositions 18, 17, 19, and 20 cover the four possible inductive cases. ☐

In related work [20], a significant portion of the proof has been formalized and verified using a lightweight formal reasoning and automated verification system.

8.1 Inductive Cases

Proposition 17 (Connect)**.** *If* $V \models (\mathcal{M}, I_1, O_1, \mathcal{C}_1) : C^*_1$*,* $V \models (\mathcal{N}, I_2, O_2, \mathcal{C}_2) : C^*_2$*, and we have by the inference rule* Connect *that*

$$\Gamma \vdash (\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}), I, O, \mathcal{C}) : C^*$$

then it is the case that $V \models (\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}), I, O, \mathcal{C}) : C^*$*.*

Proof. We show that if $V \models \mathsf{pre}((\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}), I, O, \mathcal{C}) : C^*)$ then there exists (or for all, respectively) $V'' \supseteq V$ such that

$$\begin{aligned} V'' &\models \mathsf{post}((\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}), I, O, \mathcal{C}) : C^*) \\ V'' &\models \mathcal{C}. \end{aligned}$$

Suppose $V \models \mathsf{pre}((\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}), I, O, \mathcal{C}) : C^*)$. Note that $I = I_1 \cup (I_2 - \mathsf{range}(\theta))$, so $I_1 \subseteq I$. Note also that $\mathsf{parameters}(C^*_1) \subseteq I_1$ so $C^*_1 = C^*_1 \restriction I_1$ and

$$C^*_1 \;\subseteq\; C^*_1 \restriction I \cup O \;\subseteq\; C^*_1 \cup C^*_2 \restriction I \cup O \;\subseteq\; C^*.$$

Thus, $V \models \mathsf{pre}(\mathcal{M} : C_1^*)$. By $V \models (\mathcal{M} : C_1^*)$, this implies that there exists (or for all, respectively) $V' \supseteq V$ such that $V' \models \mathsf{post}(\mathcal{M} : C_1^*)$ and by the side condition (Ct) this implies that

$$V' \models \mathsf{pre}(\mathcal{N} : C_2^*) \downharpoonleft \mathsf{range}(\theta).$$

Note also that,

$$\begin{array}{rcl} C_2^* \upharpoonright (I_2 - \mathsf{range}(\theta)) & \subseteq & C_1^* \cup C_2^* \upharpoonright (I_1 \cup (I_2 - \mathsf{range}(\theta))) \cup O \\ & \subseteq & C_1^* \cup C_2^* \upharpoonright I \cup O \\ & \subseteq & C^*. \end{array}$$

Thus, since $V \models \mathsf{pre}(\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}) : C^*)$ we have $V \models \mathsf{pre}(\mathcal{N} : C_2^*) \upharpoonright (I_2 - \mathsf{range}(\theta))$ and because $\mathsf{parameters}(C_2^*) \subseteq I_2$, $V \models \mathsf{pre}(\mathcal{N} : C_2^*)$ and so $V' \models \mathsf{pre}(\mathcal{N} : C_2^*)$. This implies by $V \models (\mathcal{N} : C_2^*)$ and $V' \supseteq V$ that there exists (or for all, respectively) $V'' \supseteq V$ such that

$$\begin{array}{rcl} V'' & \models & \mathsf{pre}(\mathcal{M} : C_1^*), \\ V'' & \models & \mathsf{pre}(\mathcal{N} : C_2^*), \\ V'' & \models & \mathsf{post}(\mathcal{M} : C_1^*), \\ V'' & \models & \mathsf{post}(\mathcal{N} : C_2^*). \end{array}$$

Because this captures all constraints within the types, it is naturally the case that

$$V'' \models \mathsf{post}(\mathbf{conn}(\theta, \mathcal{M}, \mathcal{N}) : C^*).$$

It remains to show that $V'' \models \mathcal{C}$. First, note that $V'' \models \mathcal{C}_1$ and $V'' \models \mathcal{C}_2$ by consequence of V'' satisfying all preconditions. Furthermore, $V'' \models \{o = i \mid (o, i) \in \theta\}$ by consequence of the side condition (Ct). Thus, $V'' \models \mathcal{C}$. □

Proposition 18 (Loop)**.** *If $V \models (\mathcal{M}, I_1, O_1, \mathcal{C}_1) : C_1^*$ and we have by the inference rule* Loop *that $\Gamma \vdash (\mathbf{loop}(\theta, \mathcal{M}), I, O, \mathcal{C}) : C^*$ then it is the case that $V \models (\mathbf{loop}(\theta, \mathcal{M}), I, O, \mathcal{C}) : C^*$.*

Proof. Suppose $V \models \mathsf{pre}((\mathbf{loop}(\theta, \mathcal{M}), I, O, \mathcal{C}) : C^*)$. We know that

$$\mathsf{pre}((\mathbf{loop}(\theta, \mathcal{M}), I, O, \mathcal{C}) : C^*) = \mathsf{pre}((\mathcal{M}, I_1, O_1, \mathcal{C}_1) : C_1^*) \upharpoonright (I_1 - \mathsf{range}(\theta)),$$

so it is also the case that

$$V \models \mathsf{pre}((\mathcal{M}, I_1, O_1, \mathcal{C}_1) : C_1^*) \upharpoonright (I_1 - \mathsf{range}(\theta)).$$

We have $\mathsf{domain}(V) \subseteq \mathsf{parameters}(C^*)$, so $\mathsf{domain}(V) \cap \mathsf{range}(\theta) = \emptyset$. By the second part of side condition (Lp) we have

$$V \models \mathsf{pre}((\mathcal{M}, I_1, O_1, \mathcal{C}_1) : C_1^*) \downharpoonleft \mathsf{range}(\theta).$$

Since $\mathsf{parameters}(C_1^*) \subseteq I_1$ this means that $V \models \mathsf{pre}(\mathcal{M} : C_1^*)$ and by $V \models (\mathcal{M} : C_1^*)$ we know there exists (or for all, respectively) $V' \supseteq V$ such that

$$V' \models \mathsf{post}(\mathcal{M} : C_1^*).$$

Because $\mathsf{domain}(V')$ can potentially contain new elements, we now need that $V' \models \mathsf{pre}(\mathcal{M} : C_1^*) \downharpoonleft \mathsf{range}(\theta)$, and this is implied by the side condition (Lp), so

$$V' \models \mathsf{pre}(\mathcal{M} : C_1^*).$$

Because $C^* = C_1^* \upharpoonright (I \cup O)$ means $C^* \subseteq C_1^*$, we know that V' satisfies all constraints within the types for both $\mathcal{M}$ and $\mathbf{loop}(\theta, \mathcal{M})$, so we have

$$V' \models \mathsf{post}(\mathbf{loop}(\theta, \mathcal{M}) : C^*).$$

Finally, we know that $V' \models \mathcal{C}_1$ by $V \models \mathsf{pre}(\mathcal{M} : C_1^*)$ and that $V' \models \{o = i \mid (o, i) \in \theta\}$ by side condition (Lp), so $V' \models \mathcal{C}$. □

Proposition 19 (Let)**.** *If* $V \models (\mathcal{M}_k, I_k, O_k, \mathcal{C}_k) : C_k^*$ *for* $k \in \{1, \ldots, n\}$, $V \models (\mathcal{N}, I, O, \mathcal{C}) : C^*$, *and we have by the inference rule* Let *that*

$$\Gamma \vdash (\textsf{let } X \in \{\mathcal{M}_1, \ldots, \mathcal{M}_n\} \textsf{ in } \mathcal{N}, I, O, \mathcal{C}') : C^*$$

then it is the case that $V \models (\textsf{let } X \in \{\mathcal{M}_1, \ldots, \mathcal{M}_n\} \textsf{ in } \mathcal{N}, I, O, \mathcal{C}') : C^*$.

Proof. Suppose $V \models \textsf{pre}(\textsf{let } X \in \{\mathcal{M}_1, \ldots, \mathcal{M}_n\} \textsf{ in } \mathcal{N} : C^*)$. First, note that I, O, and C^* are the same both in the premises and in the conclusion, so

$$\textsf{pre}((\textsf{let } X \in \{\mathcal{M}_1, \ldots, \mathcal{M}_n\} \textsf{ in } \mathcal{N}, I, O, \mathcal{C}') : C^*) = \textsf{pre}((\mathcal{N}, I, O, \mathcal{C}') : C^*).$$

Thus, by our inductive hypothesis we know that there exists (or for all, respectively) $V' \supseteq V$, $V' \models \textsf{post}((\mathcal{N}, I, O, \mathcal{C}) : C^*)$, and so

$$V' \models \textsf{post}((\textsf{let } X \in \{\mathcal{M}_1, \ldots, \mathcal{M}_n\} \textsf{ in } \mathcal{N}, I, O, \mathcal{C}') : C^*).$$

It remains to show that $V' \models \mathcal{C}'$. We know that if X indeed appears in $\mathcal{N}$, it must hold by the base case for [Hole] that $V' \models \textsf{pre}(X : C_0^*)$ and $V' \models \textsf{post}(X : C_0^*)$. Furthermore, it is trivially true that for every k, for every isomorphism φ,

$$V' \models \{x = \varphi(x) \mid x \in I_k\}.$$

Thus, by the side condition (Lt), it is the case that for all k, $V' \models \textsf{pre}(\mathcal{M}_k : C_k^*)$. By our inductive hypothesis, this means that for all k, V' is such that

$$\begin{aligned} V' &\models \textsf{post}(\mathcal{M}_k : C_k^*), \\ V' &\models \mathcal{C}_{k,r}. \end{aligned}$$

Thus, $V' \models \mathcal{C}'$. □

Proposition 20 (Weaken)**.** *If* $V \models \mathcal{M} : C_1^*$ *and we have by the inference rule* Weaken *that* $\Gamma \vdash \mathcal{M} : C^*$ *then it is the case that* $V \models \mathcal{M} : C^*$.

Proof. Suppose $V \models \textsf{pre}(\mathcal{M} : C^*)$. We know by the side condition (Wn) that $\textsf{pre}(\mathcal{M} : C^*) \Rightarrow \textsf{pre}(\mathcal{M} : C_1^*)$, so $V \models \textsf{pre}(\mathcal{M} : C_1^*)$. By $V \models (\mathcal{M} : C_1^*)$, this means that there exists (or for all, respectively) $V' \supseteq V$,

$$\begin{aligned} V' &\models \textsf{post}(\mathcal{M} : C_1^*) \\ V' &\models \mathcal{C}. \end{aligned}$$

Finally, the side condition (Wn) states that $\textsf{post}(\mathcal{M} : C_1^*) \Rightarrow \textsf{post}(\mathcal{M} : C^*)$ so we know that $V' \models \textsf{post}(\mathcal{M} : C^*)$. □

9 Related Work

Our formalism for reasoning about constrained-flow networks was inspired by and based upon formalisms for reasoning about programs developed over the decades within the programming languages community. While our work focuses in particular on networks and constraints on flows, there is much relevant work in the community addressing the general problem of reasoning about distributed programs. However, most previously proposed systems for reasoning in general about the behavior of distributed programs (Process algebra [3], Petri nets [27], Π-calculus [25], finite-state models [22, 23, 24], and model checking [16, 17]) rely upon the retention of details about the *internals* of a system's components in assessing their interactions with one another. While this affords these systems great expressive power, that expressiveness necessarily carries with it a burden of complexity. Such an approach is inherently not modular in its analysis. In particular, the details maintained in a representation or model of a component are not easily introduced or removed. Thus, in order for a global analysis in which components are interfaced or compared to be possible, the specifications of components must be highly coordinated. Furthermore, these specifications are often wedded to particular methodologies and thus do not have the *generality* necessary to allow multiple kinds of analysis. This incompatibility between different forms of analysis makes it difficult to model and reason about how systems specified using different methodologies interact. More generally, maintaining information about internal details makes it difficult to analyze parts of a system independently and then, without reference to the internals of those parts, assess whether they can be assembled together.

Discovering and enforcing bounds on execution of program fragments is a well-established problem in computing [32], and our notion of types (*i.e.*, linear constraints) for networks can be viewed as a generalization of type systems expressing upper bounds on program execution times. Existing work on this problem includes the aiT tool (described in [29], and elsewhere), which uses control-flow analysis and abstract interpretation to provide static analysis capabilities for determining worst and best case execution time bounds. Other works, belonging to what have been called Dependent Type Systems, provide capabilities for estimating an upper bound on execution time and memory requirements via a formal type system that has been annotated with size bounds on data types. These include (but are not limited to) Static Dependent Costs [28], Sized Type Systems [18], and Sized Time Systems [21]. Many other Dependent Type Systems directly target resource bounding for the real-time embedded community (*e.g.*, the current incarnation of the Sized Time System [13], Mobile Resource Guarantees for Smart Devices [2]).

More generally, there has been a large interest in applying custom type systems to domain specific languages (which peaked in the late nineties, *e.g.*, the USENIX Conference on Domain-Specific Languages (DSL) in 1997 and 1999). Later type systems have been used to bound other resources such as expected heap space usage (*e.g.*, [15], [2]). The support for constructing, modelling, inferring, and visualizing networks and properties of network constraints provided by our work is similar to the capabilities provided by modelling and checking tools such as Alloy [19]. Unlike Alloy's system, which models constraints on sets and relations, our formalism focuses on constraints governing flows through directed graphs.

One of the essential activities our formalism aims to support is reasoning about and finding solution ranges for sets of constraints that happen to describe properties of a network. In its most general form, this is known as the *constraint satisfaction problem* [31] and is widely studied [30]. The types we have discussed in this work are linear constraints, so one variant of the constraint satisfaction problem relevant to our work involves only linear constraints. Finding solutions respecting collections of linear constraints is a classic problem that has been considered in a large variety of work over the decades. There exist many documented algorithms [10, Ch. 29] and analyses of practical considerations [12]. However, the typical approach is to consider a homogenous list of constraints of a particular class. A distinguishing feature of our formalism is that it does not treat the set of constraints as monolithic. Instead, a tradeoff is made in favor of providing users a way to manage large constraint sets through abstraction, encapsulation, and composition. Complex constraint sets can be hidden behind simpler constraints – namely, types (*i.e.*, linear constraints) that are restricted to make the analysis tractable – in exchange for a potentially more restrictive solution range. Conjunction of large constraint sets is made more tractable by employing compositional techniques.

The work in this paper extends and generalizes our earlier work in Traffic (*Typed Representation and Analysis of Flows For Interoperability Checks* [4]), and complements our earlier work in Chain (*Canonical Homomorphic Abstraction of Infinite Network protocol compositions* [8]). Chain and Traffic are two distinct generic frameworks for analyzing existing grids/networks, and/or configuring new ones, of local entities to satisfy desirable global properties. Relative to one particular global property, Chain's approach is to reduce a large space of sub-configurations of the complete grid down to a relatively small and equivalent space that is amenable to an exhaustive verification of the global property using existing model-checkers. Traffic's approach uses type-theoretic notions to specify one or more desirable properties in the form of invariants, each invariant being an appropriately formulated type, that are preserved when interfacing several smaller subconfigurations to produce a larger subconfiguration. Chain's approach is top-down, Traffic's approach is bottom-up.

While our formalism supports the specification and verification of desirable global properties and has a rigorous foundation, it remains ultimately lightweight. By "lightweight" we mean to contrast our work to the heavy-going formal approaches – accessible to a narrow community of experts – which are permeating much of current research on formal methods and the foundations of programming languages (such as the work on automated proof assistants [26, 14, 9, 11], or the work on polymorphic and higher-order type systems [1], or the work on calculi for distributing computing [7]). In doing so, our goal is to ensure that the constructions presented to users are the *minimum* that they might need to accomplish their task, keeping the more complicated parts of these formalisms "under the hood".

10 Conclusion and Future Work

We have introduced a compositional formalism for modelling or assembling networks that supports reasoning about and analyzing constraints on flows through these networks. We have precisely defined a semantics for this formalism, and have illustrated how it can be used in specific scenarios (other examples can be found in a companion paper [6] describing NetSketch, a tool that implements this formalism). Finally, we noted that this formalism is sound with respect to its semantics in a rigorous sense (a complete formal proof of this assertion can be found in the full version of this report [5]).

In the tool that employs our formalism (NetSketch), the constraint system implemented is intended to be a proof-of-concept to enable work on typed networks (holes, types, and bounds). We intend to expand the constraint set that is supported within NetSketch to include more complex constraints. Likewise, future work involving the formalism itself could involve enriching the space of constraints. This includes both relatively straightforward extensions, such as the introduction of new relations or operators into the grammar of constraints, as well as more sophisticated ones. For instance, we have only briefly begun experimentation with making time an explicit parameter in our current framework. As a concrete example, consider the preservation of density at a fork gadget, currently defined as $d_1 = d_2 + d_3$. Time as an explicit parameter, we could describe constraints indexed with discrete time intervals (*e.g.*, $d_1(t) = d_2(t) + d_3(t)$) and can easily imagine constraints that are dependent on prior parameter values.

The equivalent of *type inference* within our formalism also deserves more attention and effort. As we indicated, there is no natural ordering of types. If no optimal constraint function is assumed, any reasonable type inference process could produce multiple, different valid types. Types can be considered optimal based on the size of their value ranges (*e.g.*, a wider or more permissive input range, and narrower or more specific output range, are preferable, in analogy with types in a strongly-typed functional language or in an object-oriented language), but even then, multiple "optimal" typings may exist. It is necessary to establish principles and algorithms by which a tool employing our formalism could assign types. Such principles or algorithms might operate by assigning weights for various valid typings.

References

[1] *Proceedings of the 8th International Conference on Typed Lambda Calculi and Applications*, Paris, France, June 2007.

[2] D. Aspinall, S. Gilmore, M. Hofmann, D. Sannella, and I. Stark. Mobile resource guarantees for smart devices. In *Construction and Analysis of Safe, Secure and Interoperable Smart Devices: Proceedings of the International Workshop CASSIS 2004*, number 3362 in Lecture Notes in Computer Science, pages 1–26. Springer-Verlag, 2005.

[3] J. Baeten and W. Weijland. *Process Algebra*. Cambridge University Press, 1990.

[4] A. Bestavros, A. Bradley, A. Kfoury, and I. Matta. Typed Abstraction of Complex Network Compositions. In *Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP'05)*, Boston, MA, November 2005.

[5] A. Bestavros, A. Kfoury, A. Lapets, and M. Ocean. Safe Compositional Network Sketches: Formalism. Technical Report BUCS-TR-2009-029, CS Dept., Boston University, September 29 2009.

[6] A. Bestavros, A. Kfoury, A. Lapets, and M. Ocean. Safe Compositional Network Sketches: Tool and Use Cases. Technical Report BUCS-TR-2009-028, CS Dept., Boston University, September 29 2009.

[7] G. Boudol. The π-calculus in direct style. In *97: 24th*, pages 228–241, 1997.

[8] A. Bradley, A. Bestavros, and A. Kfoury. Systematic Verification of Safety Properties of Arbitrary Network Protocol Compositions Using CHAIN. In *Proceedings of ICNP'03: The 11th IEEE International Conference on Network Protocols*, Atlanta, GA, November 2003.

[9] A. Ciaffaglione. *Certified reasoning on Real Numbers and Objects in Co-inductive Type Theory.* PhD thesis, Dipartimento di Matematica e Informatica Università di Udine, Italy, 2003. available as outline.

[10] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms.* The MIT Electrical Engineering and Computer Scienece Series. The MIT Press, McGraw-Hill Book Company, 1990.

[11] K. Crary and S. Sarkar. Foundational certified code in a metalogical framework. In *Nineteenth International Conference on Automated Deduction*, Miami, Florida, 2003.

[12] R. Fletcher. *Practical methods of optimization; (2nd ed.).* Wiley-Interscience, New York, NY, USA, 1987.

[13] K. Hammond, C. Ferdinand, and R. Heckmann. Towards formally verifiable resource bounds for real-time embedded systems. *SIGBED Rev.*, 3(4):27–36, 2006.

[14] H. Herbelin. A λ-calculus structure isomorphic to Gentzen-style sequent calculus structure. In *"Proc. Conf. Computer Science Logic"*, volume 933, pages 61–75. Springer-Verlag, 1994.

[15] M. Hofmann and S. Jost. Static prediction of heap space usage for first-order functional programs. In *POPL03*, pages 185–197. ACM Press, 2003.

[16] G. J. Holzmann. The Model Checker SPIN. *IEEE Transactions on Software Engineering*, 23(5):1–17, May 1997.

[17] G. J. Holzmann and M. H. Smith. A practical method for verifying event-driven software. In *Proc. ICSE99*, pages 597–607, Los Angeles, CA, May 1999.

[18] J. Hughes, L. Pareto, and A. Sabry. Proving the correctness of reactive systems using sized types. In *ACM PoPL*, pages 410–423, 1996.

[19] D. Jackson. Alloy: a lightweight object modelling notation. *Software Engineering and Methodology*, 11(2):256–290, 2002.

[20] A. Lapets and A. Kfoury. Verification with Natural Contexts: Soundness of Safe Compositional Network Sketches. Technical Report BUCS-TR-2009-030, CS Dept., Boston University, October 16 2009.

[21] H.-W. Loidl and K. Hammond. A sized time system for a parallel functional language. In *Proceedings of the Glasgow Workshop on Functional Programming*, Ullapool, Scotland, July 1996.

[22] N. Lynch and M. Tuttle. An introduction to input/output automata. *CWI-Quarterly*, 2(3)(3):219–246, Sept. 1989.

[23] N. Lynch and F. Vaandrager. Forward and backward simulations – part I: Untimed systems. *Information and Computation*, 121(2):214–233, Sept. 1995.

[24] N. Lynch and F. Vaandrager. Forward and backward simulations – part II: Timing-based systems. *Information and Computation*, 128(1):1–25, July 1996.

[25] R. Milner, J. Parrow, and D. Walker. A Calculus of Mobile Processes (Part I and II). *Information and Computation*, (100):1–77, 1992.

[26] L. C. Paulson. *Isabelle: A Generic Theorem Prover*, volume LNCS 828. Springer-Verlag, 1994.

[27] C. A. Petri. *Communication with Automata*. PhD thesis, Univ. Bonn, 1966.

[28] B. Reistad and D. K. Gifford. Static dependent costs for estimating execution time. In *LISP and Functional Programming*, pages 65–78, 1994.

[29] H. Theiling, C. Ferdinand, and R. Wilhelm. Fast and precise wcet prediction by separated cache and path analyses. *Real-Time Syst.*, 18(2-3):157–179, 2000.

[30] E. Tsang. A glimpse of constraint satisfaction. *Artif. Intell. Rev.*, 13(3):215–227, 1999.

[31] E. P. K. Tsang. *Foundations of Constraint Satisfaction.* Academic Press, London and San Diego, 1993.

[32] R. Wilhelm, J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D. Whalley, G. Bernat, C. Ferdinand, R. Heckmann, T. Mitra, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, and P. Stenström. The worst-case execution-time problem—overview of methods and survey of tools. *Trans. on Embedded Computing Sys.*, 7(3):1–53, 2008.