Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

DTU

Domains and Problem Frames

- **Event: IWAAPF 2006, Shanghai, 23 May**
- **Speaker: Dines Bjørner**
- **Affiliations:**

Computer Science and Engineering
Informatics and Mathematical Modelling
Technical University of Denmark
Bldgs. 305, 321–322, 325
DK–28000 Kgs.Lyngby, **Denmark**
db@imm.dtu.dk

School of Information Science
JAIST
1-1, Asahidai, Tatsunokuchi,
Nomi, Ishikawa 923-1292
Japan
bjorner@gmail.com

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domains and Problem Frames
The Dogma

- Before **software** can be designed
- we must understand its **requirements**.
- Before **requirements** can be prescribed
- we must understand the **domain**[1]
- In this talk we show
  - ⋆ **one** example **domain description** and
  - ⋆ **four** related example **requirements prescriptions**;
  - ⋆ the latter illustrates distinct **frames**.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[1] The term domain is here used instead of the, i PF contexts, perhaps more common term environment.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Aims & Objectives

Aims

- Illustrate aspects of
  - ⋆ problem frame **independent** domain engineering,
  - ⋆ problem frame **dependent** requirements engineering,
  - ⋆ and the **interplay** between various requirements prescriptions.

Objectives

- To plead for more systematic software engineering work around domain engineering,
- before requirements engineering sets in.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Structure of Presentation

- A long and undoubtedly boring domain description.
- An exhaustive four requirements presecriptions.
- A conclusion
  - ⋆ which relates this quadruple development to the problem frame approach, and
  - ⋆ and briefly discusses a rôle for the triptych cum problem frame approach in the VSTTE and Ubiquitous Computing grand challenges!
- We need the "multiple masses of details" to substantiate our claims.
- We have 42 minutes left — so we need skip over
  - ⋆ some of the domain description aspects and
  - ⋆ some of the four requirements developments.

+81-761-51-1275, Fax: +81-761-51-1149

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

The Domain
Net Topology
Nets, Segments and Junctions

1. Nets consists of one or more segments and two or more junctions.

type
  N, S, J
value
  obs_Ss: N → S-**set**
  obs_Js: N → J-**set**
axiom
  ∀ n:N · **card** obs_Ss(n) ≥ 1 ∧ **card** obs_Js(n) ≥ 2

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

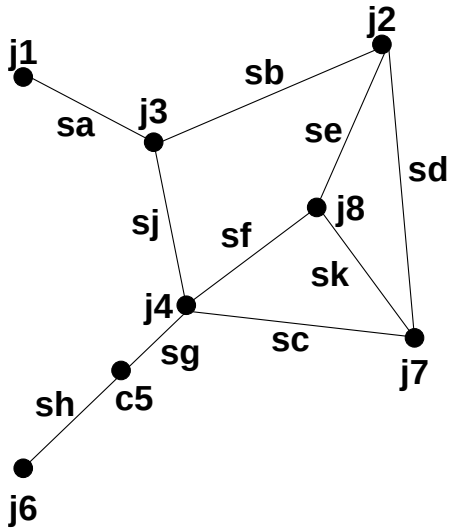

Figure 3.1: A simple net of segments and junctions

Applying the observer functions to the net of Fig. 3.1 yields:

$$\text{obs\_Ss(n)} = \{\text{sa,sb,sc,sd,se,sf,sg,sh,sj,sk}\}$$
$$\text{obs\_Js(n)} = \{\text{j1,j2,j3,j4,j5,j6,j7,j8}\}$$

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Segment and Junction Identifications

2. Segments and junctions have unique identifications.

type
  Si, Ji
value
  obs_Si: S → Si
  obs_Ji: J → Ji

Segment and junction identifications are abstract concepts.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

3. No two segments have the same segment identifier. And no two junctions have the same junction identifier.

axiom

$$\forall\ \mathrm{n{:}N} \cdot \mathbf{card}\ \mathrm{obs\_Ss(n)} \equiv \mathbf{card}\ \{\mathrm{obs\_Si(s)} | \mathrm{s{:}S} \cdot \mathrm{s} \in \mathrm{obs\_Ss(n)}\}$$

$$\forall\ \mathrm{n{:}N} \cdot \mathbf{card}\ \mathrm{obs\_Js(n)} \equiv \mathbf{card}\ \{\mathrm{obs\_Ji(c)} | \mathrm{j{:}J} \cdot \mathrm{j} \in \mathrm{obs\_Js(n)}\}$$

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Segment and Junction Reference Identifications

4. Segments are delimited by two distinct junctions. From a segment one can also observe, obs_Jis, the identifications of the delimiting junctions.

type
  Jip = {|{ji,ji′}:Ji-**set** · ji≠ji′|}
value
  obs_Jis: S → Jip

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

5. Any junction has a finite, but non-zero number of segments connected to it. From a junction one can also observe, obs_Sis, the identifications of the connected segments.

type
  Si1 = {|sis:Si-**set·card** sis ≥1|}
value
  obs_Sis: J → Si1

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

6. In any net, if s is a segment connected to connectors identified by ji and ji′, respectively, then there must exist connectors j and j′ which have these identifications and such that the identification si of s is observable from both j and j′.

axiom

$$\forall\ \text{n:N, s:S} \cdot \text{s} \in \text{obs\_Ss(n)} \Rightarrow$$
$$\quad \textbf{let}\ \{\text{ji,ji}'\} = \text{obs\_Jis(s)}\ \textbf{in}$$
$$\quad \exists!\ \text{j,j}'\text{:J} \cdot \{\text{j,j}'\} \subseteq \text{obs\_Js(n)} \wedge \text{j} \neq \text{j}' \wedge$$
$$\quad\quad \text{obs\_Si(s)} \in \text{obs\_Sis(c)} \cap \text{obs\_Sis(c}')\ \textbf{end}$$

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

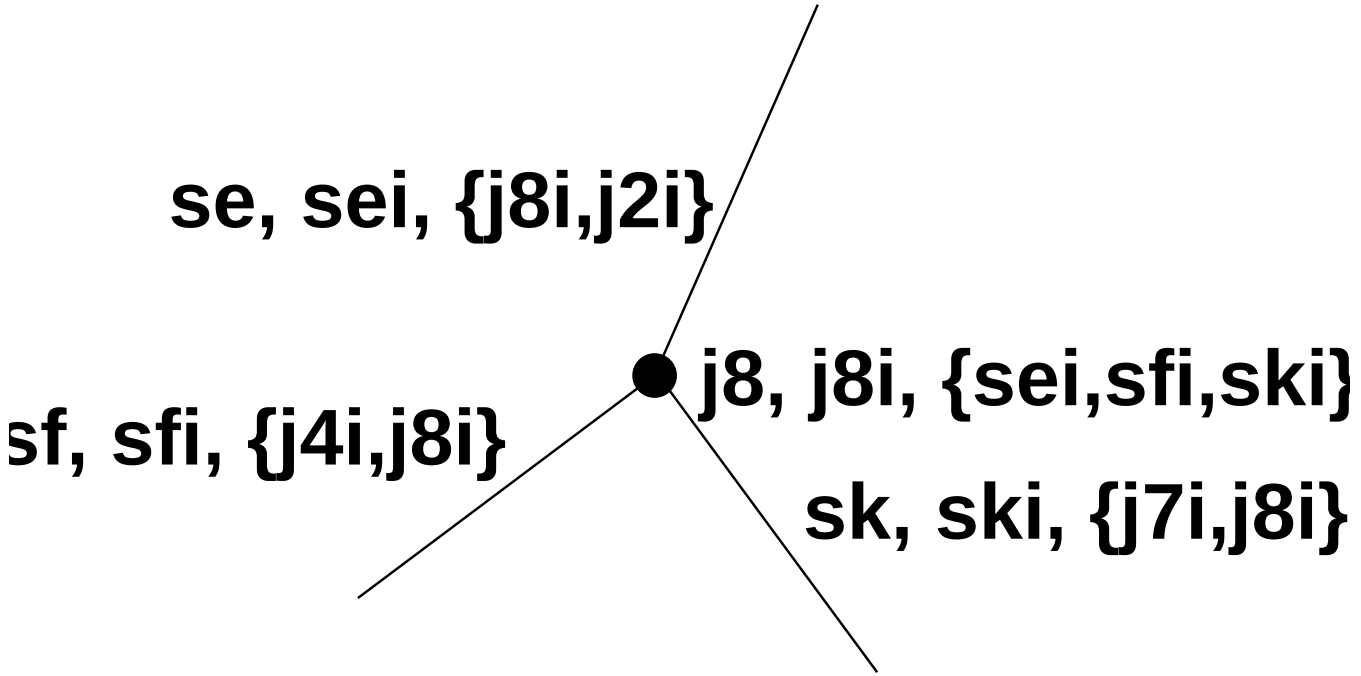

Figure 3.2: One junction and its connected segments

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

7. Vice-versa: In any net, if j is a junction connecting segments identified by si, si′, ..., si″ then there must exist segments s, s′, ..., s″ which have these identifications and such that the identification ji of j is observable from all s, s′, ..., s″.

axiom

$\forall$ n:N, j:J · j $\in$ obs_Js(n) $\Rightarrow$
let sis = obs_Sis(c), ji = obs_Ji(j) **in**
$\exists!$ ss:S-**set** · ss$\subseteq$obs_Ss(n) $\wedge$ **card** ss=**card** sis $\wedge$
sis = {|obs_Si(s)|s:S·s $\in$ ss|} **end**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Paths and Routes

8. By a path we shall understand a triplet of a junction identification, a segment identification and a junction identification.

type
  P = Ji × Si × Ji
value
  paths: N → P-**set**
  paths(n) ≡
    {(ji,si,ji′)|s:S,ji,ji′:Ji,si:Si·
      s ∈ obs_Ss(n)∧{ji,ji′} ∈ obs_Jis(s)∧si=obs_Si(s)}

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

9. By a route of a net we shall understand a list, i.e., a sequence of paths as follows:
   - A sequence of just one path of the net is a route.
   - If r and r′ are routes of the net such that the last junction identification, ji, of the last path, (_,_,ji) of r and the first junction identification, ji′, of the first path (ji′,_,_) of r′ are the same, i.e., ji=ji′, then $r \frown r'$ is a route.
   - Only routes that can be generated by uses of the first (the basis) and the second (the induction) clause above qualify as proper routes of a net.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

type
  R = {|r:P*•wf_R(r)|}
value
  wf_R: P* → **Bool**
  wf_R(r) ≡
    ∀ i:**Nat** • {i,i+1}⊆**inds**(r) ⇒
      let (_,_,ji)=r(i), (ji′,_,_)=r(i+1) **in** ji = ji′ **end**

  routes: N → R-**infset**
  routes(n) ≡
    let rs = {⟨p⟩|p:P•p ∈ paths(n)}
          ∪ {r⌢r′|r,r′:R•{r,r′}⊆rs∧wf_R(r⌢r′)} **in**
    rs **end**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Connected Nets

10. A net is connected if for any two junctions of the net there is a route between them.

value

is_connected: N → **Bool**

is_connected(n) ≡

∀ j,j′:J · {j,j′}⊆obs_Js(n) ∧ j≠j′ ⇒

let (ji,ji′) = (obs_Ji(j),obs_Ji(j′)) **in**

∃ r:R · r ∈ routes(n) ∧

first_Ji(r) = ji ∧ last_Ji(r) = ji′ **end**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Net Decomposition

11. One can decompose a net into all its connected subnets. If a net exhaustively consists of m disconnected nets, then for any pair of nets in different disconnected nets it is the case that they share no junctions and no segments. The set of disconnected nets is the smallest such set that together makes up all the segments and all the junctions of the ("original") net.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

value

decompose: N → N-**set**

decompose(n) **as** ns

obs_Ss(n) = ∪{obs_Ss(n′)|n′:N·n′ ∈ ns} ∧

obs_Js(n) = ∪{obs_Js(n′)|n′:N·n′ ∈ ns} ∧

{} = ∩{obs_Ss(n′)|n′:N·n′ ∈ ns} ∧

{} = ∩{obs_Js(n′)|n′:N·n′ ∈ ns} ∧

∀ n′:N·n′ ∈ ns ⇒ connected(n′) ∧ ...

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

That is, we have the following:

Lemma:

$$
\begin{array}{l}
\forall\ \mathrm{n{:}N} \cdot \\
\quad \textbf{let}\ \mathrm{ns} = \mathrm{decompose}\ (\mathrm{n})\ \textbf{in} \\
\quad \forall\ \mathrm{n'{,}n''{:}N} \cdot \{\mathrm{n'{,}n''}\} \subseteq \mathrm{ns} \wedge \mathrm{n'} \neq \mathrm{n''} \Rightarrow \\
\qquad \mathrm{obs\_Ss}(\mathrm{n'}) \cap \mathrm{obs\_Ss}(\mathrm{n''}) = \{\} \wedge \\
\qquad \mathrm{obs\_Js}(\mathrm{n'}) \cap \mathrm{obs\_Js}(\mathrm{n''}) = \{\}\ \textbf{end}
\end{array}
$$

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Multi-Modal Nets

General Issues

12. We introduce a concept, M, of transport mode. M is a small set of distinct, but otherwise further undefined tokens. An m in M designates a transport modality.

type
M

Segment and Junction Modes

13. With each segment, s, we can associate a single mode, m, and with each junction we can associate the set of modes of its connected segments.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

value
  obs_M: S → M
  obs_Ms: J → M-**set**
axiom
  ∀ n:N, j:J · j ∈ obs_Js(n) ⇒
    let ss = xtr_Ss(n,obs_Ji(j)) **in**
    obs_Ms(j) = {obs_M(s)|s:S · s ∈ ss} **end**
  ∀ n:N, s:S · s ∈ obs_Ss(n) ⇒
    let {ji,ji′} = obs_Jis(s) **in**
    let {j,j′} = {xtr_J(n,ji),xtr_J(n,ji′)} **in**
    obs_M(s) ∈ obs_Ms(j) ∩ obs_Ms(j′) **end end**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Single-Modal Nets and Net Projection

14. Given a multi-modal net one can project it onto a set of single modality nets, namely one for each modality registered in the multi-modal net.

type
  mmN = {|n:N · **card** xtr_Ms(n) > 1|}
  smN = {|n:N · **card** xtr_Ms(n) = 1|}
value
  xtr_Ms: N → M**-set**
  xtr_Ms(n) ≡ {obs_M(s) | s:S · s ∈ obs_Ss(n)}

  projs: N → smN**-set**
  projs(n) ≡ {proj(n,m) | m:M · m ∈ xtr_Ms(n)}

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

$$\text{proj: N} \times \text{M} \to \text{smN}$$
$$\text{proj(n,m) } \textbf{as } \text{n}'$$
post
let $\text{ss} = \text{obs\_Ss(n)}, \text{ss}' = \text{obs\_Ss(n}'\text{)},$
$\text{js} = \text{obs\_Js(n)}, \text{js}' = \text{obs\_Js(n}'\text{)}$ **in**
$\text{ss}' = \{\text{s} \mid \text{s:S} \cdot \text{s} \in \text{ss} \wedge \text{m=obs\_M(s)}\} \wedge$
$\text{js}' = \{\text{j} \mid \text{j:J} \cdot \text{j} \in \text{js} \wedge \text{m} \in \text{obs\_Ms(j)}\}$
end

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Segment and Junction Attributes

Segment and Junction Attribute Observations

We now enrich our segments and junctions.

15. Segments have lengths.
16. Junctions have modality-determined lengths between pairs of (same such modality) segments connected to the junction.
17. Segments have standard transportation times, i.e., time durations that it takes to transport any number of units of freight from one end of the segment to the other.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

18. Junctions have standard transfer time per modality of transport between pairs of segments connected to the junction.
19. Junctions have standard arrival time per modality of transport.
20. Junctions have standard departure times per modality of transport.
21. Segments have standard costs of transporting a unit of freight from one end of the segment to the other end.
22. Junctions have standard costs of transporting a unit of freight from the end of one connecting segment to the beginning of another connecting segment.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

We can now assess

- (i) length of a route,
- (ii) shortest routes between two junctions,
- (iii) duration time of standard transport along a route, including transfer, stopover and possible reloading times at junctions, and
- (iv) shortest duration time route of standard transport between two junctions.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

type
  L, TI
value
  ms:M-**set**, **axiom** ms≠{}
  obs_L: S → L
  obs_L: Si × J × M × Si → L
  obs_TI: S → TI
  obs_TI: Si × J × Si → TI
  obs_TI: J × M ~→ TI, **pre** obs_TI(j,m): m ∈ obs_Ms(j)
  obs_TI: J × M × M ~→ TI, **pre** obs_TI(j,m,m′): {m,m′}⊆obs_Ms(j)
  obs_arr_TI: J × M ~→ TI, **pre** obs_arr_TI(j,m): m ∈ obs_Ms(j)
  obs_dep_TI: J × M ~→ TI, **pre** obs_dep_TI(j,m): m ∈ obs_Ms(j)
  +: L × L → L
  +: TI × TI → TI

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Route Lengths

23. One can compute the length of a route of a net and one can find the shortest such route between two identified junctions.

value
  length: R → N ~→ L
  length(r)(n) ≡
    case r **of**
      ⟨⟩ → 0,
      ⟨(jf,si,jt)⟩ → obs_L(xtr_S(si,n)),
      ⟨(ji1,sii,ji2),(jj1,sij,jj2)⟩ ⌢ r′ →
        let si=xtr_S(sii,n),sj=xtr_S(sij,n) **in**
        obs_L(si) + obs_L(sii,xtr_J(ji2,n),sij) + length(⟨(jj1,sij,jj2)⟩ ⌢ r′) **end**
    end
    pre: r ∈ routes(n) ∧ ji2=jj1

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

value

shortest_route: Ji × Ji → N $\xrightarrow{\sim}$ R

shortest_route(jf,jt)(n) ≡

let rs = routes(n) **in**

let crs = {r|r:R·r ∈ rs ∧ first_Ji(r)=jf ∧ last_Ji(r)=jt} **in**

let sr:R · sr ∈ crs ∧ ∼∃ r:R · r ∈ crs ∧ length(r)(n)<length(sr)(n) **in**

sr **end end end**

pre: {jf,jt}⊆obs_Jis(n) ∧ jf≠jt

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Route Traversal Times

24. One can find the total time it takes to traverse a route, including the times it takes to pass through a junction, and one can find the quickest route between two identified junctions.

all_time: R → N → TI
all_time(r)(n) ≡
  obs_arr_TI(xtr_J(first_J(r),n),obs_M(first_S{r}))
  + time(r)(n)
  + obs_dep_TI(xtr_J(last_J{r},n),obs_M(last_S(r)))

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

time: R → N → TI
time(r)(n) ≡
  case r **of**
    ⟨⟩ → 0,
    ⟨(jf,si,jt)⟩ → obs_TI(xtr_S(si,n)),
    ⟨(ji1,sii,ji2),(jj1,sij,jj2)⟩ ⌢ r′ →
      let si=xtr_S(sii,n),sj=xtr_S(sij,n) **in**
      obs_TI(si) + obs_TI(sii,xtr_J(ji2,n),sij) + time(⟨(jj1,sij,jj2)⟩ ⌢ r′) **end**
  end
  pre: r ∈ routes(n) ∧ ji2=jj1

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

quickest_route: Ji × Ji → N → R
quickest_route(jf,jt)(n) ≡
  let rs = routes(n) **in**
  let crs = {r|r:R·r ∈ rs ∧ first_Ji(r)=jf ∧ last_Ji(r)=jt} **in**
  let qr:R · qr ∈ crs ∧ ∼∃ r:R · r ∈ crs ∧ all_time(r)(n)<all_time(qr)(n) i
  qr **end end end**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Transportation Costs

25. We can further assess (i) transport cost (tk:TK), (ii) lowest (per unit) freight cost (fk:FK) between two junctions, etc. We assume that if a freight item is transported into a junction and out of that junction by the same modality conveyour, then it is not reloaded, i.e., along segments of the same modality.[2]

type
  TK, FK, K = TK|FK
value
  obs_TK: (S|J) → TK
  obs_FK: (S|J) → FK

  +: K × K → K

+81-761 51 1275, Fax: +81 761 51 1149

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[2] This grossly simplifying assumption will be removed later. For the time being it allows us to operate with the simple notion of routes that was introduced above. For the reloading case we need to decorate the route notion, effectively making it into a bill of ladings notion: one that prescribes possible reloading at junctions.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

$$\text{cost: } \mathrm{R} \to \mathrm{N} \to \mathrm{K}$$
$$\text{cost}(\mathrm{r})(\mathrm{n}) \equiv$$
case r **of**
$\langle\rangle \to 0,$
$\langle(\mathrm{jf},\mathrm{si},\mathrm{jt})\rangle \to$
$\quad \text{obs\_K}(\text{xtr\_J}(\mathrm{jf},\mathrm{n}))+\text{obs\_K}(\text{xtr\_S}(\mathrm{si},\mathrm{n}))+\text{obs\_K}(\text{xtr\_J}(\mathrm{jt},\mathrm{n}))$
$\langle(\mathrm{jf},\mathrm{si},\mathrm{jt}),(\mathrm{jf}',\mathrm{si}',\mathrm{jt}')\rangle \frown \mathrm{r}' \to$ **assert:** $\mathrm{jt}=\mathrm{jf}'$
$\quad \text{obs\_K}(\text{xtr\_J}(\mathrm{jf},\mathrm{n}))+\text{obs\_K}(\text{xtr\_S}(\mathrm{si},\mathrm{n}))+\ldots+\text{cost}(\mathrm{r}')$
end

$$\text{cheapest: } \mathrm{Ji}\times\mathrm{Ji} \to \mathrm{N} \to ((\mathrm{K}\times\mathrm{K})\to\mathrm{K}) \to ((\mathrm{K}\times\mathrm{K})\to\textbf{Bool}) \to \mathrm{R}$$
$$\text{cheapest}(\mathrm{jf},\mathrm{jt})(\mathrm{n}) \equiv$$
$\text{best}(\mathrm{jf},\mathrm{jt})(\mathrm{n})(\lambda(\mathrm{k1},\mathrm{k2}):(\mathrm{K}\times\mathrm{K})\cdot\mathrm{k1}+\mathrm{k2})(\lambda(\mathrm{k1},\mathrm{k2}):(\mathrm{K}\times\mathrm{K})\cdot\mathrm{k1}<\mathrm{k2})$

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Road Nets

We wish to view road nets at different levels of abstraction. At a most detailed such level we make no distinction between the road kinds, whether community roads, provincial roads, motor roads or freeways. At another level of abstraction we wish to make exactly those distinctions. And at least detailed level of abstraction we consider certain road junctions to designate road nets of smaller or larger communities.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

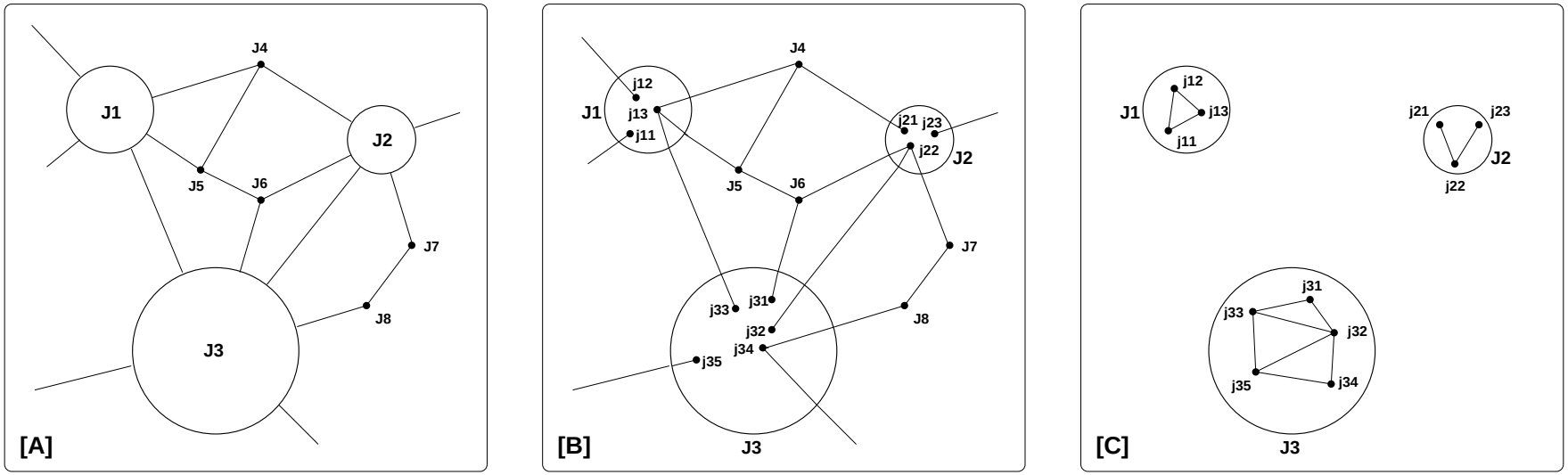

Figure 3.3: Gross [A] versus semi-detailed [B] road net — and community road nets [C]

26. Figure [A] 3.3 shows a road net. Instead of showing junctions J1, J2 and J3 as small black disks we show them as larger circles — for reasons that transpires from Fig. [B] 3.3.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

27. Junctions J1, J2 and J3 are considered composite, that is, to represent communities.
28. We may consider the road net of Fig.[A] 3.3 on the preceding page to be an abstraction of the road net hinted at in Fig.[B] 3.3 on the page before.
29. Junctions j11, j12, ..., j35 are considered simple embedded junctions.
30. We decide to allow three kinds of junctions:
    (a) composite,
    (b) simple embedded and
    (c) simple.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Railway Nets

General

A transportation net of modality railway has segments be lines between stations and have junctions be stations.

31. We concretise the concept of modes. Mode m=railway will now designate railway nets:

type
M == road | railway | ...

32. From a multi-modal transportation net we can project the railway net, rn:RN:

value
proj: N × {railway} → RN

33. Junctions of a transportation net of modality railway have sub-junctions which are stations:

value
proj: J × {railway} → ST

34. Segments of a transportation net of modality railway become lines:

value
proj: S × {railway} → LI

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Lines, Stations, Units and Connectors

Railway segments are thus called lines, and railway sub-junctions are thus called stations. A notion of connectors is introduced. It is not to be confused with the previous notion of junctions.

35. A railway net is a net of mode railway.
36. Its segments are lines of mode railway.
37. Its junctions are stations of mode railway.
38. A railway net consists of one or more lines and two or more stations.
39. A railway net consists of rail units.
40. A line is a linear sequence of one or more linear rail units.
41. The rail units of a line must be rail units of the railway net of the line.
42. A station is a set of one or more rail units.
43. The rail units of a station must be rail units of the railway net of the station.
44. No two distinct lines and/or stations of a railway net share rail units.
45. A station consists of one or more tracks.
46. A track is a linear sequence of one or more linear rail units.
47. No two distinct tracks share rail units.
48. The rail units of a track must be rail units of the station (of that track).
49. A rail unit is either a linear, or is a switch, or a is simple crossover, or is a switchable crossover, etc., rail unit.
50. A rail unit has one or more connectors.
51. A linear rail unit has two distinct connectors. A switch (a point) rail unit has three distinct connectors. Crossover rail units have four distinct connectors (whether simple or switchable), etc.
52. For every connector there are at most two rail units which have that connector in common.
53. Every line of a railway net is connected to exactly two distinct stations of that railway net.
54. A linear sequence of (linear) rail units is an acyclic sequence of linear units such that neighbouring units share connectors.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

type

35. RN = {| n:smN • obs_M(n)=railway |}
36. LI = {| s:S • obs_M(s)=railway |}
37. ST = {| c:C • obs_M(c)=railway |}

Tr, U, K

value

38. obs_LIs: RN → LI-**set**
38. obs_STs: RN → ST-**set**
39. obs_Us: RN → U-**set**
40. obs_Us: LI → U-**set**
42. obs_Us: ST → U-**set**
45. obs_Trs: ST → Tr-**set**
49. is_Linear: U → **Bool**
49. is_Switch: U → **Bool**
49. is_Simple_Crossover: U → **Bool**
49. is_Switchable_Crossover: U → **Bool**
50. obs_Ks: U → K-**set**

54. lin_seq: U-**set** → **Bool**

lin_seq(us) ≡
∀ u:U • u ∈ us ⇒ is_Linear(u) ∧
∃ q:U* • **len** q = **card** us ∧ **elems** q = us ∧
∀ i:**Nat** • {i,i+1} ⊆ **inds** q ⇒ ∃ k:K •
obs_Ks(q(i)) ∩ obs_Ks(q(i+1)) = {k} ∧
len q > 1 ⇒ obs_Ks(q(i)) ∩ obs_Ks(q(**len** q)) = {}

axiom

38. ∀ n:RN • **card** obs_LIs(n) ≥ 1 ∧ **card** obs_STs(n) ≥ 2

40. ∀ n:RN, l:LI • l ∈ obs_LIs(n) ⇒ lin_seq(l)

41. ∀ n:RN, l:LI • l ∈ obs_LIs(n) ⇒ obs_Us(l) ⊆ obs_Us(n)

42. ∀ n:RN, s:ST • s ∈ obs_STs(n) ⇒ **card** obs_Us(s) ≥ 1

43. ∀ n:RN, s:ST • s ∈ obs_LIs(n) ⇒ obs_Us(s) ⊆ obs_Us(n)

44. ∀ n:RN,l,l′:LI•{l,l′}⊆obs_LIs(n)∧l≠l′⇒obs_Us(l)∩ obs_Us(l′)={}

44. ∀ n:RN,l:LI,s:ST•l ∈ obs_LIs(n)∧s ∈ obs_STs(n)⇒obs_Us(l)∩ obs_Us(s)={}

44. ∀ n:RN,s,s′:ST•{s,s′}⊆obs_STs(n)∧s≠s′⇒obs_Us(s)∩ obs_Us(s′)={}

45. ∀ s:ST•**card** obs_Trs(s)≥1

46. ∀ n:RN,s:ST,t:Tr•s ∈ obs_STs(n)∧t ∈ obs_Trs(s)⇒lin_seq(t)

47. ∀ n:RN,s:ST,t,t′:Tr•s ∈ obs_STs(n)∧{t,t′}⊆obs_Trs(s)∧t≠t′
⇒ obs_Us(t) ∩ obs_Us(t′) = {}

52. ∀ n:RN • ∀ k:K •
k ∈ ∪{obs_Ks(u)|u:U•u ∈ obs_Us(n)}
⇒**card**{u|u:U•u ∈ obs_Us(n)∧k ∈ obs_Ks(u)}≤2

53. ∀ n:RN,l:LI • l ∈ obs_LIs(n) ⇒
∃ s,s′:ST • {s,s′} ⊆ obs_STs(n) ∧ s≠s′ ⇒
let sus=obs_Us(s),sus′=obs_Us(s′),lus=obs_Us(l) **in**
∃ u,u′,u″,u‴:U • u ∈ sus ∧
u′ ∈ sus′ ∧ {u″,u‴} ⊆ lus ⇒
let sks = obs_Ks(u), sks′ = obs_Ks(u′),
lks = obs_Ks(u″), lks′ = obs_Ks(u‴) **in**
∃!k,k′:K•k≠k′∧sks ∩ lks={k}∧sks′ ∩ lks′={k′}
end end

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Net Dynamics

- By net dynamics we shall mean the changing possibilities of flow of conveyors (cars, trains, aircraft, ships, etc.) along segments and through junctions.
- We speak of direction of flow along segments in terms of *"from the junction at one end of the segment to the junction at the other end"*.
- And we speak of flow through a junction as *"proceeding from one segment incident upon the junction into a (udually different) segment emanating from that junction"*.
- Segments connected to a junction are both incident upon that junction and emanates from that junction.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Segment and Junction States

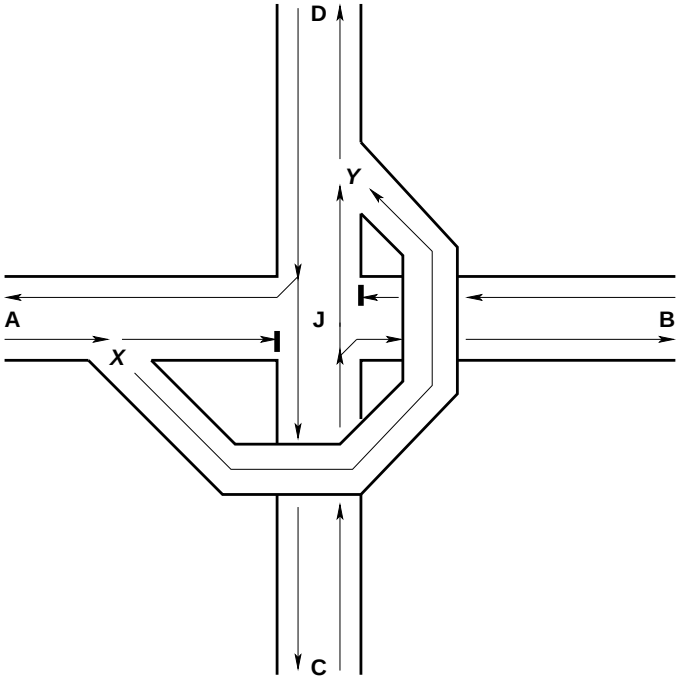

Figure 3.4: A Special "Carrefour" Junction

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

55. Segments may be open for traffic in either or both directions (between the segments' two junctions [identified by ji_x and ji_y]) or may be closed.
56. We model the state, $s\sigma : S\Sigma$, of a segment, $s : S$, as a set of pairs of junction identifications, namely of the two identifications of the junctions that the segment connects. This state, $s\sigma : S\Sigma$, is
    (a) either empty, i.e., the segment is closed ($\{\}$),
    (b) or has one pair, $\{(ji_x, ji_y)\}$, that is, the segment is open in direction from junction ji_x to junction ji_y,
    (c) or another pair $\{(ji_y, ji_x)\}$,
    (d) or both pairs $\{(ji_x, ji_y), (ji_y, ji_x)\}$, that is, is open in both directions.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

57. Junctions may direct traffic from any subset of incident segments to any subset of emanating segments.
58. We model the state, $j\sigma : J\Sigma$, of a junction, $j : J$, as a set of pairs of segment identifications, namely of identifications of segments connected to the junction.
    (a) Let the set of identifications of segments connected to junction j be $\{si_1, si_2, ..., si_m\}$.
    (b) If, in some state, $j\sigma$ of the junction, it is possible (allowed) to pass through the junction from the segment identified by si_j to the segment identified by si_k, then the pair (si_j, si_k) is in $j\sigma$.
    (c) The junction state may be empty, i.e., closed: no traffic is allowed through the junction.
    (d) Or the junction state may be "anarchic full", that is, it contains all combinations of the pairs of identifiers of segments incident upon the junction.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

type
  $S\Sigma = (Ji \times Ji)$**-set**
  $J\Sigma = (Si \times Si)$**-set**
value
  obs_SΣ: $S \to S\Sigma$
  obs_JΣ: $J \to J\Sigma$

  xtr_Jis: $S\Sigma \to Ji$**-set**, $xtr\_Jis(s\sigma) \equiv \{ji | ji:Ji \cdot (ji,\_) \in obs\_s\sigma \vee (\_,ji) \in obs\_s\sigma\}$
  xtr_Sis: $J\Sigma \to Si$**-set**, $xtr\_Sis(j\sigma) \equiv \{si | si:Si \cdot (si,\_) \in obs\_j\sigma \vee (\_,si) \in obs\_j\sigma\}$
axiom
  $\forall\ s:S \cdot xtr\_Jis(obs\_S\Sigma(s)) \subseteq xtr\_Jip(s)$,
  $\forall\ j:J \cdot xtr\_Sis(obs\_J\Sigma(j)) \subseteq xtr\_Sis(j)$

axiom
  ...

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

59. The junction of Fig. 3.4 shows four segments, identified by A, B, C and D.
60. The figure also suggests a state in which traffic lights prohibit movements from A into J, from B into J,
61. from C via J into A, and from D via J into B.
62. The "bypass" from A/X into Y/D appears to be such that traffic can always pass from A into D.
63. The current state alluded to in Fig. 3.4 on page 43 appears to be:

$$j\sigma_J : \{(A, D), (C, B), (C, D), (D, A), (D, C)\}$$

64. (A, D) is potentially a member of every state that the junction can possibly be in — see next section.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Segment and Junction State Spaces

65. A segment can be in one of several segments states.
66. A junction can be in one of several junction states.
67. Hence we introduce segment and junction state spaces.

type
  $\mathrm{S}\Omega = \mathrm{S}\Sigma$**-set**
  $\mathrm{J}\Omega = \mathrm{J}\Sigma$**-set**
value
  $\mathrm{obs\_S}\Omega$: $\mathrm{S} \to \mathrm{S}\Omega$
  $\mathrm{obs\_J}\Omega$: $\mathrm{J} \to \mathrm{J}\Omega$
axiom
  $\forall$ s:S $\cdot$ $\mathrm{obs\_S}\Sigma(\mathrm{s}) \subseteq \mathrm{obs\_S}\Omega(\mathrm{s})$,
  $\forall$ j:J $\cdot$ $\mathrm{obs\_J}\Sigma(\mathrm{j}) \subseteq \mathrm{obs\_J}\Omega(\mathrm{j})$

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

More on Net Dynamics: Traffic

Vehicles and Positions

68. There is a further undefined notion of vehicles, V.
69. And there is a notion of the position, P, of a vehicle.
    (a) Either a vehicle is positioned in a junction, and then its position is designated by the junction identifier.
    (b) Or a vehicle is positioned along a segment, and then its position is designated by a triplet:
        i. the identifier of the junction it is moving away from,
        ii. the identifier of the junction it is moving towards, and

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

iii. the fraction of the distances from the position to the two junctions:
   A. If the fraction is 0, then the vehicle has just entered the segment,
   B. if the fraction is 1, then the vehicle is just about to leave the segment, and, hence,
   C. if the fraction is a proper real between o and 1, but neither 0 nor 1, then the vehicle is properly within the segment.

type
  F = {|f:**Real**·0≤f≤1|}
  P == mkP_at_J(ji:Ji) | mkP_along_S(fji:Ji,f:F,tji:Ji)

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Traffic

70. Traffic is now a function from time to a pair of
   (a) a net,
   (b) and the positions of vehicles within the net.

type
  V
  T
  $\mathrm{TF} = \mathrm{T} \xrightarrow{m} (\mathrm{N} \times (\mathrm{V} \xrightarrow{m} \mathrm{P}))$

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Proper Vehicle Positions

71. The positions of a traffic must designate proper junctions of the net.

axiom
  ∀ tf:TF ·
    ∀ t ∈ **dom** tf ·
      let (n,vps) = tf(t) **in**
      ∀ p:P · p ∈ **rng** vps ⇒
      case p **of**
        mkP_at_J(ji) → ji ∈ obs_Jis(n),
        mkP_along_S(jf,_,jt) → {jf,jt}⊆obs_Jis(n)
      end end

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Other Traffic Constraints

72. Traffic must be smooth: Positions of vehicles do not "jump around", i.e., movement are monotonic.
73. No "ghost vehicles":
    (a) If at times t and t'
    (b) considered close to one another
    (c) a vehicle is in the traffic
    (d) then it is also in the traffic at all times in between t and t'.

We omit the formalisations of the above.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Time Tables and Traffic

Time Tables

- By a time table we understand an entity which to named transport vehicles associate journey descriptions.
- By a journey description we understand a sequence of junction visits.
- By a junction visit we understand a triple: Arrival time, junction identifier and departure time.

type

TT = Vn $\overrightarrow{m}$ Journey

Journey = (at:T × ji:Ji × dt:T)*

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Scheduling

- By scheduling we shall here, in a narrow sense, understand
  - ⋆ a function from nets and time tables to
  - ⋆ a possibly infinite set of traffics
  - ⋆ such that each traffic satisfies the time table.

value
  sched: TT → N → TF**-infset**
  sched(tt)(n) **as** tfs
    pre: wf_TT_and_N(tt,n)
    post: ∀ tf:TF · tf ∈ tfs ⇒ wf_TF(tf) ∧ sat(tf,tt)

  wf_TT_and_N: TT × N → **Bool**, ...
  sat: TF × TT → **Bool**, ...

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

And so on!

- We have shown fragments of a description of a domain of transportation nets.
- There is, of course, much more. "Years of work still to be done!"
- But, for the time being we have enough to illustrate some reasonably interesting requirements.

+81-761-51-1275, Fax: +81-761-51-1149

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

A Set of Requirements

- We shall consider the following three sets of requirements:
  - ⋆ requirements for software to **monitor net maintenance**,
  - ⋆ requirements for software to **monitor & control net traffic**,
  - ⋆ requirements for software to **simulate net traffic**, and
  - ⋆ requirements for software to **support transport logistics**: optimal routes etc.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Plan of Development of Requirements

- The plan is now to
  - ⋆ first give a brief, rough sketch narrative of the four sets of requirements.
    - ◇ We do so, here, in this talk, in an **unusual** way.
    - ◇ First we **extend** the **domain** description give earlier.
    - ◇ Then we **project, instantiate**, and make less non-deterministic (**determination**) the extended **domain description**,
    - ◇ that is: We transform it into **domain requirements prescriptions**.

  But first we present the **domain extensions**.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

- The plan is further
  - ⋆ to analyse these four domain extension sketches wrt. such common "features" that may be **shared** by the three (or pairs of two) software implementations.
  - ⋆ to present the requirements for each of the four specific software "packages".
  - ⋆ and finally to present the requirements for such a shared "core" of software. That is, we are **fitting**.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Brief Narrative of the Four Sets of Requirements

Domain Requirements

- By domain requirements we understand requirements that can be sôlely expressed using terms of the domain (and ordinary, non-technical language).[3]
- In this talk we shall only consider domain requirements.
- Of course, many, if not most of the interesting problems of software development in relation also to 'problem frames' may be those due to interface and machine requirements.

+81-761 51 1275, Fax: +81 761 51 1149

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[3] By machine requirements we understand requirements that can be sôlely expressed using terms of the machine (and ordinary, non-technical language). By interface requirements we understand requirements that can be expressed only by using terms of both the domain and the machine (and ordinary, non-technical language).

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

'Net Maintenance' Software

- We propose a (parameterised) software package to be developed for
- monitoring and supporting the management of the maintenance of both road and rail nets.
- An instantiation parameter (road,rail) shall determine whether the package works for road or for rail nets.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

'Net Maintenance' Domain Description: An Extension

- Segments and junctions need be maintained, that is,
  - ⋆ we **may** associate a set of quality attributes related to the upkeep of segments and junctions, as well as of any traffic signals associated with these,
  - ⋆ we **may** further associate actual and estimated date(s), cost(s), and duration(s) of previous and next maintenance services, etc.,
  - ⋆ and we **may** keep "such" records of all segments, junctions and signals of the net.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

- To monitor the net quality attributes, in the domain, some need perform **work** that help
  - ⋆ advise maintenance staff to evaluate and report quality attributes of segments, junctions and signals,
  - ⋆ follow-up on missing such reports,
  - ⋆ and help update the attributes of the records kept when reported.
- To support the management of net maintenance some need perform, in the domain, **work** that help management schedule and allocate resources
  - ⋆ for the monitoring of net quality and corresponding update of records,
  - ⋆ for the actual maintenance work,
  - ⋆ and for handling "unforeseen" reports on segment, junction and signal malfunctioning (i.e., in need of repair).

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

'Net Maintenance' Domain Requirements

• Entities

- Segments and junctions need be maintained, that is,
  - ⋆ we **must** associate a set of quality attributes related to the upkeep of segments and junctions, as well as of any traffic signals associated with these,
  - ⋆ we **must** further associate actual and estimated date(s), cost(s), and duration(s) of previous and next maintenance services, etc.,
  - ⋆ and we **must** keep "such" records of all segments, junctions and signals of the net.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

• Monitoring Functions

- To monitor the net quality attributes, in the domain, the software **must** have **functions** that help
  - ⋆ advise maintenance staff to evaluate and report quality attributes of segments, junctions and signals,
  - ⋆ follow-up on missing such reports,
  - ⋆ and help update the attributes of the records kept when reported.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

• Management Functions

- To support the management of net maintenance the software **must** have **functions** that help management schedule and allocate resources
  - ⋆ for the monitoring of net quality and corresponding update of records,
  - ⋆ for the actual maintenance work,
  - ⋆ and for handling "unforeseen" reports on segment, junction and signal malfunctioning (i.e., in need of repair).
- **... here follows precise requirements details ...**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domain to Requirements Operations

In summary:

- **Projection:** Most of the net attributes have been kept. Many of the concepts (routes, ..) and evaluation functions (time, length, ...) have been "projected away".
- **Instantiation:** Usually the software, when delivered to a client, is instantiated to the specific net characteristics of the client.
- **Determination:** No example.
  (Looseness and non-determinism is removed.)
- ***Etcetera!***

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

'Traffic Control' Software

- We propose a software package to be developed for monitoring and controlling road net traffic
- not just at local junctions
- but along segments, and providing for "green" flow along certain route directions.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domain Description: A Very Rough Sketch Extension

- Traffic control in the conventional, non-technological net domain
- is done by traffic police controlling junction flows
- or by local sensors and actuators
  - ⋆ positioned near junctions
  - ⋆ sensors monitor only local traffic
  - ⋆ and actuators control only local junction semaphores.
- An assessment is made (by police or sensors) of local traffic density only,
- and appropriate arm signals or semaphore ligting (red, yellow, green) acts as controls.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domain Requirements

• Net Representation "In the Machine"

- The road net must be represented: segments, junctions and signals.
- Signals must be controlled.
- Segment, junction and signal states must be represented.
- Segment lengths and segment and junction (e.g., average) "traversal" times must be represented.
- Vehicle positions in segments and junctions must be represented.
- Vehicle positions must be monitored.
- We assume sensors to record and inform of "density" of vehicles at segment lanes in vicinity of junctions and leading into these.
- **... here follows precise requirements details ...**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

• Traffic Monitoring Functions

- Functions shall regularly sample traffic density.
- There must be functions for inquiring about and reporting on unusual traffic situations (accidents, fog, road conditions in general).
- It is assumed that there are functions which otherwise report on the statues of the road net.
  - ⋆ (That is, functions which relate to the net maintenance software.)
- **... here follows precise requirements dertails ...**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

• Traffic Control Functions

The objective of the use of these functions is to ensure smooth traffic.

- Individual functions shall determine the setting of signals at junctions.
- Composite functions shall determine the setting of signals, say in "green waves" along routes —
  - ⋆ hence the road net representation must be augmented with information about
    - ◇ major and minor routes,
    - ◇ time of day preferred directions: am "into town", pm "out of town",
    - ◇ and the like.
- **... here follows precise requirements details ...**

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domain to Requirements Operations

- **Projection:** Only the junction and segment state attributes need be kept.
- **Instantiation:** The net is instantiated to a particular road net of a particular city, i.e., that of the client.
- **Determination:** Some segments are designated as priority segments, with determined directions being "favoured" for "green traffic flow" at determined time intervals of the day. Accordingly some junction state transitions are "favoured" over others.
- ***Etcetera!***

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

'Traffic Simulation' Software

- We propose a software package to be developed for simulating road net traffic.
- In the domain there is, we assume, as yet no such simulation software.
- So we cannot domain describe what we mean by simulation —
- or rather: any such domain description becomes the domain requirements.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Net Representation

- Net representation " in the machine":
  - ⋆ The road net must be represented: segments, junctions and signals.
  - ⋆ Segment, junction and signal states must be represented.
  - ⋆ Segment lengths and segment and junction (e.g., average) "traversal" times must be represented.
  - ⋆ Vehicle positions in segments and junctions must be represented.
- Assumptions: Vehicles, when moving, move at average speed plus/minus some minor deviations.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Simulation Concepts

We suggest, not as part of the requirements, but as a software implementation idea, the following two ideas:

- Representation of segment geodetic profile:
  - ⋆ A segment is decomposed into geodetic blocks.
  - ⋆ The curvature of each block is represented by two 3D vectors, from which a Bezier curve for that block can be constructed.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

- Representation of segment velocity profile:
  - ⋆ A segment is decomposed into velocity blocks.
  - ⋆ The increase/decrease of speed for each block can be represented by two 2D vectors, from which a Bezier velocity curve for that block can be constructed:
    - ◇ The computation of the curve will, depending on vector characteristics (long or short vectors), compute close, or less close, or "far away" points on the curve,
    - ◇ and we shall take the varying density of these computed points to designate positions of a vehicle at any one time,
    - ◇ one vehicle per computation of the velocity curve.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Traffic Simulation Functions

- Initialise states of segments and junctions wrt. signals.
- Initialise states of segments and junctions wrt. vehicle positions.
  - ⋆ That is: allow vehicles to start their journey
    - ◇ along segments and in junctions when the simukation begins, and/or
    - ◇ at different times during the simulation (say according to some time table).
- Schedule simulation interval and resolution (granularity, i.e., one unit of simulation time = R units or real time.[4]).
- "Play, stop, recommence" simulation.
- Change granularity while "playing".
- Insert vehicles during simulation.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[4] R can be any real above 0. If R is less than 1 simulation is microscopic, if it is 1 simulation is "real", if it is larger than 1 simulation is macroscopic.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domain to Requirements Operations

- **Projection:** We project away almost all but the net and time tables. We adhere to definition of traffic (i.e., TF).
- **Instantiation:** We instantiate to a specific net.
- **Determination:** We may decide to constrain to segment-determined constant velocity traffic.
- ***Etcetera!***

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

'Transport Logistics' Software

- We propose a software package to be developed for
- supporting freight (incl. container) transport logistics.

Domain Description: An Extension

- In the domain planning a journey, for travelling (on a crucial trip) as a passenger on trains, by bus, airplane or by ship, usually requires the use of one or more time tables.
- Considerations of alternative routes, of multi modal travel, of cost: fast, perhaps expensive, hrried travel versus slower, perhaps less costly, and of overnight stays en route may be important.
- This applies to freight transport too: refrigeration of freight load, "first to market", etc.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Domain Requirements

• Net Representation "In the Machine"

- The multi modal net must be represented: segments and junctions
- Segment lengths and average traversal times and traversal costs of segments and junctions[5] must be represented —
- usually the latter (times and costs) are provided by transport vehicle (truck, train, boat and aircraft) time tables.

We may thus discover that we need to **extend** our domain description:

- Junction hubs, where freight is transferred from one modality transport to another, may need be further detailed, e.g., as to warehouse facilities (godowns), etc.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[5] The traversal time and cost of junctions could be differentiated wrt. modalities: freight being unload/loaded when incoming and outgoing segment modalities are different, etc.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

• Logistics Functions

- $\mathcal{E}$tcetera !

Domain to Requirements Operations

- **Projection:** The net, its segments and junctions, their length, time, and cost attributes. Also time tables. Most functions related to these.
- **Instantiation:** Maybe we instantiate to only a shipping net, or only a rail net?
- **Determination:** As a representation of the segment and junction traversal times we may rely on the time tables.
- ***$\mathcal{E}$tcetera!***

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Requirements Prescription of Shared Software

- All four rough sketch requirements prescriptions projected into their requirements a core of the net, its segments and junctions.
- We therefore conclude
  - ⋆ that a repository, i.e., a database, is needed,
  - ⋆ one in which segments and junctions are stored.
  - ⋆ A repository (software system) which allows
    - ◇ flexible representation of segment and junction attributes and
    - ◇ their initialisation, retrieval and update.
  - ⋆ So we decide on using some relational database management system.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Net Repository (i.e., Net Database)

Informal Rough Sketch

- Segment representations are in the form of relation tuples.
- Segment attributes are attributes of relations.
- Junction representations are in the form of relation tuples.
- Junction attributes are attributes of relations.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Formalisation — a Sketch

type

SR = ST**-set**
JR = JT**-set**
ST :: si:Si ftj:Jip m:M le:L ti:TI k:K f:F sσ:SΣ sω:SΩ
JT :: ji:Ji si:Si**-set** m:M ti:TI k:K f:F jσ:JΣ jω:JΩ

- This is noit quite first normal form relational representation.
- A junction connected to n segments and with a state-space of m possible states — in (primitive) first normal form would require $m \times n$ tuples.
- Of course "smarter" ways of representing sets of segment identifiers and state space (ω) can be devised. That is not a requirements issue, but a software design issue.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Repository Functions

Rough Sketch Ideas

- The observer functions of the domain description are now simple tuple projections.
- Query facilities offered by the relational DBMS[6] being deployed can be used in connection with many of the functions transformed from the domain description into the specific domain requirements prescriptions. They are the functions that make "heavy" use of observer functions.
- The various domain requirements prescriptions additionally prescribe repository initialisation and refreshment (i.e., update) functions — and again their design and implementation can be greatly facilitated by the update functions of the chosen relational DBMS.
- Of course, queries "against" an RDBMS really deposit results in a designated workspace and displays this on the GUI.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[6] DBMS: Database Management System, like Frontbase www.frontbase.com **the best**, or DB2 www.ibm.com/db2 or SQL www.oracle.com.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Specific Function Signatures

value

obs_Jip: S → Jip

sql_project: RelNm×{|"`si=seg_name`"|}×{|"`ftj`"|}×Wn → Jip×GUI

- The former function is the "further undefined" domain specification observer function.
- The latter function "approximates" an SQL query — where we do not show the functional arguments for the RDBMS and the workspace.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

"General" Function Signatures

- We intimate database
  - ⋆ retrieve (query, observer),
  - ⋆ initialise, and
  - ⋆ refresh (update),

  function signatures:

value

query: retrive_function × RDBMS × Wn → GUI
init: (S|J)**-set** × RDBMS → RDBMS × GUI
refresh: (S|J)**-set** × RDBMS → RDBMS × GUI

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

And So On!

What Have we Covered

- We have given a rather large fragment of a **domain description**.
- We have postulated and given small fragments of four **domain requirement prescriptions**.
- We have indicated how these domain requirements were **"derived"** from the domain description.
- We have formalised the domain description.
- We hardly formalises the domain requirements. But could (easily) do that!
- The four domain requirements reflect **different problem frames**.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

DTU

Domains, Requirements and Problem Frames

- We claim to have intimated the following problem frames (PF):
  - ⋆ **Maintenance**: **Weak Reactive**[7] ⊕ II PF
  - ⋆ **Traffic Control**: **Strong Reactive**[8] ⊕ II PF.
  - ⋆ **Simulation**: **Computation** ⊕ **Virtual Real-time** ⊕ II PF.
  - ⋆ **Logistics**: **Computation** ⊕ II PF.
  - ⋆ **Common Software**: **II: Information Intensive** PF.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[7] Weak reactive: Non real-time
[8] Strong reactive: "Critical" (i.e., hard) real-time

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

The Triptych and the Problem Frame Approaches

General Observations

- The triptych approach advises that software development includes:
  - ⋆ domain engineering (**DE**),
  - ⋆ requirements engineering (**RE**), and
  - ⋆ software design (**SD**).
- The triptych approach **does not replace** the PF approach.
- To me the triptych approach **augments, supplements** the PF approach.

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Specific Observations

- The triptych approach
  - ⋆ does not mandate strict linear adherence to **DE → RE → SD**
  - ⋆ but assumes **DE ↔ RE ↔ SD ↔ DE** iteration.
- In fact:
  - ⋆ It is impossible to "discover"
    - ◇ all that is relevant about the domain
    - ◇ before proceeding to understand the requirements,

    and
    - ◇ all that is relevant about the requirements
    - ◇ before proceeding to design the software,
  - ⋆ $\mathcal{E}$tcetera!

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Grand Challenges of Computing Science

The Grand Challenge of VSTTE

- The GC of VSTTE[9] to me
  - ⋆ appears to focus on "a million lines" of program code
  - ⋆ that to me appears to be verified
  - ⋆ with respect to program code annotations
  - ⋆ where it is not clear to what extent those annotations
  - ⋆ relate to properties of the code,
  - ⋆ to requirements, and
  - ⋆ to domain assumptions.

-761-51-1275, Fax: +81-761-51-1149

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[9] VSTTE: Verified Software: Theories, Techniques and Experiments

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

The Grand Challenge of Ubiquitous Computing

- The grand challenge of **ubiquitous computing** appears to offer a very nice opportunity for a "foothill"[10] experimental project.
  - ⋆ Take the proposed **Automated Highway** project.
  - ⋆ As it could be conceived one is thinking of deploying computers and communication wherever feasible (sometime in future) in the safe and efficient driving of cars, in sorting out cross traffic, etc.
  - ⋆ So here a far more detailed domain description of transportation nets than intimated here is needed.
  - ⋆ Etcetera!

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[10] "Foothill" project: This is one of those terible "americanisms": apparently used to characterise a pre-cursor like, or aerhaps rather intial stage project.

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Conclusion

- So I immodestly propose
  - ⋆ that research into and use of the PF approach be augmented by research into and use of the triptych approach,

  and
  - ⋆ to adjoin the ("otherwise") highly laudable VSTTE effort
  - ⋆ with some serious, viz., triptych-oriented program code development.
- I hope to be able to contribute to the grand challenge of ubiquitous computing.

-761-51-1275, Fax: +81-761-51-1149

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

DTU

Thanks

E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner