Compositional Controller Synthesis for Vehicular Traffic Networks

Eric S. Kim, Murat Arcak, Sanjit A. Seshia

***Abstract*— We tackle the issue of scalability when synthesizing controllers for large signalized vehicular traffic networks with linear temporal logic specifications. Traffic networks lend themselves to a compositional synthesis approach because they are naturally decomposed into sub-networks. However, naïvely synthesizing controllers for individual sub-networks and interconnecting them can violate the specifications on the monolithic network. By exploiting notions of supply and demand in our system dynamics, we construct contracts between sub-networks that guarantee the soundness of the overall synthesized controller. The resulting decentralized control architecture consists of controllers that rely only on local state information.**

I. INTRODUCTION

Discrete abstraction-based temporal logic controller synthesis for high dimensional systems is hampered by an exponential state explosion arising from the act of partitioning continuous state spaces. A common method to tackle the curse of dimensionality is to synthesize for individual components of a system and stitch them together such that the monolithic system exhibits the desired behavior.

We consider the problem of designing control policies for a network of signalized intersections to satisfy temporal logic specifications [1]. Our fluid-like model of traffic flow is a modified version of the cell transmission model (CTM) [2]. The system has piecewise affine dynamics in each of a finite number of control modes. Flow between network links is characterized by demand, the number of vehicles a link would like to send, and supply, the number of vehicles a link can accept. Congestion arises when there is inadequate downstream supply to fulfill an upstream link's demand. Previously, a control policy for a network of signalized intersections was synthesized by constructing a finite state abstraction of the continuous dynamics [3].

This paper's first contribution is to introduce supply-demand contracts between adjacent sub-networks so that satisfaction of a specification is ensured after a network is partitioned. Given a network partition, the proposed compositional synthesis approach consists of three steps:

1) For pairs of adjacent sub-networks, design agreed upon bounds for supply and demand. A sub-network's own supply-demand bound is a *guarantee* to be satisfied, whereas its *assumption* consists of guarantees from adjacent sub-networks.
2) For each sub-network, encode assumptions on its adjacent sub-networks' behavior by appropriately modifying the dynamics of its finite abstraction, then encode its guarantees in a new temporal logic specification.
3) For each sub-network, individually synthesize control policies enforcing the augmented specification.

To an extent, our supply-demand contracts resemble existing notions of discrete system robustness [4] [5]. Our compositional approach is especially useful if the local specification and control policy change, because adjacent sub-networks' specifications are not inadvertently violated.

This paper's second contribution is a proof that, for a class of traffic network topologies and specifications, the number of initial states for which a control policy can be synthesized is monotonic with respect to the contract parameters. We use this monotonicity property to efficiently search the contract design space and understand tradeoffs between networks.

Cooperative control strategies have previously been investigated in the traffic control literature. Gating, the practice of restricting flow upstream of a set of protected links, was used to prevent over-saturation in a city-scale urban network [6]. Sub-optimal network performance from the lack of coordination between a freeway ramp meter and a local traffic intersection has also been observed in practice [7].

II. TRAFFIC NETWORK MODELING AND SYNTHESIS

A. Notation

For a given set $\mathcal{S}$ we let $|\mathcal{S}|$, $2^{\mathcal{S}}$, $\mathcal{S}\times\mathcal{T}$, and $\mathcal{S}\setminus\mathcal{T}$ respectively denote the cardinality, powerset (set of all subsets), Cartesian product with set $\mathcal{T}$, and the set of elements which are contained in $\mathcal{S}$ and not $\mathcal{T}$. An empty set is represented by $\emptyset$. The terms *upstream* and *downstream* specify the vehicular flow direction; specifically, they flow from upstream to downstream.

B. Network Dynamics

We adopt the signalized network traffic model presented in [3]. A traffic network topology $(\mathcal{L},\mathcal{V})$ consists of a set of *links* $\mathcal{L}$ and a set of *vertices* (or intersections) $\mathcal{V}$. Function $\eta:\mathcal{L}\to\mathcal{V}$ maps a link to its downstream vertex and $\tau:\mathcal{L}\to\mathcal{V}\cup\epsilon$ maps a link to its upstream vertex. By $\tau(l)=\epsilon$ we signify that l has no upstream vertex (see links l_3, l_6 in Fig. 1). Vertex v'sincoming and outgoing links are:

$$\mathcal{L}_v^{\text{in}} := \{l\in\mathcal{L} : \eta(l)=v\} \tag{1}$$

$$\mathcal{L}_v^{\text{out}} := \{l\in\mathcal{L} : \tau(l)=v\}. \tag{2}$$

This work was supported in part by NSF grant CNS-1446145, the NSF Graduate Research Fellowship Program, NSF Expeditions grant CCF-1139138 and by STARnet, a Semiconductor Research Corporation program, sponsored by MARCO and DARPA.

The authors are with the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley. {eskim, arcak, sseshia}@eecs.berkeley.edu

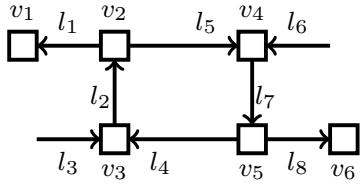

Fig. 1: Example network with $\mathcal{L} = \{l_1, \ldots, l_8\}$ and $\mathcal{V} = \{v_1, \ldots, v_6\}$. Link l_4's downstream and upstream vertices are $\eta(l) = v_3$ and $\tau(l) = v_5$. Vertex v_5 has $\mathcal{L}^{\text{in}}_{v_5} = \{l_7\}$ and $\mathcal{L}^{\text{out}}_{v_5} = \{l_4, l_8\}$ Link l_4 has $\mathcal{L}^{\text{up}}_{l_4} = \{l_7\}$, $\mathcal{L}^{\text{down}}_{l_4} = \{l_2, l_4\}$, and $\mathcal{L}^{\text{adj}}_{l_4} = \{l_8\}$. The network has input/output sets $\mathcal{I} = \{l_3, l_6\}$ and $\mathcal{O} = \{l_1, l_8\}$.

Link l's upstream, downstream, adjacent, and local links are:

$$\mathcal{L}^{\text{up}}_l := \{j \in \mathcal{L} : \tau(l) = \eta(j)\} \tag{3}$$

$$\mathcal{L}^{\text{down}}_l := \{l\} \cup \{k \in \mathcal{L} : \eta(l) = \tau(k)\} \tag{4}$$

$$\mathcal{L}^{\text{adj}}_l := \mathcal{L}^{\text{out}}_{\tau(l)} \setminus \{l\} \tag{5}$$

$$\mathcal{L}^{\text{loc}}_l := \mathcal{L}^{\text{up}}_l \cup \mathcal{L}^{\text{down}}_l \cup \mathcal{L}^{\text{adj}}_l. \tag{6}$$

The input links $\mathcal{I} = \{l \in \mathcal{L} : \mathcal{L}^{up}_l = \emptyset\}$ serve as entry points to the network. Likewise, the output links $\mathcal{O} = \{l \in \mathcal{L} : \mathcal{L}^{down}_l \setminus \{l\} = \emptyset\}$ serve as exit points from the network.

Each link l has a *maximum capacity* $x^{\text{cap}}_l \in \mathbb{R}_{\geq 0}$ and an associated *link occupancy* $x_l[t] \in [0, x^{\text{cap}}_l]$ at a discrete time $t \in \mathbb{Z}_{\geq 0}$. The state space of the traffic network is thus

$$\mathcal{X} := \prod_{l \in \mathcal{L}} [0, x^{\text{cap}}_l] \subset \mathbb{R}^{|\mathcal{L}|}. \tag{7}$$

Vehicles flow from upstream links, through a vertex, to downstream links. A link's *demand* represents the amount of vehicles it would like to send to downstream links. The demand function is upper bounded by a *saturation flow* c_l determined by, e.g, speed limits or road width. Link l's demand function $\Phi_l : [0, x^{\text{cap}}_l] \to [0, c_l]$ is defined as

$$\Phi_l(x_l[t]) := \min(x_l[t], c_l). \tag{8}$$

A link's demand is split by a parameter $\beta_{lk} \in [0, 1]$ that denotes the fraction of link l's total outflow that enters downstream link k. Intuitively,

$$\sum_{k \in \mathcal{L}^{\text{down}}_l \setminus \{l\}} \beta_{lk} \leq 1, \tag{9}$$

where $\beta_{lk} \neq 0$ only if $k \in \mathcal{L}^{\text{down}}_l \setminus \{l\}$ and strict inequality occurs when some vehicles exit to unmodeled links.

A link is *actuated* if the traffic signal permits outward flow from the link. The network controls vehicular flow by choosing a set of actuated links $u[t] \in \mathcal{U}$ at each time step. The set of all control actions $\mathcal{U} \subset 2^{\mathcal{L}}$ is restricted by considering the set of available signal configurations at each intersection. At intersection v a signal configuration u_v is a set of actuated incoming links $u_v \in 2^{\mathcal{L}^{\text{in}}_v}$. Intersection v_3 in Fig. 1 for instance has some subset of $\{\emptyset, \{l_3\}, \{l_4\}, \{l_3, l_4\}\}$ as its available configurations.

A link's *supply* represents the maximum number of vehicles a link can accept from upstream. We define link l's supply function $\Psi : [0, x^{\text{cap}}_l] \to [0, x^{\text{cap}}_l]$ as

$$\Psi_l(x_l[t]) := x^{\text{cap}}_l - x_l[t]. \tag{10}$$

The supply parameters $\alpha^{u_v}_{lk}$ denotes the capacity available to l from link k given the signal configuration u_v of vertex $v := \tau(k) = \eta(l)$. The supply is split amongst upstream links, so for all $u_v \in 2^{\mathcal{L}^{\text{in}}_v}$,

$$\sum_{k \in \mathcal{L}^{\text{up}}_l} \alpha^{u_v}_{kl} = 1. \tag{11}$$

If $l \notin u[t]$, then the flow out of link l, f^{out}_l, is given by

$$f^{\text{out}}_l(x^{\text{down}}_l[t], u[t]) = 0. \tag{12}$$

If $l \in u[t]$, then

$$\begin{aligned} &f^{\text{out}}_l(x^{\text{down}}_l[t], u[t]) \\ &= \min\left\{x_l[t], c_l, \min_{k \in \mathcal{L}^{\text{down}}_l \setminus \{l\}} \left\{\tfrac{\alpha_{lk}}{\beta_{lk}}(x^{\text{cap}}_k - x_k[t])\right\}\right\}. \end{aligned} \tag{13}$$

The minimization in (13) indicates that link l's outflow cannot exceed the current occupancy, the saturation flow, or the supply provided from downstream links. The third term in the outer minimization disappears for output links; this is effectively identical to assuming infinite supply outside the network. The flow f^{out}_l is strictly a function of $\{x_k[t]\}_{k \in \mathcal{L}^{\text{down}}_l}$, so f^{out}_l is a function of x^{down}_l in (13).

The evolution of a link's occupancy depends on local links and follows a conservation of mass equation

$$\begin{aligned} x_l[t+1] &= F_l(x^{\text{loc}}_l[t], u[t], d_l[t]) \\ &= \min\Big\{x^{\text{cap}}_l, x_l[t] - f^{\text{out}}_l(x^{\text{down}}_l[t], u[t]) \\ &\quad + \sum_{j \in \mathcal{L}^{\text{up}}_l} \beta_{jl} f^{\text{out}}_j(x^{\text{down}}_j[t], u[t]) + d_l[t]\Big\} \end{aligned} \tag{14}$$

where $d_l[t] \in \mathcal{D}_l$ is an exogenous flow entering link l at time t and $\mathcal{D}_l \subseteq [0, x^{\text{cap}}_l]$. A network-wide state update equation encompasses the dynamics from (13) and (14):

$$\begin{aligned} x[t+1] &= F(x[t], u[t], d[t]) \\ u[t] &\in \mathcal{U}, \quad d[t] \in \mathcal{D} := \mathcal{D}_1 \times \ldots \times \mathcal{D}_{|\mathcal{L}|}. \end{aligned} \tag{15}$$

We succinctly represent our traffic network model as a tuple $\mathcal{N} := (\mathcal{L}, \mathcal{V}, \mathcal{X}, \mathcal{U}, \mathcal{D}, F)$.

C. Finite State Abstraction

We partition the continuous state space $\mathcal{X}$ into a rectangular grid and compute a finite state abstraction of the continuous dynamics. The finite set of partitions is denoted as $\mathbb{X}$. Each partition of the continuous space exactly corresponds with a single state in the finite abstraction; thus, we refer to the two interchangeably. We construct an *approximate quotient transition system* [3] (or simply *finite abstraction*) of $\mathcal{N}$'s continuous dynamics.

Definition 1. *Network $\mathcal{N}$ has approximate quotient transition system $\mathbb{S} := (\mathbb{X}, \mathcal{U}, \mapsto)$ where $\mathbb{X}$ is a set of discrete*

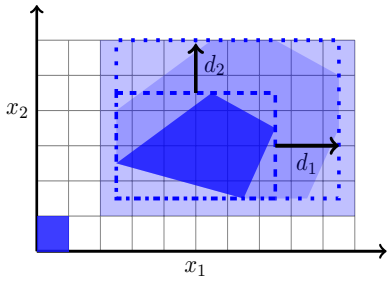

Fig. 2: Illustration of finite over-approximation construction.

states, $\mathcal{U}$ is a finite set of control actions, and $\mapsto \subseteq \mathbb{X} \times \mathcal{U} \times \mathbb{X}$ is a transition relation that satisfies the following:

$$\text{if } \exists d \in \mathcal{D}, \exists x \in p \text{ such that } F(x,u,d) \in p'$$
$$\text{then } (p,u,p') \in \mapsto$$

Transition relation $\mapsto$ in Definition 1 is an over-approximation because it permits transitions that may not be possible in the underlying continuous dynamics. As explained in Section II-E, our synthesis procedure accounts for these spurious transitions.

The traffic model above is amenable to a scalable method for computing over-approximated transition relations without polytope set operations [8], which we illustrate in Fig. 2. From a partition (lower left box), there exists a true reachable set without and with additive disturbances (solid and translucent polytopes). We efficiently compute tight rectangular over-approximations (dashed and dotted outlines) of these reachable sets and over-approximate the set of next possible partitions (translucent box) by checking for intersections with the dotted box. The efficiency in the reachability computation arises from the fact that rectangular boxes are characterized by two corner points (see [8] for further details).

D. Linear Temporal Logic

We denote regions of interest by introducing a labeling function $L : \mathcal{X} \to 2^{AP}$ that specifies which *atomic propositions* in a set AP hold at a given point. For instance, all points in the region $\{x \in \mathcal{X} : x_{l_1} \leq 10\}$ can satisfy the atomic proposition "low occupancy in l_1". Obtaining the discrete labeling function $L : \mathbb{X}_n \to 2^{AP}$ must be done with care to respect the partition and the specification to be satisfied. For example, when a label b signifies a region to be avoided we conservatively assign b to partition/finite state p if there exists an $x \in p$ such that $b \in L(x)$.

We express the specifications in linear temporal logic (LTL) [1], which operates on these atomic propositions and introduces temporal operators $\bigcirc$ (next) and $\cup$ (until) in addition to the Boolean operators $\wedge$ (conjunction), $\vee$ (disjunction), and $\neg$ (negation). From these operators, we can also derive additional Boolean operator $\rightarrow$ (implies) and temporal operators $\Box$ (always) and $\Diamond$ (eventually). Traffic networks are a natural domain for LTL specifications e.g.,

- $\Box\Diamond(x_1 \leq C \wedge x_2 \leq C)$
  "It is always true that at some future time links l_1, l_2 both contain no more than C vehicles. "
- $(x_1 \leq C_1) \cup \neg(x_2 \geq C_2)$
  "Link l_1 will have low occupancy until link l_2 is no longer congested"

E. LTL Controller Synthesis

The objective in LTL controller synthesis is to find a finite memory control policy $\mathcal{C} : \mathbb{X}^* \to \mathcal{U}$ so that a LTL specification ϕ is satisfied. We only state key points about the LTL controller synthesis procedure, and refer the reader to [3][9] for a more details. The non-determinism in the translation relation $\mapsto$ is viewed as an adversarial environment who seeks to prevent satisfaction of ϕ. We solve a non-deterministic game to obtain the (possibly empty) largest set of initial states for which there exists a satisfying control policy, as well as the policy itself. A returned policy enforces satisfaction of ϕ in spite of the non-deterministic transitions and over-approximations included in the construction of $\mapsto$.

III. Supply-Demand Contracts

A. Compositional Synthesis

We decompose the network into *sub-networks* and synthesize controllers for each individually. Upon interconnection, a downstream network's input links can impede flow from an upstream network's output links. We enforce cooperation between sub-networks to account for this dynamic coupling. Each sub-network requests that the demand and supply from adjacent networks remain in agreed upon intervals, and accounts for this uncertainty by modifying its finite abstraction's transition relation. We then synthesize controllers for each sub-network to satisfy its original specifications and promises to adjacent sub-networks.

B. Network Decomposition

Let the set of links $\mathcal{L}$ and signalized intersections $\mathcal{V}$ be partitioned into N nonempty subsets $\{\mathcal{L}_1, \ldots, \mathcal{L}_N\}$ and $\{\mathcal{V}_1, \ldots, \mathcal{V}_N\}$, and let $\mathcal{N}_n$ denote the nth sub-network. The link partition implicitly yields new sets of continuous and discrete states $\mathcal{X}_n$ and $\mathbb{X}_n$ and the vertex partition yields a control action set $\mathcal{U}_n$. To simplify our analysis, network partitions must satisfy the following assumptions:

Assumption 1. *$\mathcal{N}_n$ is weakly connected. That is, after removing the edge directions in the network's underlying graph, there exists a path from any link or vertex to any other link or vertex.*

Assumption 2. *All $v \in \mathcal{V}_n$ must have incoming links that are only in $\mathcal{L}_n$.*

Assumption 3.

$$\phi^{original} := \bigwedge_{n \in \{1,\ldots,N\}} \phi_n^{original} \tag{16}$$

Additionally, each $\phi_n^{original}$ cannot contain atomic propositions that depend on the state of a link in other sub-networks.

Assumption 2 serves only to set a convention for the decomposition and is not restrictive. Assumption 3 requires

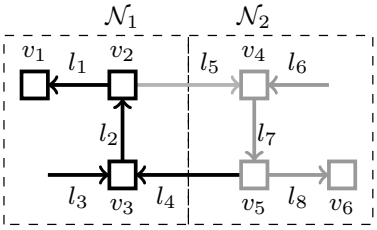

Fig. 3: Network from Fig. 1 partitioned into two sub-networks $\mathcal{N}_1 = (\{l_1, \ldots, l_4\}, \{v_1, v_2, v_3\})$ and $\mathcal{N}_2 = (\{l_5, \ldots, l_8\}, \{v_4, v_5, v_6\})$. $\mathcal{N}_1$ has interfacing links $\mathcal{I}_1 = \{l_4\}$ and $\mathcal{O}_1 = \{l_2\}$, and adjacent upstream/downstream links $\mathcal{A}_1^{\text{up}} = \{l_7\}$ and $\mathcal{A}_1^{\text{down}} = \{l_5\}$. The set of interconnecting vertices is $\{v_2, v_5\}$. $\mathcal{N}_1$ is upstream from $\mathcal{N}_2$ at v_2 but is downstream from $\mathcal{N}_2$ at v_5.

that the specification on the monolithic network ϕ^{original} is a conjunction of sub-specifications for each sub-network.

The *interfacing input (output) links* in sub-network $\mathcal{N}_n$ are links with upstream (downstream) links not contained in $\mathcal{L}_n$:

$$\mathcal{I}_n = \{l \in \mathcal{L}_n : \mathcal{L}_l^{\text{up}} \setminus \mathcal{L}_n \neq \emptyset\} \tag{17}$$

$$\mathcal{O}_n = \{l \in \mathcal{L}_n : \mathcal{L}_l^{\text{down}} \setminus \mathcal{L}_n \neq \emptyset\}. \tag{18}$$

Network $\mathcal{N}_n$ has a set of *adjacent upstream links* $\mathcal{A}_n^{\text{up}} \subset \mathcal{L} \setminus \mathcal{L}_n$ and *downstream links* $\mathcal{A}_n^{\text{down}} \subset \mathcal{L} \setminus \mathcal{L}_n$ that lie in other networks:

$$\mathcal{A}_n^{\text{up}} = \bigcup_{l \in \mathcal{I}_n} \mathcal{L}_l^{\text{up}} \tag{19}$$

$$\mathcal{A}_n^{\text{down}} = \bigcup_{l \in \mathcal{O}_n} (\mathcal{L}_l^{\text{down}} \setminus \mathcal{L}_n). \tag{20}$$

These sets comprise the outside links to which a sub-network has a supply or demand obligation; $\mathcal{N}_n$ guarantees it will: 1) provide adequate supply to links in $\mathcal{A}_n^{\text{up}}$, and 2) not introduce unreasonably high demand to links in $\mathcal{A}_n^{\text{down}}$.

A vertex $v \in \mathcal{V}$ is an *interconnecting vertex* if it contains incoming and outgoing links in two different sub-networks, that is, there exist distinct network indices $\overline{v}, \underline{v} \in \{1, \ldots, N\}$ such that $\mathcal{L}_v^{\text{in}} \cap \mathcal{L}_{\overline{v}} \neq \emptyset$ and $\mathcal{L}_v^{\text{out}} \cap \mathcal{L}_{\underline{v}} \neq \emptyset$. At v, sub-network $\mathcal{N}_{\overline{v}}$ is the *upstream sub-network* and sub-network $\mathcal{N}_{\underline{v}}$ is a *downstream sub-network*. There may be multiple downstream sub-networks $\mathcal{N}_{\underline{v}_1}, \ldots, \mathcal{N}_{\underline{v}_m}$ corresponding to each $\underline{v}_i, i = 1, \ldots, m$, such that $\mathcal{L}_v^{\text{out}} \cap \mathcal{L}_{\underline{v}_i} \neq \emptyset$. Note that a sub-network can be both upstream and downstream at different interconnecting vertices (see Fig. 3).

The supply and demand parameters between links in different sub-networks are not explicitly included in the dynamics for the individual sub-networks, but arise in the subsequent definitions for supply-demand contracts.

C. Supply Contracts

At an interconnecting vertex v, the upstream network $\mathcal{N}_{\overline{v}}$ requests that all downstream networks $\mathcal{N}_{\underline{v}_i}$ provide a minimum supply $\sigma_l^{\text{contract}} \geq 0$ to the output link $l \in \mathcal{O}_{u^v}$.

Definition 2. *Downstream sub-network $\mathcal{N}_{\underline{v}_i}$ fulfills its supply contract to upstream link l at time t if $\mathcal{N}_{\underline{v}_i}$'s state $x[t]$ satisfies:*

$$\sigma_l^{contract} \leq \alpha_{lk}^{u_v}(x_k^{cap} - x_k[t]) \tag{21}$$

for all $k \in \mathcal{L}_l^{down} \cap \mathcal{L}_{\underline{v}_i}$ and all signal configurations u_v. An upper bound on the available supply to link l is $\sigma_l^{best} = \min_{k \in \mathcal{L}_l^{down} \cap \mathcal{L}_{\underline{v}_i}} \alpha_{lk} x_k^{cap}$.

We accordingly modify (13) to reflect the outflow assumption $\mathcal{N}_{\overline{v}}$ makes from the supply contract.

Proposition 1. *If all downstream sub-networks $\mathcal{N}_{\underline{v}_i}$ fulfill their supply contracts to upstream link $l \in \mathcal{O}_{\overline{v}}$ for all t, then l's outflow satisfies:*

$$\begin{aligned} &f_l^{out}(x_l^{down}[t], u[t]) \\ &\in \Bigg\{ \min\Bigg\{ x_l[t], c_l, \min_{k \in \mathcal{L}_l^{down} \cap \mathcal{L}_{\overline{v}}} \left\{ \frac{\alpha_{lk}}{\beta_{lk}}(x_k^{cap} - x_k[t]) \right\}, \frac{\sigma}{\beta_{lk}} \Bigg\} \\ &: \sigma \in [\sigma_l^{contract}, \sigma_l^{best}] \Bigg\} \end{aligned} \tag{22}$$

when $l \in u[t]$. If $l \notin u[t]$, then $f_l^{out}(x_l^{down}[t], u[t]) = 0$.

D. Demand Contracts

At interconnecting vertex v, a downstream network $\mathcal{N}_{\underline{v}_i}$ can request that upstream network $\mathcal{N}_{\overline{v}}$ impose a maximum demand, $\delta_k^{\text{contract}} \geq 0$, it may introduce to input link $k \in \mathcal{I}_{\underline{v}_i}$.

Definition 3. *Upstream sub-network $\mathcal{N}_{\overline{v}}$ fulfills its demand contract to downstream link $k \in \mathcal{I}_{\underline{v}_i}$ at time t if $\mathcal{N}_{\overline{v}}$'s state $x[t]$ satisfies:*

$$\forall u[t] \in \mathcal{U}_{\overline{v}} \sum_{j \in \mathcal{L}_k^{up} \cap \mathcal{L}_{\overline{v}} \cap u} \beta_{jk} f_j^{out}(x[t], u[t]) \leq \delta_k^{contract}. \tag{23}$$

We replace the update equation (14) with (24) below.

Proposition 2. *If upstream sub-network $\mathcal{N}_{\overline{v}}$ fulfills its demand contract to downstream link $k \in \mathcal{I}_{\underline{v}_i}$ for all t, then link k's future state satisfies:*

$$\begin{aligned} &x_k[t+1] \\ &\in [0, x_k^{cap}] \cap \Bigg\{ \begin{array}{l} x_k[t] - f_k^{out}(x_k^{down}[t], u[t]) \\ + \sum_{j \in \mathcal{L}_k^{up} \cap \mathcal{L}_{\underline{v}_i}} \beta_{jk} f_j^{out}(x_j^{down}[t], u[t]) \\ + \Delta_k + \delta \end{array} \\ &\qquad : d_k \in \mathcal{D}_k, \delta \in [0, \delta_k^{contract}] \Bigg\}. \end{aligned} \tag{24}$$

In (24) all of the additions are scalar Minkowski set additions because the f^{out} terms may be sets as in (22).

E. Modified Synthesis Procedure

We concatenate a sub-network's supply-demand assumptions and guarantees into a set of four vectors. Sub-network $\mathcal{N}_n$ makes supply and demand requests on behalf of its interfacing output and input links, respectively, which we encode in the vectors $\Sigma_n \in \mathbb{R}^{|\mathcal{O}_n|}$ and $\Delta_n \in \mathbb{R}^{|\mathcal{I}_n|}$. Dually, $\mathcal{N}_n$ must fulfill its supply-demand obligations to adjacent upstream and downstream links; these obligations

are encoded in vectors $\tilde{\Sigma}_n \in \mathbb{R}^{|\mathcal{A}_n^{\text{up}}|}$ and $\tilde{\Delta}_n \in \mathbb{R}^{|\mathcal{A}_n^{\text{down}}|}$. All elements in vectors $\Sigma_1, \tilde{\Sigma}_1, \ldots, \Sigma_N, \tilde{\Sigma}_N$ are from the set of all supply contract parameters $\{\sigma_l^{\text{contract}} : l \in \mathcal{L}\}$ and likewise for $\Delta_1, \tilde{\Delta}_1, \ldots, \Delta_N, \tilde{\Delta}_N$.

1) Modified Dynamics Under Contract Assumptions: Assuming all adjacent networks fulfill the supply-demand requests from $\mathcal{N}_n$, we use (22) and (24) to construct a finite abstraction $\mathbb{S}(\Sigma_n, \Delta_n)$.

Definition 4. *Sub-network $\mathcal{N}_n$ has approximate quotient transition system $\mathbb{S}(\Sigma_n, \Delta_n) := (\mathbb{X}_n, \mathcal{U}_n, \mapsto_{(\Sigma_n, \Delta_n)})$ where $\mathbb{X}_n$ and $\mathcal{U}_n$ are defined similar to Definition 1, and $\mapsto_{(\Sigma_n, \Delta_n)} \subseteq \mathbb{X}_n \times \mathcal{U}_n \times \mathbb{X}_n$ is an over-approximating transition relation that respects the dynamical constraints (22) and (24).*

2) Guaranteeing Contract Fulfillment: By encoding contract satisfaction in the LTL specification, each sub-network is guaranteed to fulfill its requests from adjacent sub-networks. To encode fulfillment of $\mathcal{N}_n$'s supply and demand obligations as given in Definitions 2 and 3, we introduce the new atomic propositions $\chi_n^{\text{supply}}(\tilde{\Sigma}_n)$ and $\chi_n^{\text{demand}}(\tilde{\Delta}_n)$ and updated alphabet $AP_{\text{new}} := AP \cup \chi_n^{\text{supply}}(\tilde{\Sigma}_n) \cup \chi_n^{\text{demand}}(\tilde{\Delta}_n)$. We introduce a new specification ϕ^{new} for the monolithic network of the form

$$\phi^{\text{new}} := \bigwedge_{n \in \{1,\ldots,N\}} \phi_n^{\text{new}} \tag{25}$$

$$\phi_n^{\text{new}} := \phi_n^{\text{original}} \wedge \phi_n^{\text{contract}}(\tilde{\Sigma}_n, \tilde{\Delta}_n) \tag{26}$$

$$\phi_n^{\text{contract}}(\tilde{\Sigma}_n, \tilde{\Delta}_n) := \Box \chi_n^{\text{supply}}(\tilde{\Sigma}_n) \wedge \Box \chi_n^{\text{demand}}(\tilde{\Delta}_n), \tag{27}$$

which allows us to synthesize a $\mathcal{C}_n$ for each individual $\mathcal{N}_n$.

If satisfying controllers are synthesized for each sub-network under these assumptions, then the entire network meets the original specification because $\phi^{\text{new}} \rightarrow \phi^{\text{original}}$. Failure to synthesize a cooperative control policy for even one sub-network invalidates the assumptions for all adjacent sub-networks the contract parameters need to be revised.

IV. Example

We synthesize control policies for two sub-networks depicted in Fig. 4 $\mathcal{N}_1$'s behavior defaults to maximizing flow through the primary links l_0, l_2, l_4. If secondary link l_1 is actuated, then 30% of l_2's supply is allocated to l_1. Through a partitioning that is more granular for states with lower link occupancy, $\mathcal{N}_1$'s abstraction has 57,344 discrete states and its LTL specification simply ensures that ramps don't persistently overflow:

$$\phi_1^{\text{original}} := \bigwedge_{i=1,3} \Box\Diamond(x_{l_i} \leq 20). \tag{28}$$

A smaller capacity sub-network $\mathcal{N}_2$ flows into l_1. Its objective is to prevent saturation of links l_5, l_6 and l_8:

$$\phi_2^{\text{original}} := \Box\Diamond(x_{l_6} \leq 12) \wedge \bigwedge_{i=5,8} \Box\Diamond(x_{l_i} \leq 15). \tag{29}$$

$\mathcal{N}_2$'s abstraction contains 54,000 discrete states. We were unable to construct an abstraction of the monolithic network, which would consist of roughly 3.1 billion states, on a laptop with 8 GB memory and 2.4 GHz Intel Core i7 processor.

Sub-network $\mathcal{N}_1$ parameters:

$(x_{l_0}^{\text{cap}}, \ldots, x_{l_4}^{\text{cap}}) = (80, 40, 80, 24, 80)$

$(c_{l_0}, \ldots, c_{l_4}) = (30, 15, 29, 12, 30)$

$\mathcal{D}_1 := \{d : 0 \leq d \leq [10, 0, 0, 3, 0]\}$

$\beta_{02} = \beta_{24} = 0.8,\ \beta_{12} = \beta_{34} = 1.0,$

$u_{v_0} \in \{\{l_0\}, \{l_0, l_1\}\}, \quad u_{v_1} \in \{\{l_2\}, \{l_2, l_3\}\}$

If l_1 actuated, then $\alpha_{02} = 0.7, \alpha_{12} = 0.3$

If l_3 actuated, then $\alpha_{24} = 0.7, \alpha_{34} = 0.3$

Otherwise $\alpha_{02} = \alpha_{24} = 1$

Sub-network $\mathcal{N}_2$ parameters:

$(x_{l_5}^{\text{cap}}, \ldots, x_{l_8}^{\text{cap}}) := (30, 18, 30, 30)$

$(c_{l_5}, \ldots, c_{l_8}) := (12, 6, 14, 14)$

$\mathcal{D}_2 := \{d : 0 \leq d \leq [4, 3, 0, 3]\}$

$u_{v_3} \in \{\{l_5\}, \{l_6\}\}, \quad u_{v_4} \in \{\{l_7\}, \{l_8\}\}$

$\beta_{57} = \beta_{67} = 1$

Link l_7's supply is allocated to the link actuated by v_3.

Inter-network flow parameters:

$\beta_{71} = \beta_{81} = .8$

Link l_1's supply is allocated to link actuated by v_4.

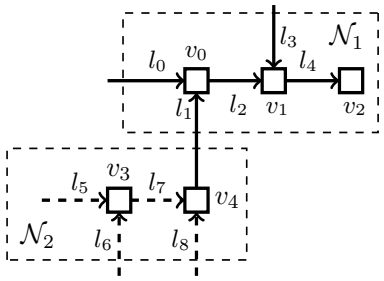

Fig. 4: Two sub-networks $\mathcal{N}_1, \mathcal{N}_2$. Dashed arrows are links in $\mathcal{N}_2$.

Sub-network $\mathcal{N}_2$ assumes (Σ_2) that $\mathcal{N}_1$ fulfills its obligation ($\tilde{\Sigma}_1$) of ensuring adequate supply from l_1. Likewise, $\mathcal{N}_1$ assumes (Δ_1) that $\mathcal{N}_2$ fulfills its obligation ($\tilde{\Delta}_2$) of limiting demand from l_7, l_8. Thus,

$$\Delta_1 = \delta_{l_1}^{\text{contract}} = 10 = \tilde{\Delta}_2 \tag{30}$$

$$\tilde{\Sigma}_1 = \sigma_{l_7}^{\text{contract}} = \sigma_{l_8}^{\text{contract}} = 9 = \Sigma_2, \tag{31}$$

where the next section describes the methodology for identifying the numerical values of these parameters. These parameters translate to contract atomic propositions:

$$\chi_1^{\text{supply}}(\tilde{\Sigma}_1) = \{x \in \mathcal{X}_1 : x_{l_1} \leq 31\} \tag{32}$$

$$\chi_1^{\text{demand}}(\tilde{\Delta}_1) = \text{True} \tag{33}$$

$$\chi_2^{\text{supply}}(\tilde{\Sigma}_2) = \text{True} \tag{34}$$

$$\chi_2^{\text{demand}}(\tilde{\Delta}_2) = \{x \in \mathcal{X}_2 : x_{l_7} \leq 12.5 \wedge x_{l_8} \leq 12.5\}. \tag{35}$$

Synthesizing control policies for $\mathcal{N}_1$ and $\mathcal{N}_2$ each took approximately 11 minutes and example trajectories are shown in Fig. 5.

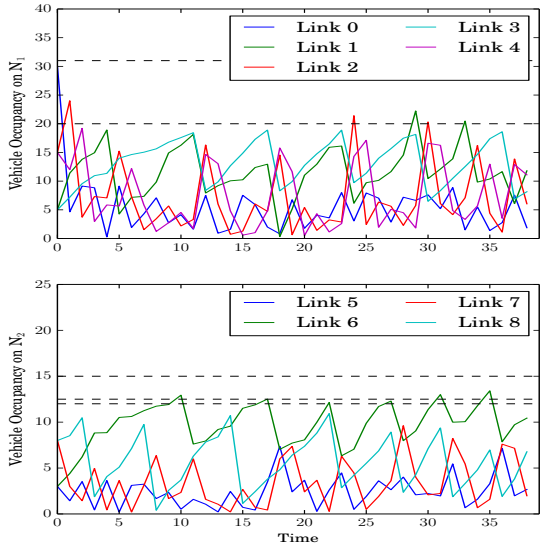

Fig. 5: Trajectories on both example sub-networks. Dashed lines highlight important occupancy levels appearing in the specification.

V. Contract Parameter Monotonicity

Identifying appropriate supply and demand contract parameters may be difficult because they affect a sub-network's ability to satisfy a specification. Both parameters present a tradeoff between being able to synthesize for a sub-network at the expense of adjacent ones. The next two subsections formalize the following informal statements:

A. "Making obligations to adjacent sub-networks less stringent makes controller synthesis easier."

B. "Increased exogenous demand or reduced supply availability from adjacent sub-networks makes controller synthesis harder."

Statement A holds for general networks and specifications, but Statement B holds for a specific class of networks and associated specifications.

A. Loosened Obligations

Let $\mathbb{S}(\Sigma_n, \Delta_n)$ be a given finite state abstraction and $\phi_n^{\text{contract}}(\tilde{\Sigma}_n, \tilde{\Delta}_n)$, $\phi_n^{\text{contract}}(\tilde{\Sigma}'_n, \tilde{\Delta}'_n)$ be two different sets of contract obligations. Let $\tilde{\Sigma}'_n \leq \tilde{\Sigma}_n$ and $\tilde{\Delta}'_n \geq \tilde{\Delta}_n$ elementwise, meaning the obligation $\phi_n^{\text{contract}}(\tilde{\Sigma}'_n, \tilde{\Delta}'_n)$ is more stringent than obligation $\phi_n^{\text{contract}}(\tilde{\Sigma}_n, \tilde{\Delta}_n)$. For a given initial state, suppose there exists a sequence of control actions $u = u_0 u_1 u_2 \dots$ such that $\phi_n^{\text{contract}}(\tilde{\Sigma}'_n, \tilde{\Delta}'_n)$ is satisfied. Then that control sequence must satisfy $\phi_n^{\text{contract}}(\tilde{\Sigma}_n, \tilde{\Delta}_n)$ as well because $\phi_n^{\text{contract}}(\tilde{\Sigma}_n, \tilde{\Delta}_n) \to \phi_n^{\text{contract}}(\tilde{\Sigma}'_n, \tilde{\Delta}'_n)$.

B. Less Cooperative Adjacent Sub-Networks

We first present the preliminaries before proving Statement B above. A partition has lower occupancy than another via a partial order $\leq_{\mathbb{X}_n}$ on $\mathbb{X}_n$; $p \leq_{\mathbb{X}_n} p_{\text{h}}$ if and only if there exists $x_{\text{h}} \in p_{\text{h}}$ such that $x \leq x_{\text{h}}$ elementwise for all $x \in p$. Recall that $p \in \mathbb{X}_n$ acts both as a partition of continuous space $\mathcal{X}$ and as a discrete state of abstraction $\mathbb{S}(\Sigma_n, \Delta_n)$.

Definition 5. *A subset $\mathbb{P} \subseteq \mathbb{X}_n$ is a lower set if $p_h \in \mathbb{P}$ and $p \leq_{\mathbb{X}_n} p_h$ imply $p \in \mathbb{P}$.*

Lower sets prevent specifications from encouraging high occupancy and $\mathbb{G}$ in Fig. 7 is an example. We consider the following set of specifications:

$$\phi_n^{\text{original}} := \square\theta \wedge \lozenge\square\gamma \wedge \bigwedge_{i=1,\dots,L} \square\lozenge\nu_i \wedge \bigwedge_{i=1,\dots,M} \lozenge\kappa_i \quad (36)$$

where L and M are non-negative integers and atomic propositions θ, γ, ν_i, and κ_i are true for lower sets of $\mathbb{X}_n$. We restrict ourselves to a monolithic network and sub-networks with no diverging intersections, i.e. for every intersection $v \in \mathcal{V}$, the set $\mathcal{L}_v^{\text{out}}$ is empty or a singleton. This structural assumption ensures that the network exhibits *monotone* dynamics [8] and contract atomic propositions $\chi_n^{\text{supply}}(\tilde{\Sigma}_n)$ and $\chi_n^{\text{demand}}(\tilde{\Delta}_n)$ hold on lower sets of $\mathbb{X}_n$. Monotone systems maintain a partial ordering on states [10]. In traffic networks, monotone dynamics ensure that "higher occupancy now, higher demand, and lower supply imply higher vehicular occupancy later". Diverging intersections violate monotonicity because congestion in one link restricts upstream flow and reduces occupancy on adjacent links.

We consider two different sets of supply-demand requests that sub-network $\mathcal{N}_n$ can make to adjacent networks, (Σ'_n, Δ'_n) and (Σ_n, Δ_n). We let

$$\Sigma'_n \leq \Sigma_n \text{ and } \Delta'_n \geq \Delta_n \text{ elementwise} \quad (37)$$

and refer to $\mathbb{S}(\Sigma_n, \Delta_n)$ as a *nominal sub-network* and $\mathbb{S}(\Sigma'_n, \Delta'_n)$ as a *stressed sub-network* that experiences increased demand and reduced supply.

Due to space constraints, we omit a formal proof of Statement B but provide a visual explanation in Fig. 6 and 7. The main technical difficulties are 1) the non-determinism in the finite abstraction's transition relation, 2) how to relate the outputs of the synthesis procedure for the stressed and nominal networks. We solve these issues by focusing on the worst case behaviors of both networks. If the worst case behavior of the stressed network satisfies (36), then the nominal network should satisfy it as well. Fig. 6 illustrates some properties on transition relation $\mapsto_{(\Sigma_n, \Delta_n)}$. Let $\mathbb{P}_t^u$ denote the set of possible states for $\mathbb{S}(\Sigma_n, \Delta_n)$ at time t under given control sequence $u = u_0 \dots u_{t-1}$. A *behavior* of $\mathbb{S}(\Sigma_n, \Delta_n)$ is a sequence of states $\rho_u = p_0 \dots p_t$ such that $p_i \in \mathbb{P}_i^u$ for all $i = 0, \dots, t$, and a *worst* element x of a set $\mathbb{P} \subseteq \mathbb{X}_n$ is an element such that no $p \in \mathbb{P} \backslash \{x\}$ satisfies $x \leq_{\mathbb{X}_n} p$.

Property 1. *Each set of next reachable states has a unique worst element. In Fig. 6a, $worst(\mathbb{P}_1^{u'}) = p'_1$.*

Property 2. *A stressed sub-network has a "worse" set of reachable states in the sense that $worst(\mathbb{P}_1^u) \leq_{\mathbb{X}_n} worst(\mathbb{P}_1^{u'})$ in Fig. 6a.*

Property 3. *Starting from a worse initial state makes the set of next reachable states worse, e.g. in Fig. 6b, $worst(\mathbb{P}_1^u) \leq_{\mathbb{X}_n} worst(\mathbb{P}_1^{u'})$.*

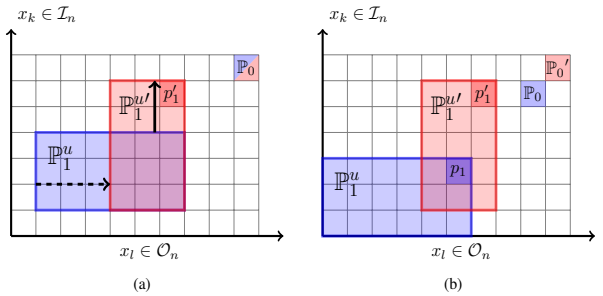

Fig. 6: (a) $\mathbb{P}_1^{u\prime}$ (red) is obtained by deforming $\mathbb{P}_1^u$ (blue). Decreased supply for output link x_l prunes (dashed arrow) the leftmost elements of $\mathbb{P}_1$, and increased demand on input link x_k appends (solid arrow) elements on top of $\mathbb{P}_1$. (b) Worse initial states have worse reachable sets.

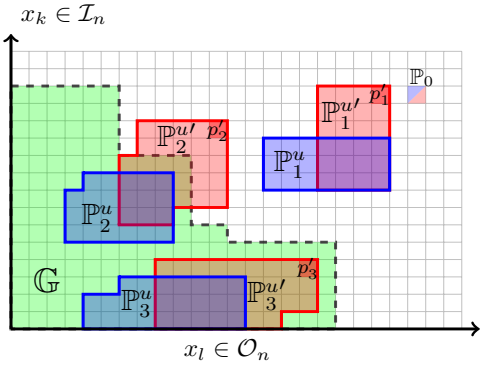

Fig. 7: Illustration of Property 3 for some control sequence u.

Property 1 holds because the abstraction procedure in Section II-C computes rectangular reachable sets, while properties 2 and 3 follow from the traffic network's monotone dynamics. Property 3 is used to generalize properties 1 and 2 from one step reachable sets to a worst case behavior $p_u = p_1' p_2' p_3' \ldots$ in Fig. 7.

Suppose that from some initial state, a control sequence $u = u_0 \ldots u_{t-1}$ exists such that the stressed subnetwork's worst case behavior satisfies an atomic proposition in (36) at time t. For an identical control sequence, the nominal network's state must have lower occupancy on all links at time t. All atomic propositions in (36) correspond to lower sets, so lower occupancy on a traffic link implies proposition satisfaction. Thus, it must be that the nominal network also satisfies that predicate at time t with the same initial state and control sequence and it's clear that the nominal network must then satisfy specification (36).

C. Removing Unsatisfactory Contract Parameters

Suppose a controller cannot be synthesized for a downstream network but can for an upstream one. Any higher upstream demand or more stringent supply requirements will not yield a control strategy, so an appropriate orthant of the parameter space can be eliminated. As depicted in Fig. 8, the number of satisfying initial states is an increasing function with respect to the elements of $\Sigma_n, \tilde{\Delta}_n$ and a decreasing

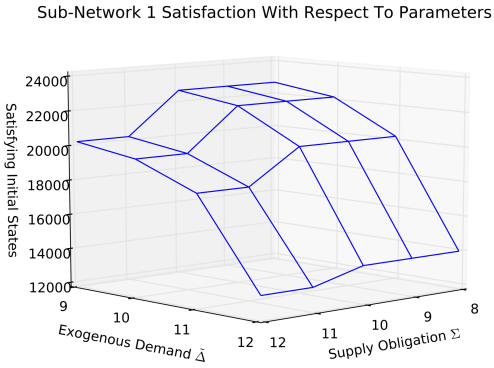

Fig. 8: The number of satisfying initial states for sub-network $\mathcal{N}_1$ in Section IV decreases as supply obligation $\tilde{\Sigma}$ and exogenous demand Δ increase.

function with respect to the elements of $\Delta_n, \tilde{\Sigma}_n$ Whenever a controller cannot be synthesized for a sub-network, only the few contract parameters that pertain to that sub-network need to be altered.

VI. Conclusion and Future Work

We have presented a contract-based methodology for synthesizing local controllers that guarantee global specifications. Future research will focus on expanding the types of contracts between networks beyond contracts of the form (27). Also, another future direction is identifying methods to partition the network to either speed up controller synthesis or to make contracts less restrictive.

VII. Acknowledgments

We thank Samuel Coogan for insightful discussions and providing the simulation and synthesis code from [3].

References

[1] A. Pnueli, "The temporal logic of programs," in *18th Annual Symposium on Foundations of Computer Science*, ser. SFCS '77, 1977, pp. 46–57.

[2] C. F. Daganzo, "The cell transmission model: A dynamic representation of highway traffic consistent with the hydrodynamic theory," *Transportation Research*, vol. 28, pp. 269–287, 1994.

[3] S. Coogan, E. A. Gol, M. Arcak, and C. Belta, "Traffic network control from temporal logic specifications," *IEEE Transactions on Control of Network Systems*, vol. 99, 2015.

[4] P. Tabuada, S. Yamac Caliskan, M. Rungger, and R. Majumdar, "Towards robustness for cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3151–3163, 2014.

[5] U. Topcu, N. Ozay, J. Liu, and R. Murray, "On synthesizing robust discrete controllers under modeling uncertainty," *Hybrid Systems: Computation and Control*, 2012.

[6] M. Keyvan-Ekbatani, A. Kouvelas, I. Papamichail, and M. Papageorgiou, "Exploiting the fundamental diagram of urban networks for feedback-based gating," *Transportation Research*, vol. 46, pp. 269–287, 2012.

[7] D. Su, X.-Y. Lu, R. Horowitz, and Z. Wang, "Coordinated ramp metering and intersection signal control," *International Journal of Transportation Science and Technology*, vol. 3, no. 2, pp. 45–63, 2014.

[8] S. Coogan and M. Arcak, "Scalable finite abstraction of mixed monotone systems," *Hybrid Systems: Computation and Control*, 2015.

[9] B. Yordanov, J. Tumov, I. Černy, J. Barnat, and C. Belta, "Temporal logic control of discrete-time piecewise affine systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 6, pp. 1491–1504, 2012.

[10] D. Angeli and E. Sontag, "Monotone control systems," *IEEE Transactions of Automatic Control*, vol. 48, no. 10, pp. 1684–1698, 2003.