Opening

- **Title of Lectures:**

  Domains and Domain Enginering

- **Lecturer:**

  Dines Bjørner (DB)

- **Affiliations:**

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

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

Background for Lectures & their Objectives

- Software developed today still suffers from

  (a) not being the right software

  (b) and that the software is not right, i.e., correct ($\models$).

- (a) Software engineers do not professionally understand the domain (the environment, the context) of the software.
- (b) In proofs of correctness of software (S) wrt. requirements (R) assumptions are often made about the domain (D):

  $D, S \models R$

- Hence we must include domain engineering as a prerequisite for requirements engineering and software design.

Thus: Aims & Objectives

- Aims: What we cover
- Objectives: What we wish to achieve

Aims

- Cover essential aspects of a methodology of domain engineering.
- Link domain engineering to requirements engineering.

Objectives

- To achieve that the audience in future will possess a new software engineering dimension, namely that software engineering must rely on domain engineering.
- To encourage the research and development (the R&D) of domain models (domain descriptions) of "large scale" domains — possibly in "large scale, grand challenge" R&D between government, academia and industry.

Structure / Contents of 4 Lectures

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

2nd + 3rd Examples: ‘The Market’ + Financial Services

Domain Description Principles

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

4th Example:

Domain Facets

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

5th Example Public Government

A Glimpse of Requirements Engineering

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

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

Closing

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

On Examples

- The lectures will hinge, i.e., depend on examples.
- These will then be systematically commented.
- Formalisations will not be explained.
  - ⋆ Formalisation, hand-in-hand with the indispensable narrative
  - ⋆ is, however, essential in proper, professional software engineering
  - ⋆ as is the use of mathematics in all other branches of engineering.
- We show formulas,
  - ⋆ but only in small fontsize
  - ⋆ so that you should not be able to read them,
  - ⋆ but so that we have substantiated our claim.

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

On Lecturing Material

1. Dines Bjørner. **Software Engineering**, **Vol. 1: Abstraction and Modelling**. Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006.
2. Dines Bjørner. **Software Engineering**, **Vol. 2: Specification of Systems and Languages**. Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006. Chapters 12–14 are primarily authored by Christian Krog Madsen.
3. Dines Bjørner. **Software Engineering**, **Vol. 3: Domains, Requirements and Software Design**. Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006.

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

Topic 1

Overview of Domain Engineering

Structure of Rest of Today's Lecture

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

Example Transportation

- By transport[1] we mean
  - ⋆ that **something**, a transport item,
  - ⋆ is being **moved** (i.e., transported),
  - ⋆ along a **route** (of a transport net of junctions and segments)
  - ⋆ by a **conveyour**
  - ⋆ exerting a locomotive **force** (on the transport item).
- We shall only describe some of these aspects.

[1]— following the German philosopher Hegel, around 1830

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

- **Please note:**
  - ⋆ **Before setting out, take time to reflect**
  - ⋆ **on a proper characterisation, as above,**
  - ⋆ **of what the major domain concept is ontologically.**

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

Net Topology

- We shall think of nets having topology, i.e., “layout” of segments and junctions.
- We conceptualise as segments the physically manifest phenomena of
  - ⋆ roads (between adjacent street intersections),
  - ⋆ rail tracks (between adjacent train stations),
  - ⋆ air lanes (between adjacent airports) and
  - ⋆ shipping lanes (between adjacent harbours).
- We likewise conceptualise as junctions
  - ⋆ street intersections, train stations, airports and harbours.

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

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

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

Annotations:

- N, S, J are considered abstract types, i.e., sorts. N, S and J are type names, i.e., names of types of values. Values of type N are nets, values of type S are segments and values of type J are junctions.
- One can observe from nets, n, their (one or more) segments (obs_Ss(n)) and their (two or more) junctions (obs_Js(n)); n is a value of type N.
- Functions have names, obs_Ss, and obs_Js, and functions, f, have signatures, f: A $\rightarrow$ B (not illustrated), where A and B are type names. A designates the definition set of f and B the range set.
- A-set is a type expression. It denotes the type whose values are finite, possibly empty set of A values.
- These observer functions are postulated.
- They cannot be formally defined.
- They are "defined" once a net has been pointed out[2]
- The axiom expresses that in any net there is at lest one segment and at least two junctions.

[2] Take the transportation net Europe. By inspecting it, and by deciding which segments and which associated junctions to focus on (i.e., "the interesting ones") we know which are all the interesting roads, rail tracks, air lanes and shipping lanes, respectively the interesting (associated) street intersections, trains stations, airports and harbours.

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

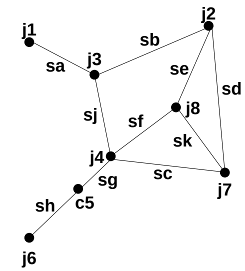


Figure 2.1: A simple net of segments and junctions

Applying the observer functions to the net of Fig. 2.1 yields:

obs_Ss(n) = {sa,sb,sc,sd,se,sf,sg,sh,sj,sk}
obs_Js(n) = {j1,j2,j3,j4,j5,j6,j7,j8}

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 $\rightarrow$ Si
  obs_Ji: J $\rightarrow$ Ji

Segment and junction identifications are abstract concepts.

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.
4. And no two junctions have the same junction identifier.

axiom
  $\forall$ n:N $\cdot$ **card** obs_Ss(n) $\equiv$ **card** {obs_Si(s)|s:S $\cdot$ s $\in$ obs_Ss(n)}
  $\forall$ n:N $\cdot$ **card** obs_Js(n) $\equiv$ **card** {obs_Ji(c)|j:J $\cdot$ j $\in$ obs_Js(n)}

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

Annotations:

- **card** set expresses the cardinality of the set set, i.e., its number of distinct elements.
- {f(a)|a:A · p(a)} expresses the set of all those B elements f(a) where a is of type A and has property p(a) [where we do not further state f, A and B. p is a predicate, i.e., a function, here from A into truth values of type **Bool**, for Boolean].
- The axioms now express that the number of segments in n is the same as the number of segment identifiers of n — which is a circumscription for: No two segments have the same segment identifier.
- Similar for junctions.

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

Segment and Junction Reference Identifications

5. Segments are delimited by two distinct junctions.
6. 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

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

Annotations:

- {|a:A · p(a)|} is a subtype expression. It expresses a subset of type A, namely those A values which enjoys property p(a) [p is a predicate, i.e., a function, here from A into truth values in the type **Bool**]. In the above p(a) is ji≠ji′.
- In this case Jip is the subtype of Ji-**set** whose values are exactly 2 element sets of Ji elements.

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

7. Any junction has a finite, but non-zero number of segments connected to it.
8. 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

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

Annotations:

- Si1 is the type whose values are non-empty, but still finite sets of Si values.

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

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

axiom
$\forall$ n:N, s:S • s $\in$ obs_Ss(n) $\Rightarrow$
  let {ji,ji′} = obs_Jis(s) **in**
  $\exists!$ j,j′:J • {j,j′}$\subseteq$obs_Js(n) $\wedge$ j$\neq$j′ $\wedge$
    obs_Si(s) $\in$ obs_Sis(c) $\cap$ obs_Sis(c′) **end**

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

Annotations:

- We read the above axiom:
  - ⋆ for all nets n and for all segments s in n
  - ⋆ let ji and ji′be the two distinct junction identifications observable from s, then
  - ⋆ exists exactly two distinct junctions, j and j′ of the net,
  - ⋆ such that the segment identification of s is in both the sets of segment identifications observable from j and j′.

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

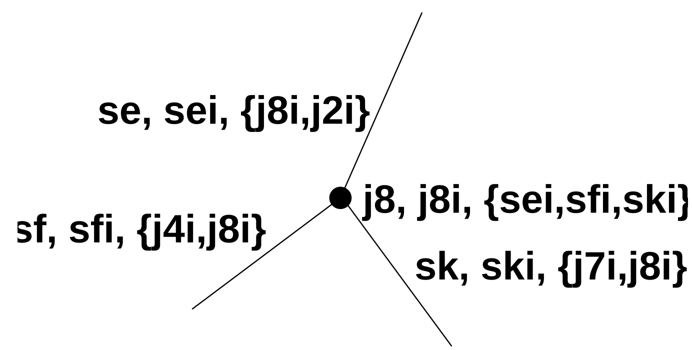


Figure 2.2: One junction and its connected segments

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

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

axiom
  ∀ n:N, j:J • j ∈ obs_Js(n) ⇒
    let sis = obs_Sis(c), ji = obs_Ji(j) **in**
    ∃! ss:S-**set** • ss⊆obs_Ss(n) ∧ **card** ss=**card** sis ∧
    sis = {|obs_Si(s)|s:S•s ∈ ss|} **end**

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

Annotations:

- Let us read the above axiom:
  - ⋆ for all nets, n, and all junctions, j, of that net
  - ⋆ let sis be the set of segment identifications observed from j, and let ji be the junction identifier of j, then
  - ⋆ there exists a unique set, ss, of segments of n with as many segments as there are segment identifications in sis, and such that
  - ⋆ sis is exactly the set of segment identifications of segments in ss.

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

Paths and Routes

11. By a path we shall understand a triplet of
    (a) a junction identification,
    (b) a segment identification and
    (c) 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)}

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

Annotations:

- Paths are modelled as Cartesians.
- One can generate all the paths of a net.
- It is the set of path triplets, two for each segment of the net and such that the pair of junction identifications, ji and ji′, observable from a segment is at either “end” of the triplet, and such that the segment identification is common to the two triplets (and in the “middle”).

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

12. By a route of a net we shall understand a list, i.e., a sequence of paths as follows:
    (a) A sequence of just one path of the net is a route.
    (b) If r and r′ are routes of the net
        i. such that the last junction identification, ji, of the last path, (_,_,ji) of r
        ii. and the first junction identification, ji′, of the first path (ji′,_,_) of r′
        iii. are the same, i.e., ji=ji′,
        iv. then $r \frown r'$ is a route.
    (c) 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.

-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

```
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
```

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

Annotations:

- Routes are well-formed sequences of paths.
- A sequence of paths is a well-formed route if adjacent path elements of the route share junction identification.
- Give a net we can compute all its routes as follows:
  - ⋆ let rs be the set of routes to be computed. It consists first of all the single path routes of the net.
  - ⋆ Then rs also contains the concatenation of all pairs of routes, r and r′, such that these are members of rs and such that their concatenation is a well-formed route.
  - ⋆ If the net is circular then the set rs is an infinite set of routes. The least fix point of the recursive equation in rs is the solution to the "routes" computation.

-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

13. 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
```

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

Annotations:

- A net n is connected if
  - ⋆ for all two distinct connectors of the net
  - ⋆ where ji and ji′ are their junction identifications,
  - ⋆ there exists a route, r, of the net,
  - ⋆ whose first junction identification is ji and whose last junction identification is ji′.

-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

Net Decomposition

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

+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


```
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′) ∧ ...
```

-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

Annotations:

- A set ns of nets constitutes a decomposition of a net, n,
  (a) if all the segments of n appear in some net of ns,
  (b) if all the junctions of n appear in some net of ns,
  (c) if no two or more distinct nets of ns share segments,
  (d) if no two or more distinct nets of ns share junctions, and
  (e) if all nets of ns are connected.
- **Comment:** It appears that items 3 and 4 are unnecessary, that is, are properties once items 1, 2 and 5 hold.

That is, we have the following:

Lemma:

```
∀ n:N •
  let ns = decompose (n) in
  ∀ n′,n″:N • {n′,n″}⊆ns ∧ n′≠n″ ⇒
    obs_Ss(n′) ∩ obs_Ss(n″) = {} ∧
    obs_Js(n′) ∩ obs_Js(n″) = {} end
```

+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

Multi-Modal Nets

General Issues

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

```
type
  M
```


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

Segment and Junction Modes

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

```
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
```


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

Annotations:

- From a segment one can observe its mode.
- From a junction one can observe its set of modes.
- Let us read the first axiom:
  - ⋆ for all net, n, and all junctions, j, of that net
  - ⋆ let ss be the set of segments connected to j,
  - ⋆ now the set of modes of c is equal to the set of modes of the segments in ss.
- Let us read the second axiom:
  - ⋆ for all net, n, and all segments, s, of that net
  - ⋆ let ji and ji′ be the junction identifiers of the two junctions to which s is connected, and
  - ⋆ let j and j′ be the two corresponding junctions,
  - ⋆ then the segment mode is in both the set of modes of the two junctions.

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

- We can define a function, xtr_Ss, which from a net, n, and a junction identification, ji, extracts the set of segments, ss, connected to the junction identified by ji.
- xtr_Ss(n,ji) yields the set of segments, ss, in the net n for which ji is one of the observed junction identifications of s.
- And we can define a function, xtr_J, of signature N × Ji → J, which when applied to a net, n, and a junction identification, ji,
- extracts the junction in the net which has that junction identifier.

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

Single-Modal Nets and Net Projection

20. Given a multi-modal net
    (a) one can project it onto a set of single modality nets,
    (b) 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)}

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

proj: N × M → smN
proj(n,m) **as** n′
  post
    let ss = obs_Ss(n), ss′ = obs_Ss(n′),
        js = obs_Js(n), js′ = obs_Js(n′) **in**
    ss′ = {s | s:S • s ∈ ss ∧ m=obs_M(s)} ∧
    js′ = {j | j:J • j ∈ js ∧ m ∈ obs_Ms(j)}
    end

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

Annotations:

- A multi-modal net is a net with more than one mode. mmN is thus the subtype of nets, n:N, which are multi-modal.
- A single-modal net is a net with exactly one mode. smN is thus the subtype of nets, n:N, which are multi-modal.
- The xtr_Ms function extracts the mode of every segment of a net.
- The projs function applies to any net, n:N, and yields the set of single-modal subnets of n, one for each mode of n. The projs function makes use of the proj function.

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

- The proj function applies to any n, n:N, and any mode of that net, and yields the single-modal subnet on n whose mode is the given mode.
  - ⋆ The proj function is expressed by a post condition, i.e., a predicate that characterises the necessary and sufficient relation between the argument net, n, and the result net n′.
  - ⋆ In a single-modal net, n′, projected from a multi-modal net, n, and of mode m, we keep exactly those segments, ss′, of n whose mode is m,
  - ⋆ and we keep exactly those junctions, js′, of n whose mode contains m.
  - ⋆ No more is needed in order to express the necessary and sufficient condition for a single-modal net to be a subnet of a proper net.
  - ⋆ That is, some single-modal nets are not proper nets since in proper nets every junction have the set of modes of all the segments connected to the junction.

Segment and Junction Attributes

• Segment and Junction Attribute Observations

We now enrich our segments and junctions.

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

    (One can think of (tabulated) varieties of transport times.)

24. Junctions have standard transfer time per modality of transport between pairs of segments connected to the junction.
25. Junctions have standard arrival time per modality of transport.
26. Junctions have standard departure times per modality of transport.
27. Segments have standard costs of transporting a unit of freight from one end of the segment to the other end.
28. Junctions have standard costs of transporting a unit of freight from the end of one connecting segment to the beginning of another connecting segment.

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.


```
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
```

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

Annotations:

- L and Ti are sorts designating length and time values.
- ms denotes a non-empty set of modes.
- From a segment one can observe, obs_L, its length.
- From a segment one can observe, obs_TI, a time duration for a normal conveyour of the mode of the segment to travel the length of the segment.

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

- From a junction and a mode (of that junction) one can observe, obs_TI, a time duration for a normal conveyour of the mode to cross, i.e., to travel through the junction.
- From a junction and a pair of modes (m and m′ of that junction) one can observe, obs_TI, a time duration which represents the normal time it takes to transfer freight from a conveyour of mode m to a conveyour of mode m′. (The two modes may be the same.)
- From a junction and a mode (of that junction) one can observe, obs_arr_TI, a time duration for an item of freight destined for a normal conveyour of the mode to arrive and be "entry" processed (including loaded) at that junction.
- From a junction and a mode (of that junction) one can observe, obs_dep_TI, a time duration for an item of freight destined for a normal conveyour of the mode to arrive and be "exit" processed (including unloaded) at that junction.
- One can add lengths.
- One can add time durations.

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

• Route Lengths

29. One can talk about the length of a route of a net:
   (a) If the route is empty, the length is 0.
   (b) If the route consists of a single path, i.e., a segment
      i. then the length of the route is the length of the segment.
   (c) If the route r consists of a path connected — at junction j — to a non-empty route r' then the length of route r is
      i. the length of the segment of the path,
      ii. plus the traversal lenght of the junction from the incoming route segment to the outgoing route segment
      iii. plus the length of the remaining route, i.e., of r'.

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

```
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
```

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

30. and one can talk about the shortest such route between two identified junctions *jf* and *jt* of a net *n*.
    (a) Ler *rs* be the set of all routes of the net *n*.
    (b) Ler *crs* be that subset of *rs* whise members are routes from *jf* to *jt*.
    (c) Let *sr* be a route in *crs* such that there does not exist another route *r* in *crs* which is shorter.
    (d) Then *sr* is a desired shortest route in the net *n* from junction *jf* to junction *jt*.

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 ∼→ 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
```


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

Annotations:

- The length of a single modality route of a net
  - ⋆ is 0 if the route is empty,
  - ⋆ otherwise it is the length of the first segment of the route plus the length of the rest of the route computed as follows:
    - ◇ If the route consists of just one segment, then 0,
    - ◇ else, the length of the junction from incident segment to emanating segment plus
    - ◇ the length of the rest of the route computed as otherwise specified above.
- The shortest route of a net between two of its identified junctions (the precondition) can be abstractly determined as follows:
  - ⋆ First we find all the routes, rs, of the net.
  - ⋆ Then we find those routes, crs, whose first and last junction identifications are the given ones, jf and jt.
  - ⋆ Amongst those we find a shortest one, that is, one, in crs, for which there are no shorter routes, r, in crs.

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

Route Traversal Times

31. One can describe the total time it takes to traverse a route, including the times it takes to pass through a junction.
32. It is the sum of three time durations:
    (a) the time it takes to arrive at the first segment from the fist junction — given the mode of that segment,
    (b) the time to traverse the route (where that "time duration" can be described very much like was the route length), and
    (c) the time to leave (depart) the last junction — given the mode of the last segment.

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

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)))

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

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

33. and one can describe the quickest route between two identified junctions — very much like was the shortest route.

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) **in**
  qr **end end end**

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

Transportation Costs

34. We can further describe
   (a) transport cost (tk:TK),
   (b) lowest (per unit) freight cost (fk:FK) between two junctions,
   (c) etc.

   We assume

   (d) that if a freight item is transported into a junction and out of that junction by the same modality conveyour,
   (e) then it is not reloaded, i.e., along segments of the same modality.[3]

[3] 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

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

  cost: R → N → K
  cost(r)(n) ≡
    case r **of**
      ⟨⟩ → 0,
      ⟨(jf,si,jt)⟩ →
        obs_K(xtr_J(jf,n))+obs_K(xtr_S(si,n))+obs_K(xtr_J(jt,n))
      ⟨(jf,si,jt),(jf′,si′,jt′)⟩⌢r′ → **assert:** jt=jf′
        obs_K(xtr_J(jf,n))+obs_K(xtr_S(si,n))+...+cost(r′)
    end

  cheapest: Ji×Ji → N → ((K×K)→K) → ((K×K)→**Bool**) → R
  cheapest(jf,jt)(n) ≡ best(jf,jt)(n)(λ(k1,k2):(K×K)•k1+k2)(λ(k1,k2):(K×K)•k1<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

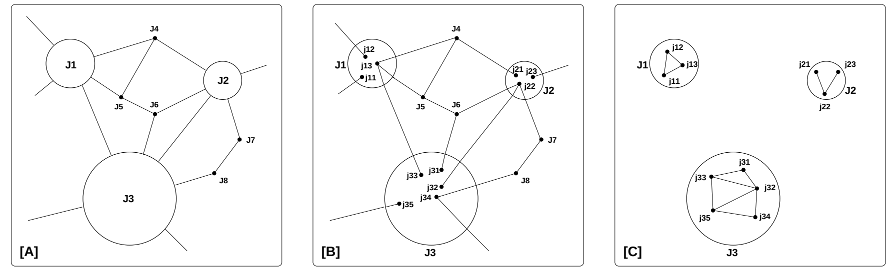


Figure 2.3: Gross [A] versus semi-detailed [B] road net — and community road nets [C]

35. Figure [A] 2.3 shows a road net.
    (a) Instead of showing junctions J1, J2 and J3 as small black disks
    (b) we show them as larger circles —
    (c) for reasons that transpires from Fig. [B] 2.3.

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

36. Junctions J1, J2 and J3 are considered composite, that is, to represent communities.
37. We may consider the road net of Fig.[A] 2.3 on the facing page to be an abstraction of the road net hinted at in Fig.[B] 2.3 on the preceding page.
38. Junctions j11, j12, . . . , j35 are considered simple embedded junctions.
39. We decide to allow three kinds of junctions:
    (a) composite,
    (b) simple embedded and
    (c) simple.

    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

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

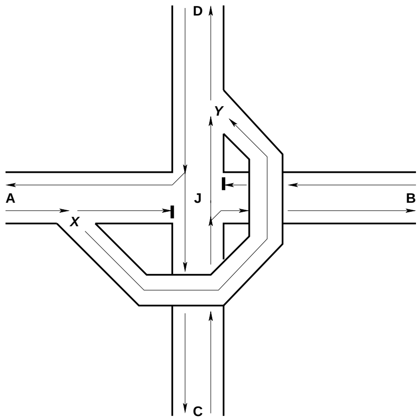


Figure 2.4: A Special "Carrefour" Junction

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

40. 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.
41. 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.

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

42. Junctions may direct traffic from any subset of incident segments to any subset of emanating segments.
43. 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.

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


```
type
  SΣ = (Ji×Ji)-set
  JΣ = (Si×Si)-set
value
  obs_SΣ: S → SΣ
  obs_JΣ: J → JΣ

  xtr_Jis: SΣ → Ji-set, xtr_Jis(sσ) ≡ {ji|ji:Ji • (ji,_) ∈ obs_sσ ∨ (_,ji) ∈ obs_sσ}
  xtr_Sis: JΣ → Si-set, xtr_Sis(jσ) ≡ {si|si:Si • (si,_) ∈ obs_jσ ∨ (_,si) ∈ obs_jσ}
axiom
  ∀ s:S • xtr_Jis(obs_SΣ(s)) ⊆ xtr_Jip(s),
  ∀ j:J • xtr_Sis(obs_JΣ(j)) ⊆ xtr_Sis(j)
```

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

Observations:

- A junction, $j : J$, of just one segment, $s : S$, that is, s is a cul de sac, may either be closed, and vehicles trying to enter j will be queued up, or it is open, and vehicles entering j will be lead back to s.
- As a consequence segment s, in order for this latter routing to happen, must be open in both directions when j is "open".
- In general, if the state of a junction j (identified by ji) contains a pair (si_x, si_y) then the state of the designated segments, sx and sy, must respectively contain pairs (ji', ji), respectively (ji, ji''), where $\{ji, ji'\}$ and $(ji, ji''\}$ are the pairs of junction identifications associated with si_x and si_y respectively.
- And this must hold for all states of junctions and adjacent segments.
- This is captured in the axioms below.

axiom

...

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

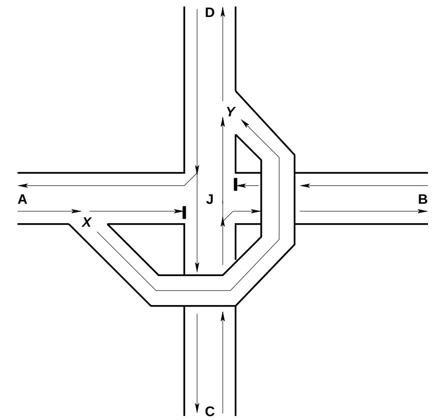


Figure 2.5: A Special "Carrefour" Junction

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

44. The junction of (repeated) Fig. 2.5 shows four segments, identified by *A*, *B*, *C* and *D*.
45. The figure also suggests a state in which traffic lights prohibit movements from *A* into *J*, from *B* into *J*,
46. from *C* via *J* into *A*, and from *D* via *J* into *B*.
47. The "bypass" from *A*/*X* into *Y*/*D* appears to be such that traffic can always pass from *A* into *D*.
48. The current state alluded to in Fig. 2.4 on page 69 appears to be:

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

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

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

Segment and Junction State Spaces

50. A segment can be in one of several segments states.
51. A junction can be in one of several junction states.
52. Hence we introduce segment and junction state spaces.

type
  SΩ = SΣ-**set**
  JΩ = JΣ-**set**
value
  obs_SΩ: S → SΩ
  obs_JΩ: J → JΩ
axiom
  ∀ s:S • obs_SΣ(s) ⊆ obs_SΩ(s),
  ∀ j:J • obs_JΣ(j) ⊆ obs_JΩ(j)

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

More on Net Dynamics: Traffic

• Vehicles and Positions

53. There is a further undefined notion of vehicles, V.

type
  V

54. 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

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

      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)

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

Traffic

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

type
  T
  TF = T $\overrightarrow{m}$ (N × (V $\overrightarrow{m}$ P))

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

• Proper Vehicle Positions

56. 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

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

• Other Traffic Constraints

57. Traffic must be smooth: Positions of vehicles do not "jump around", i.e., movement are monotonic.
58. 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.

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
  $\mathsf{TT} = \mathsf{Vn} \underset{m}{\rightarrow} \mathsf{Journey}$
  $\mathsf{Journey} = (\mathsf{at{:}T} \times \mathsf{ji{:}Ji} \times \mathsf{dt{:}T})^*$

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: $\forall$ tf:TF • tf $\in$ tfs $\Rightarrow$ wf_TF(tf) $\wedge$ sat(tf,tt)

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

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.

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

Characterisation of Domains and Their Description

- So which can be examples of domains?
  - ⋆ airports,
  - ⋆ air traffic,
  - √ the financial service industry
  - ⋆ (container) freight logistics,
  - ⋆ healthcare,
  - ⋆ manufacturing,
  - √ "the market"
  - √ public administration,
  - √ transportation
    - ◇ airline
    - ◇ train
    - ◇ automobile
    - ◇ shipping
  - ⋆ etc.
- The √s designate domains that has been or will be partially exemplified.
- Volume 3 Sect. 1.2.1 and Chap. 8 characterises the concept of 'domain' more properly.

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

Justification of Domain Engineering

The Dogma and The Triptych

- The dogma:
  - ⋆ Before software cen be designed
  - ⋆ one must its requirements.
  - ⋆ Before requirements can be formulated
  - ⋆ one must understand the domain.
- The triptych model of software development:
  - ⋆ domain engineering,
  - ⋆ requirements engineering, and
  - ⋆ software design.

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

Physics and Classical Engineering

- Physics is at the "bottom" of all classical engineering.
- Noone in their right mind would hire an
  - ⋆ aeronautics, an automotive, a telecommunications, etc., engineer
  - ⋆ unless that person had a solid degree in the subject field,
  - ⋆ one that included a firm basis in physics
  - ⋆ and in the mathematics "to go with it":
  - ⋆ calculus, graph theory, combinatorics, statistics, probability, etc.
- Software engineers
  - ⋆ not onlyh shy away from much simpler math: discrete math,
  - ⋆ but most, in their practice, do not bother about asking about an underlying theory of the application domain.

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

Phases of Domain Engineering

1. Domain Stakeholders
2. Domain Acquisition
3. Domain Analysis
4. Domain Modeling
5. Domain Verification
6. Domain Validation
7. Domain Theory

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

Domain Stakeholders

- In acquiring knowledge about the domain one need inquire with a widest spectrum of stakeholders:
  - ⋆ domain (segment) owners,
  - ⋆ all levels of management,
  - ⋆ all shades of workers,
  - ⋆ users,
  - ⋆ most shades of suppliers,
  - ⋆ regulators and public admin.,
  - ⋆ local and state politicians,
  - ⋆ etc.
- A serious effort must be made to establish and maintain strong liaison to all stakeholders.
- Stakeholders have a right to be heard and informed wrt. both domain and requirements engineering results.

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

Domain Acquisition

- For domain acquisition to succeed
- the domain engineer must be intimately familiar with
- what goes into a proper domain description (i.e., domain model).

Acquisition Modes

1. Hermeneutics[4], that is, studying texts on the domain.
2. From informal chats to semi-systematic discussions with 3-4 different stakeholder groups of the domain.
3. Rough sketch informal and formal domain modelling.
4. Formulation of serious questionaire forms (Q-forms).
5. Questionnairing: helping stakeholders to fill out the Q-forms.
6. Sorting and indexing Q-forms.
7. Possible reiteration of steps (1.–6.).

[4] Wikipedia: Hermeneutics is a philosophical technique concerned with the interpretation and understanding of texts. It may be described as the theory of the interpretation and understanding of a text on the basis of the text itself. The concept of "text" has been extended beyond written documents to include, for example, speech, performances, works of art, and even events. Thus, one might speak of and interpret a "social text".

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

Questionnaire Units: Description + Attributes

- Questionnairing results in attributed description units.
- A description unit describes something.
  - ⋆ **Example:** *A street consists of several indentically (road-)named segments separated by street intersections.*
- A description unit attribute places the d-unit in a social context.
- Some d-unit attributes:
  - ⋆ Name, place and time of stakeholder and answer
  - ⋆ Stakeholder group identifier
  - ⋆ Ontological classification: Entity, function, event, behaviour
  - ⋆ Name of domain acquisitioner (i.e., domain engineer)

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

Domain Analysis

- We identify five "cases" of analysis
  - ⋆ **Concept formation**
  - ⋆ **Inconsistency analysis**
  - ⋆ **Conflict analysis**
  - ⋆ **Incompleteness analysis**
  - ⋆ Property analysis
- We shall treat property analysis under the heading of 'verification'.
- Domain analysis is a costly but necessary activitiy: time and manpower.

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

Concept Formation

- Abstraction of phenomena into concepts.
  - ⋆ **Examples:**
    - ◇ *Street, rail line, shipping lane and airlane segments into just segments.*
    - ◇ *Road intersections, train stations, harbours, and airports into junctions (or hubs).*
    - ◇ *Automobiles, trains, ships and aircraft into conveyours (or vehicles).*
- That is,
  - ⋆ from phenomena to mental ideas,
  - ⋆ from manifest, designations into definitions.

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

Inconsistency Analysis

- Often two or more description units "contradict one another".
- **Example:**
  - ⋆ *A segment is delimited by one or two junctions.*
  - ⋆ *A segment is delimited by two junctions.*
- An inconsistency, in general gives rise to provability of both P and $\neg P$.
- An inconsistecy is a "contradiction"
  - ⋆ which can be resolved through mediation by the domain engineer:
  - ⋆ reconciling the description units as expressed by the two or more stakeholders.

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

Conflict Analysis

- A conflict is a "contradiction"
  - ⋆ which can not be resolved through mediation by the domain engineer;
  - ⋆ the two or more "contradicting" stakeholders must seek reaolution from a "common boss";
  - ⋆ the two or more "contradicting" stakeholders were basically in their "full right" to disagree ("they were told so by a common boss").
- **Example:**
  - ⋆ `Road pricing politician:` *The fee for travelling a segment shall be low during week days and higher during week ends.*
  - ⋆ `Road pricing collector:` *The fee . . . shall only depend on axle pressure of automobile.*

The "common boss" here (↑) is probably the minister of transport or the paliament.

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

Incompleteness Analysis

- An incompleteness is a set of descriptions (d-units) which fail to account for "all cases".
- **Example:** *Road traffic is*
  - ⋆ *above 1000 vehicles per hour between 6 am and 9 am and between 3 pm and 7 pm,*
  - ⋆ *below 200 . . . between 10 pm and 6am,*
  - ⋆ *and varies between 400 and 600 between 10 am and 2 pm.*
- An incompleteness may need be resolved.
- Usually by the domain engineer and the appropriate stakeholder group.

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

Summary of Domain Analysis

- Concept formation, inconsistency, conflict and incompleteness analysis
  - ⋆ is based initially on description units
  - ⋆ arising from domain acquisition.
- Property analysis (verification)
  - ⋆ is based, usually,
  - ⋆ on (usually) formal descriptions (i.e., formalised models).
- Domain analysis is an
  - ⋆ indispensable,
  - ⋆ time and manpower consuming

  domain engineering activity.

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

Domain Modeling

• — the main theme of these lectures —

- Domain modeling is what these four days are mostly about!
- So I will not say so much here.
- Tuesday and Wednesday will detail a number of principles and techniques of domain description:
  - ⋆ an ontology of descriiption items,
  - ⋆ michael Jackson's desription ideas, and
  - ⋆ facets of domain models.

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

• Some Preliminary Remarks

- Suffice it to now, today, to say the following:
  - ⋆ Domain modeling collects and are based on all the domain description units.
  - ⋆ Domain description involves both establishing a "complete" terminology, an informal yet precise narrative and a formal description.
  - ⋆ Formal domain description cannot be done only in one formal specification language.
  - ⋆ Usually we combine for example [event–]B or VDM-SL or RAISE (RSL) or Z with Petri Nets, Message or Live Sequence Charts, Statecharts and Duration Calculus (DC) or TLA+.
- Thus domain modeling results in the prime document of domain engineering.

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

Domain Verification

- By domain verification we shall understand
  - ⋆ the informal reasoning or the formal proof
- of properties of a domain description.
- A domain description
  - ⋆ should express most domain properties rather immediately,
  - ⋆ but some only follows from these,
  - ⋆ so must be shown to hold.
- We shall not touch the issue of domain verification other than saying that it helps secure that the domain engineer
  - ⋆ describes the domain right (i.e., correctly).

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

Domain Validation

- By domain validation we shall understand
  - ⋆ the informal process (and the resulting document)
  - ⋆ of making sure that what has been described
  - ⋆ is what the domain stakeholders meant.
- Domain validation is necessarily an informal activity and document:
  - ⋆ the domain “itself” is only informally manifest, that is,
  - ⋆ the input to domain description was informal,
  - ⋆ and real people, the stakeholders, must “sign off” on the description.
- We shall not touch the issue of domain validation other than saying that it helps secure that the domain engineer
  - ⋆ describes the right domain right.

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

Domain Theory

- By a domain theory we understand a triplet:
  - ⋆ a formal description of some domain — in typically several relatable formal specification languages,
  - ⋆ the semantics and proof systems of these languages,
  - ⋆ and a number of proven, model checked and/or tested theorems, lemmas and propositions about the description.
- We shall not touch the issue of domain theories other than saying that it helps secure that the domain engineer
  - ⋆ achieves a proper foundation for or of the domain.
- Domain theory work can go on for decades.

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

The Contents of a Domain Engineering Development

- Domain engineering entails
  - ⋆ administrative work, relected in **informative documents**,
  - ⋆ descriptive work, relected in **descriptive documents**, and
  - ⋆ analytic work, relected in **analysis documents**.
- Some documents, notably the informative documents are necessarily informal.
- Analytic documents are meta-descriptive: proofs, model checks, tests.
- Descriptive documents should alternate between informal narratives and formal descriptions.
- We overview a contents listings of representative documents.

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

1. Information
   (a) Name, Place and Date
   (b) Partners
   (c) Current Situation
   (d) Needs and Ideas
   (e) Concepts and Facilities
   (f) Scope and Span
   (g) Assumptions and Dependencies
   (h) Implicit/Derivative Goals
   (i) Synopsis
   (j) Standards Compliance
   (k) Contracts
   (l) The Teams
      i. Management
      ii. Developers
      iii. Client Staff
      iv. Consultants

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

2. Descriptions
   (a) Stakeholders
   (b) The Acquisition Process
      i. Studies
      ii. Interviews
      iii. Questionnaires
      iv. Indexed Description Units
   (c) Terminology
   (d) Business Processes
   (e) Facets:
      i. Intrinsics
      ii. Support Technologies
      iii. Management and Organisation
      iv. Rules and Regulations
      v. Scripts
      vi. Human Behaviour
   (f) Consolidated Description

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

3. Analyses
   (a) Domain Analysis and Concept Formation
      i. Inconsistencies
      ii. Conflicts
      iii. Incompletenesses
      iv. Resolutions
   (b) Domain Validation
      i. Stakeholder Walk-Throughs
      ii. Resolutions
   (c) Domain Verification
      i. Model Checkings
      ii. Theorems and Proofs
      iii. Test Cases and Tests
   (d) (Towards a) Domain Theory

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

Lecture Summary

- We have shown a small fragment of a domain model.
- We have then, ever so briefly, surveyed important stages of the phase of domain engineering:
  - ⋆ stakeholder liaison,
  - ⋆ domain acquisition,
  - ⋆ domain analysis,
  - ⋆ domain modeling,
  - ⋆ domain verification,
  - ⋆ domain validation, and
  - ⋆ domain theory construction.
- And we have finally overviewed a contents listing of a great number of documents that arise from domain engineering.
- We are now ready, in the next two days, to go in more depth wrt. domain modeling.

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

Topic 2

Domain Description Principles

Structure of Today's Lecture

Example 'The Market'

- By 'The Market' we mean
  - ⋆ the free **exchange**
  - ⋆ of items of **value** (**merchandise, service** and **monies**)
  - ⋆ between **sellers**
  - ⋆ and **buyers**.
- The term 'free' is quite important here.
- **Please note:**
  - ⋆ Before setting out, take time to reflect
  - ⋆ on a proper characterisation, as above,
  - ⋆ of what the major domain concept is ontologically.

Buyers and Sellers

- A buyer is
  - ⋆ a person or an enterprise
  - ⋆ with cash or credit(ability)
  - ⋆ who is in the market to buy.
- A seller is
  - ⋆ a person or an enterprise
  - ⋆ with merchandise (or services)
  - ⋆ who is in the market to sell (to offer).

Buyer

- For the buyer to "be in the market" means
  - ⋆ to have an idea as what merchandise[5] to look for and to look for it (**inquire**),
  - ⋆ To possibly **order** it, **accept** (delivery of) it and an invoice, and to **pay** for it.
  - ⋆ To possibly, later, **return** it under the warranty, etc.
- All of **inquiry, ordering, acceptance**, and **payment** may be considered one action (**buy**) or a sequence of actions. Etc.

Seller

- For the seller to "be in the market" means
  - ⋆ To somehow stock merchandise.
  - ⋆ To **offer** merchandise for sale, **accept** (or **reject**) **orders**, **delivery, invoicing** and **receipt of payments**.
  - ⋆ To accept **returns** under warranty, to **repair, replace** or **credit**.
- All of **offering, accepting** or **rejecting orders, delivery, invoicing**, and **receipt of payments** may be considered one action (**sell**) or a sequence of actions. Etc.

[5] from now on we will just use the term 'merchandise' to also cover a concdept of 'service'.

Organisation of The Market

A Simplified Overview

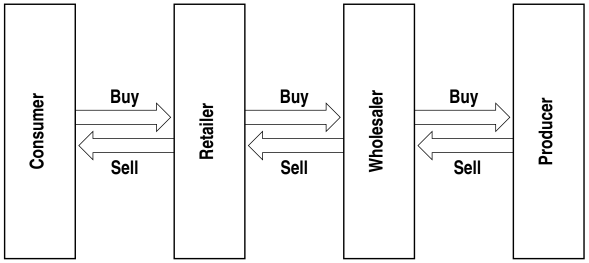


Figure 3.6: Basic Market Players — A Simplified Supply Chain

• Explanation of Fig. 3.6

- Consumers trade with retailers, retailers with consumers and wholesalers, and wholesalers with retailers and producers.
- Thus retailers and wholesalers acr both as sellers and buyers, consumers only as buyers and producers only as sellers.
- Of course, in other contexts consumers sell their services (work for an employer) and producers buy parts for production.
- The **buy** functions include **inquire, order, accept delivery, pay**, etcetera.
- The **sell** functions include **offer, accept order, deliver, invoice, accept payment**, etcetera.

A Less Simplified Overview

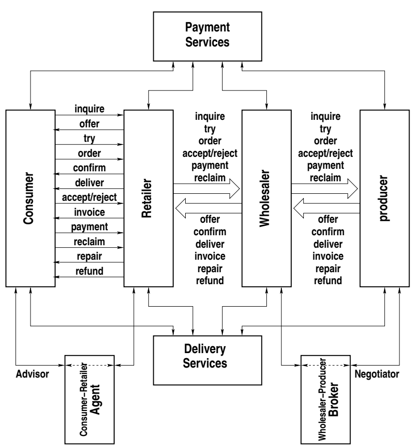


Figure 3.7: The Market Players + Details: The Supply Chain

• Explanation of Fig. 3.7

- Four additional "players" act in 'the market'.
  - ⋆ **Payment Services** (banks, credit card companies, etc.) provide (technological supports, i.e.) means of transferring funds.
  - ⋆ **Delivery Services** (seller's own truck, taxis, local truck company, DHL, FEDEX, UPS, etc.) provide (technological supports, i.e.) means of delivery.
  - ⋆ **Agents** act on behalf either of a buyer, or a seller, and provides service "for one to find the other", i.e., to accomodate a sale.
  - ⋆ **Brokers** act on behalf of both buyers and sellers and provides service for the "parties" to "find one another".
- We shall (probably) not have occasion to further describe these additional four classes of "market players".

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

Example Financial Service Industry

- By a **financial service industry** we shall understand
  - ⋆ a structure of **clients** (i.e., citizens, public and private institutions and enterprises)
  - ⋆ and such **"companies" which handle financial instruments** (monies (i.e., cash), stocks, bonds, mortgages, etc.)
  - ⋆ such that clients and financial instrument handlers **achieve a common good** in the form of
  - ⋆ the **safeguarding and increase of capital** and
  - ⋆ the **accomodation of loans**.

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

A Segment of The Financial Service Industry Structure

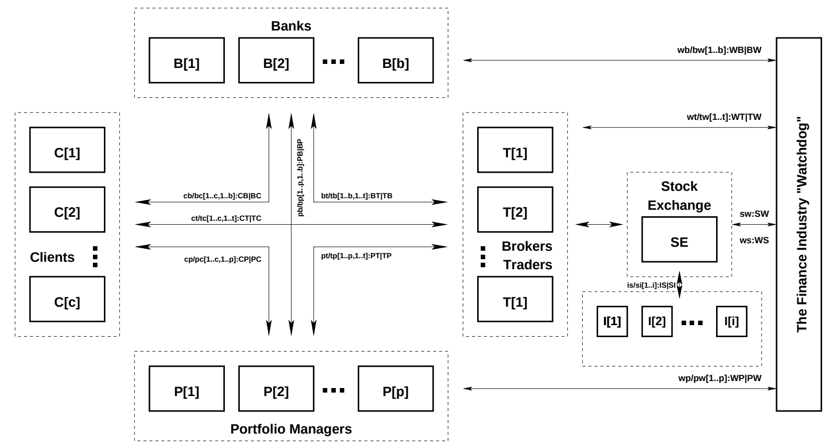


Figure 4.8: "The Financial Service Industry" — An Excerpt

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

• Explanation of Fig. 4.8

- A segment of of the **financial service industry** consists of
  - ⋆ one or more **clients** (in need of financial services),
  - ⋆ one or more **banks** offering traditional banking services (demand/deposit, savings and mortgage accounts),
  - ⋆ one or more **portfolio managers** offering capital investment services,
  - ⋆ one or more **brokers** handling placement and clearing of the buying and selling of stocks and bonds,
  - ⋆ one or more **stock exchanges** where stock and bond buy and sell orders are traded,
  - ⋆ one or more (stock and bond) incorporated **enterprises** and
  - ⋆ the **financial service industry "watch dog"**.
- The double-arrowed (↔) lines shall indicate communication interfaces between the "players" in the financial "market".

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

Ontological Description Principles

- We shall, in these lectures, advocate a simple approach to description,
- one that focuses on the
  - ⋆ **entities** ("things"),
  - ⋆ **functions** ("operations"),
  - ⋆ **events** ("insantaneous happenings"), and
  - ⋆ **behaviours** ("processes")

  of the domain.
- There may be more complicated approaches, cf. Sowa, but
  - ⋆ ours is sufficient
  - ⋆ and is justified by the formal means of description available.

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

• Phenomena and Concepts

- Entities, functions, events and behaviours of the domain
  - ⋆ are either phenomenological, i.e.,
    - ◇ are manifest,
    - ◇ can be pointed to,
    - ◇ designated,
  - ⋆ or are conceptual,
    - ◇ can be defined
    - ◇ on the basis of designations.

-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

Domain entities and their description: Vol.3, Sect.5.2, pp 125–138

- **Entity:** By an *entity* we shall loosely understand
  - ⋆ something fixed, immobile or static;
  - ⋆ although that thing may move,
  - ⋆ after it has moved it is essentially the same thing,
  - ⋆ an entity
- **Examples:**
  - ⋆ bank
  - ⋆ bank account
  - ⋆ client
  - ⋆ money (cash)
  - ⋆ bank statement
  - ⋆ broker
  - ⋆ stock exchange
  - ⋆ portfolio “manager”

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

Atomic Entities

• General

- By an atomic entity we intuitively understand an entity which “cannot be taken apart” (into other, the sub-entities).
- Whether an entity is considered atomic (or composite) is a decision made entirely by the describer.
- **Examples:**
  - ⋆ bank account
  - ⋆ person (client without a purse with cash)
  - ⋆ unit of cash (coin or bank note)
  - ⋆ stock certificate

-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

• Atomic Entity Attributes: Types and Values

- With an atomic entity we can associate
  - ⋆ one or more **attributes**:
  - ⋆ that is, a **type** and a **value** for each of these attributes.
- **Examples:**
  - ⋆ **Person:**

Type:	*Value:*
◇ Name	◇ Dines Bjørner
◇ Weight	◇ 118 pounds
◇ Height	◇ 179 cm
◇ Gender	◇ male
◇ ...	◇ ...

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

- **Bank Account:**

Type:	*Value:*
⋆ number	⋆ 212 023 361 918
⋆ balance	⋆ 1,678,123 Yen
⋆ interest rate	⋆ 1.5 %
⋆ credit limit	⋆ 400,000 Yen
⋆ ...	⋆ ...

- **A Unit of Cash:**

Type:	*Value:*
⋆ currency	⋆ Danish
⋆ denomination	⋆ 500 Kroner
⋆ form	⋆ bank note
⋆ ...	⋆ ...

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

Composite Entities

• General

- By a composite entity we intuitively understand an entity which "can be taken apart" (into other, the sub-entities).
- Whether an entity is considered (atomic or) composite is a decision made entirely by the describer.
- **Examples:**
  - ⋆ financial industry (into clients, banks, brokers, stock exchange, portfolio managers, etc.)
  - ⋆ bank (into HQ and branch offices)
  - ⋆ bank branch offices (with accounts, etc.)
  - ⋆ client (into person and purse)

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

• Composite Entity Subentities, Mereology and Attributes

- We speak of the
  - ⋆ **subentities** ⋆ **mereology** ⋆ and **attributes**

  of a composite entity.
- **Example:** Transportation Net
  - ⋆ **Subentities**: segments and junctions
  - ⋆ **Mereology**:
    - ◇ "set" of one or more s ◇ "set" of two or more j
    - ◇ such that ss are delimited by two js ◇ and js connects one or more ss
  - ⋆ **Attributes**:
    - ◇ multimodal: road and rail
    - ◇ transportation net of: Denmark
    - ◇ year: 2003

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

Larger Example: Financial Industry (I)

Subconsciously omitting explicit mention of the atomic, composite, subentity, attribute and mereology meta-concepts we enlarge on the financial industry example:

- The financial service industry consists of
  - ⋆ one or more uniquely identified banks,
  - ⋆ one or more uniquely identified portfolio managers,
  - ⋆ one or more brokers (of securities instruments),
  - ⋆ one (or more) stock (or securities instrument) exhange,
  - ⋆ one or more insurance companies,
  - ⋆ one or more credit card companies,
  - ⋆ etc.

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

- A bank consists
  - ⋆ of one or more branch offices and
  - ⋆ a headquarters office.
- A bank branch office consists of
  - ⋆ zero, one or more uniquely identified demand/deposit accounts;
  - ⋆ zero, one or more uniquely identified mortgage accounts;
  - ⋆ a register which records the demand/deposit account and the mortgage account identifiers (account numbers) of each client; and
  - ⋆ a register which, for every account number records the names (etc.) of the one (or more) clients (sharing this account);
  - ⋆ etc.

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

- ⋆ Each demand/deposit account has the following attributes:
  - ◇ balance,
  - ◇ interest rate (i.e., yield),
  - ◇ credit limit,
  - ◇ list of transactions (performed since reporting most recent list of transactions),
  - ◇ etc.
- ⋆ Each mortgage account has the following atributes:
  - ◇ remaining loan,
  - ◇ date of precious repayment,
  - ◇ interest rate,
  - ◇ fee schedule,
  - ◇ frequency of repayments,
  - ◇ etc.

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

- A stock exchange consists of
  - ⋆ a set of outstanding buy orders,
  - ⋆ a set of outstanding sell orders,
  - ⋆ a set of deferred buy orders, and
  - ⋆ a set of deferred sell orders.
  - ⋆ Each buy (sell) order is
    - ◇ uniquely identified,
    - ◇ names a securities instrument (e.g., IBM),
    - ◇ states when the order was placed,
    - ◇ states the size of the batch being ordered,
    - ◇ states high and low price range for buying (selling),
    - ◇ states the "open window" for trading,
    - ◇ etc.
  - ⋆ Etcetera!

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

Discussion of Parts and Whole

• Mereology = Parts-whole Relations

- Another term for 'mereology' is 'parts-whole relations'.
- Mereology and the attributes of a composite entity shows that
  - ⋆ The "real whole" is more than the sum of its parts:
  - ⋆ $Whole \ominus Parts = Mereology \oplus Attributes$

• Examples of Mereologies

- **Example: Nets**
  - ⋆ The mereology of nets is expressed through the provision and constraints of segment and junction identifiers.
  - ⋆ Thus the mereology implies a graph of edges (esgments) and nodes (junctions) with no dangling segments or isolated junctions.

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

- **Example: Route**
  - ⋆ The *'linear sequencing'* of segments and junctions expresses the mereology.
- **Example: Bank Accounts**
  - ⋆ The bank accounts component is *'a set of uniquely identified'* accounts, i.e., a *'map from'* account numbers (i.e., identifiers) *' to'* accounts.
- **Example: Bank**
  - ⋆ A bank is a *'composition'* of bank accounts, mortgage accounts, client-account-numbers registry, *'and'* account-to-clients-regustry.
  - ⋆ The bank mereology is expressed by the *'composition'*, the commas, and the *'and'* — implying a Cartesian product.

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

Domain functions and their description

- By a domain function we mean
  - ⋆ the naming,
  - ⋆ summary description (i.e., signature), and
  - ⋆ functional description

  of operations as they are performed by stakeholders of and in the domain.
- **Examples**

  Giving only function names and signatures for demand/deposit banking:
  - ⋆ open: Name × PersonalInfo × BANK → BANK × AcctNo
  - ⋆ deposit: AcctNo × Cash × BANK → BANK
  - ⋆ withdraw: AcctNo × Amount × BANK → BANK × Cash
  - ⋆ close: AcctNo × BANK → BANK × Cash

+81-761-51-1275, Fax: +81-761-51-1149 © Dines Bjørner, 2006 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

Function Descriptions

- Domain function descriptions emphasise
  - ⋆ **what** the function does
  - ⋆ and certainly not **how** the function may be performed.
- **Example:** Calculating mortgage repayments:
  - ⋆ On every due-payment-date a fixed amount, the annuity a, is paid to the bank for mortage account m.
  - ⋆ The bank calculates the interest, i, on the loan since last repayment and adds that amount of a to the banks' interest account α_i (+ interest cash register ρ_i),
  - ⋆ looks up the fee, f, for repayment and adds that amount of a to the banks' fee account α_f (+ fee cash registerρ_f),
  - ⋆ subtracts $a-(i+f)$ from account m, and puts the same amount (of a) into the banks' loans cash register ρ_ℓ, and ... .
  - ⋆ Any round-off in calculating i is handled as follows: ... .

-761-51-1275, Fax: +81-761-51-1149 © Dines Bjørner, 2006 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

Function Signatures

- We bring a number of examples:
- **Example: "The Market"**
  - ⋆ Let Σ_B, Σ_S identify state attributes of buyers and sellers, then

    value

    inq, ord, acc, pay, rec, ... : Args × ΣB × ΣS → ΣS × ΣB
    ofr, con, del, inv, acc, ... : Args × ΣS × ΣB → ΣB × ΣS
  - ⋆ express the schematic signature of the
    - ◇ *inquire, order, accept (offer and delivery), pay (invoice), reclaim*, etc., operations of buyers "against" sellers, and
    - ◇ *offer, confirm (order), deliver, invoice, accept (payment)*, etc., operations of sellers "against" uyers.

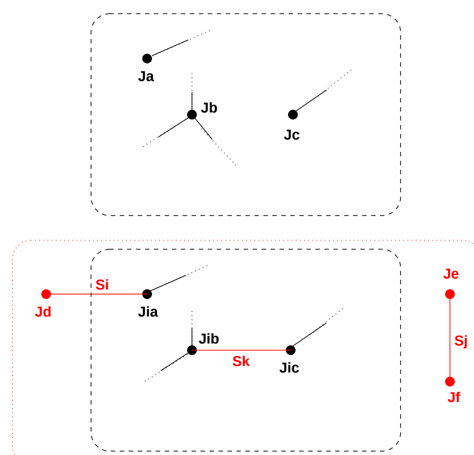
+81-761-51-1275, Fax: +81-761-51-1149 © Dines Bjørner, 2006 E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

- ⋆ Note the position of state arguments.
- ⋆ Note that the states are made explicit,
  - ◇ as in functional programming (a la SML),
  - ◇ and in contrast to imperative progamming (a la Java and C#)
  - ◇ where implicit references to database are assumed.
- ⋆ And note that any and all of the primitive operations
  - ◇ (*inquire, order, accept (offer and delivery), pay (invoice), reclaim*, and *offer, confirm (order), deliver, invoice, accept (payment)*)
  - ◇ "operate" like "sending 'argument' messages from one player to the other,
  - ◇ that no reply messages are intended,
  - ◇ but that states in both sender and receiver are normally changed.

- ⋆ These basic or primitive functions when combined, in various combinations (compositions) shall mimic the casual buying and selling actions of buyers and sellers — more on this later.
- ⋆ And these basic or primitive functions,
  - ◇ by leaving state changes in respective actors (buyer and seller)
  - ◇ enable these to more-or-less non-deterministically
  - ◇ take up, i.e., continue expected subsequent operations:
    - ◦ after a buyer initiated inquiry
    - ◦ the contacted seller may decide to (not) respond with an offer,
    - ◦ and after a seller initiated offer the contacted buyer may decide to (not) respond with an order,
    - ◦ etcetera.
- ⋆ Notice also the possibility of out-of-sequence operations.

- **Example: Transportation Net:**
  - ⋆ The problems to be described are the operation of expanding and contracting nets, that is
  - ⋆ basically of inserting and removing appropriate junctions and segments.
  - ⋆ For a net to be well-formed, recall:
    - ◇ There can be no isolated junctions in a net.
    - ◇ And all segments are connected to two distinct junctions.
  - ⋆ Our operations of developing (expanding) a net must take well-formed nets and "connections" and leave well-formed nets in which these connections are inserted.
  - ⋆ We introduce, therefore a concept of 'connection'.

- ⋆ The figure below is intended to show a net before and the net after the insertion of 'connections', a path, i.e., triples of two junctions and a segment:



In the below net, left to right:

- ⋆ new J, new S, old J (by ref.: Ji)
- ⋆ old J (by ref.: Ji′), new S, old J (by ref.: Ji′′)
- ⋆ new J, new S, new J

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

- ⋆ The three cases are, from left to right in the figure above:
  - ⋄ A new junction, a new segment and a known junction (by reference to its identifier).
  - ⋄ Two known junctions (by reference to their identifiers) and a new segment.
  - ⋄ Two new junctions and a new segment.
- ⋆ So there are, accordingly three kinds of connections and one operation:

type
  Conn == JSJi(j:J,s:S,ji:Ji)|JiSJi(ji1:Ji,s:S,ji2:Ji)|JSJ(j1:J,s:S,j2:J)
value
  insert: Conn $\times$ N $\xrightarrow{\sim}$ N
  remove: Conn $\times$ N $\xrightarrow{\sim}$ N

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

- ⋆ There might be other operations in connection, for example, with insertion, deletion or maintenance work:

value
  close,maint,open: (Ji|Si) $\to$ N $\to$ N

- ⋆ Of course, signature could instead be:

value
  close,maint,open: ((Ji$\times$Si-**set**)|(Ji$\times$Si$\times$**Nat**-**set**$\times$Ji)) $\to$ N $\to$ N

- ⋆ to indicate that only part of a junction, or only some lanes in one direction of a segment are operated upon.

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

- **Examples: Financial Transactions:**
  - ⋆ To open, deposit monies into, withdraw manoies from and close a bank demand/deposit account are simple operations:

type
  Client_Info, Bank, Act_No, Cash
value
  open: Client_Info $\times$ Bank $\to$ Bank $\times$ Actt_No
  deposit: Act_No $\times$ Cash $\times$ Bank $\to$ Bank $\times$ {|ok|no_ok|}
  withdraw: Act_No $\times$ Amount $\times$ Bank $\to$ Bank $\times$ Cash | {|no_ok|}
  close: Act_No $\times$ Bank $\to$ Bank $\times$ Cash | {|no_ok|}

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

- ⋆ To transfer monies between accounts likewise:

type
  BId
  Bnks = BId $\overrightarrow{m}$ Bank
value
  transfer: (Act_No$\times$BId)$\times$Amount$\times$(Act_No$\times$BId)$\times$Bnks$\to$Bnks$\times${|ok|nok|}

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

- ⋆ To place a *buy* or a *sell* offer, such an offer is "put" (by a broker) with the *stock exchange* (bourse) which may or may not accept the offer.
- ⋆ A *trade* is an instantaneous change of state of the *stock exchange* whereby one or more *buy* and one or more *sell* offers are more-or-less matched and *tra*nsacted.
- ⋆ A *suspension* (of the trading of a listed stack (*si:Si*) removes all buy and sell offers designated that stock to the suspended "list" (*sus*)

type
Ono,Price,Date
Buy = mkBuy(o:Ono,si:Si,am:**Nat**,lo:Price,hi:Price,b:Date,e:Date)
Sel = mkSell(o:Ono,si:Si,am:**Nat**,lo:Price,hi:Price,b:Date,e:Date)
StockExchg :: buy:Ono-**set**×sel:Ono-**set**×sus:Ono-**set**×tra:(Ono×Price)-**set**
value
place: (Buy|Sell) → StockExchg → StockExchg × {|ok|nok|}
trade: StockExchg → StockExchg
suspend: Si → StockExchg → StockExchg

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

Domain Events and Their Description

- By an event we understand
  - ⋆ an instantaneous change of state
  - ⋆ not directly brought about by some explicitly willed action in the domain,
  - ⋆ but either by "external" forces.
  - ⋆ or implicitly as a non-intended result of an explicitly willed action.
- Events may or may not lead to the initiation of explicitly issued operations.

+81-761-51-1275, Fax: +81-761-51-1149 | © Dines Bjørner, 2006 | 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

- **Examples:**
  - ⋆ **Events in Transportation Nets:**
    - ◇ A road segment (lane) breaks down, cannot be used for traffic.
      - ○ May force the road net authority to
      - ○ close a segment
      - ○ and/or set signals for the "detouring" of taffic.
    - ◇ A junction partially or fully breaks down, and can only partially (or maybe totally not) be used for traffic.
      - ○ May force the road net authority to
      - ○ close a segment
      - ○ and/or set signals for the "detouring" of taffic.

-761-51-1275, Fax: +81-761-51-1149 | © Dines Bjørner, 2006 | 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

- ⋆ **Events in The Market:**
  - ◇ An inquiry, or an order is left unanswered.
  - ◇ A seller runs out-of-stock of some merchandise.
  - ◇ A buyer fails to honour an invoice.
  - ◇ A delivery fails to materialise.
  - ◇ The delivery of an unordered item of merchandise.
  - ◇ The receipt of an invoice for an unordered item of merchandise.

+81-761-51-1275, Fax: +81-761-51-1149 | © Dines Bjørner, 2006 | 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

⋆ **Events in Financial Service Industry:**

- ◇ A(n attempt at a) withdraw action (would cause) causes the balance of the designated account to exceed (i.e., go below) the credit limit.
- ◇ Failure of a mortgage holder to pay annuity by the due date.
- ◇ A bank runs out-of-cash:
  - ○ Usually the bank then borrows money from the national (federal) bank.
- ◇ A bank crash.
- ◇ The "bad loans" of a bank exceed 3% of its assets.
- ◇ A financial report of a stock listed company
  - ○ forces a stock exchange to suspend tradings its stocks.

  The former is the event (the occurrence of the reort), the latter may be a response action.
- ◇ The discovery of "insider trading".

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

Domain Behaviours and Their Description

- By a simple domain behaviour we understand
  - ⋆ a sequence of zero, one or more
  - ⋆ actions (i.e., application, invocation of functions) and events.
- By a parallel (i.e., non-simple) domain behaviour we understand
  - ⋆ the simultaneous occurrence, over time
  - ⋆ of two or more behaviours.
- By a coordinated behaviour we understand
  - ⋆ a parallel behaviour
  - ⋆ in which two or more events in distinct behaviours "relate" to one another.

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

Examples

- **Transport Net Behaviours:**
  1. (Segment behaviour:) traffic
     - ⋆ along a segment,
     - ⋆ segment break-down,
     - ⋆ close of segment,
     - ⋆ rerouting (action sequence),
     - ⋆ repair of segment,
     - ⋆ reopening of segment,
     - ⋆ traffic along that segment, etc.
  2. (Junction behaviour:) sequence of semaphore (traffic light) settings at one junction
  3. The coordinated simultaneous behaviours of all segments and junctions.

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

- **Market Behaviours:**
  1. inquiry, offer, order, confirm, delivery, accept, invoice, payment
  2. offer
  3. order
  4. delivery, reject
  5. the simultaneous occurrence
     - ⋆ of a definite number
     - ⋆ of the above kind and other such behaviours
     - ⋆ amongst
       - ◇ several consumers,
       - ◇ several retailers,
       - ◇ several wholesalers and
       - ◇ several producers.

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

- **Financial Service Industry Behaviours:**
  1. open, deposit, deposit, withdraw, close
  2. open, deposit, deposit, withdraw, exceeding credit limit, withdraw, ...
  3. open, deposit, bank crash
  4. place buy offer, trade, ...
  5. place buy offer, suspend stock, withdraw offer, ...

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

Description Approaches

- Ordinary text, as above
- Petri Nets
- Message Sequence Charts (MSCs)
- Live Sequence Charts (LSCs)
- Statecharts
- CSP
- RAISE (which includes a variant of CSP)
- CafeOBJ
- ccs, π-Calculus, etc.

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

Summary

- We have reviewed the following description principles
  1. **Entities**
     - ⋆ **Atomic**
       - ◇ **Attributes**:
         - ○ Types
         - ○ Values
     - ⋆ **Composite**
       - ◇ **Attributes**
       - ◇ **Sub-entities**
       - ◇ **Mereology**
  2. **Functions**
     - ⋆ Notions of **State**
     - ⋆ Function **Signature**: Name and Type
     - ⋆ Function **Description**
  3. **Events**
  4. **Behaviours**
     - ⋆ Simple
     - ⋆ Parallel
     - ⋆ Coordinated

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

Michael Jackson's Description Principles (MJ)

- MJ's description principles centers arround:
  - ⋆ **designations**: phenomena that you can immediately point to
  - ⋆ **definitions**: what can be defined, that is, conceptualised
  - ⋆ **refutable assertions**: what may be claimed or postulated as properties — that may possibly be refuted

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

Designations

An Introductory Example

- My pair of Lloyd's shoes:
  - ⋆ The color is black.
  - ⋆ The material throughout is leather, soles too.
  - ⋆ The size is $42\frac{1}{2}$.
  - ⋆ The shoe lace fits into 2×5 holes.
  - ⋆ The shine is matte.
  - ⋆ Etcetera.
- The above concretely designated entity is an example of the abstracted concept of shoe.

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

Senses and Physical Units

- By a designation we mean
  - ⋆ a phenomenon
  - ⋆ that is manifest, that is, can be
    - ◇ seen, heard, touched, smelled and tasted
    - ◇ measured by physical device
      - ◦ mass, length, time
      - ◦ electric current, thermodynamic temperature, amount of substance, luminous intensity
      - ◦ etcetera (?)

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

Designation Description

- A designation is presented by
  - ⋆ naming it,
  - ⋆ and stating recognition rules.
- The recognition rules
  - ⋆ center around the humanly and/or physically manifest phenomena,
  - ⋆ and must be formulated such that a person who has otherwise understood the rules can recognise the described phenomenon.

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

Further Examples

- Our examples are mostly of entities.
- We leave it to the student to provide examples of function, event and behaviour designations.

1. **A Transport Net Designation:**
   - The entity is that of the road *Fredsvej*,
     - ⋆ located in the township of *Holte* in the incorporated city of *Søllerød*.
     - ⋆ The *Fredsvej* road is a cul-de-sac, is covered by tarma, edged by a single curb of granite stones, and with the sidewalks being covered by rough beach sand cum small pebbles.
   - Etcetera — we categorize the *Fredsvej* road as a segment.

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

2. **A Market Designation:**

- The "Rosengaard" grocery store
  - ⋆ cum mini-market on Parcelvej in the township of Virum, in the incorporated city of Lyngy-Tårbæk, Dennark.
  - ⋆ This retailer (entity) has approximately 6000 square feet of shopping space and approximately 4000 square feet of storage rooms.
  - ⋆ There are around 18 sets of 5 shelf stacks one of which is cooled and two large semi-freezer "tanks" featuring a usual array of daily groceries: bread products, cleaning products, drinks, dairy products, frozen meats, fish and seafoods, vegetables and foots.
  - ⋆ There is one service desk (for tobacco and alcohol) and two cash register "queues".

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

3. **A Financial Industry Designation:**

- The BG Bank branch office on Øverødvej 3,
  - ⋆ in the township of Holte, in the incorporated city of Søllerød.
  - ⋆ The branch office features two ATM machines: one inside and one outside the bank office proper, and one cash-less service desk for cashless bank book transactions.
  - ⋆ Six bank staff otherwise service the customers: financial advice, establishing loans, and securiries instrument brokerage services.
  - ⋆ There is also a customer-oriented safe room with safe boxes.

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

Definitions

- These lecture (note)s abound with definitions.

An Introductory Example

- By a finite, directed graph we understand
  - ⋆ a finite set, ns, of nodes,
  - ⋆ a finite set, es, of edges,
  - ⋆ and a function, f, which map edges of es to a pairs of nodes of ns.

type
  N, E, G = N-**set** × E-**set** × E $\overrightarrow{m}$(N×N)
value
  wf_G: G → **Bool**
  wf_G(ns,es,f) ≡
    ns≠{} ∧ es≠{} ∧ **dom** f = es ∧
    let ps = **rng** f **in** forall (n,n′):(N×N) · {n,n′}⊆ns **end**

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

General

- By a definition we mean
  - ⋆ an expression
  - ⋆ which introduces a new term
  - ⋆ and ascribes meaning to it.
- Definitions are usually expressed as a pair of
  - ⋆ a name, the term being defined (definiendum), and
  - ⋆ a definition body — an expression ascribing meaning to the term.
- The definition body (definiens) may include
  - ⋆ terms being defined elsewhere
  - ⋆ and/or the term being (thereby recursively) defined.

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

Further Examples

1. **A Transport Net Definition:**
   - Let subscripted js and ss denote junctions and segments.
   - Let distinctly indexed js (ss) denote distinct junctions (segments).
   - An out-and-return route
     - ⋆ consists of a pair of equal length routes,
     - ⋆ an out-route, r_o, which consists of a set of n paths (j_i, s_i, j_{i+1}), for $i = 1, 2, \ldots, n$, and
     - ⋆ a return-route, r_r, which consists of a set of n paths (j_{k+1}, s_k, j_k), for $k = 1, 2, \ldots, n$
     - ⋆ such that for each triplet (j_a, s_b, j_c) in r_o
     - ⋆ there is a (j_c, s_b, j_a) in r_r.

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

2. **A Market Definition:**
   - Let subscripted ms, p_rs, p_ws, ds and qs denotes merchandise, retailer sale prices, wholesaler sale prices, delivery terms and quantities-on-hand.
   - A retailer catalogue
     - ⋆ lists for each distinct merchandise m_i
     - ⋆ its retailer and wholesaler prices p_r and p_w,
     - ⋆ the delivery (to customer) terms, and
     - ⋆ the quantity that the retailer has in store.
   - Some constraints:
     - ⋆ The quantity-on-hand q may be zero,
     - ⋆ the retailer price p_r is usually (40%) higher than the non-zero wholesaler price p_w.

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

3. **A Financial Industry Definition:**
   - Let $o, s, q, p_{lo}, p_{hi}, d_f, d_t$ and o stand for order number, stock (name), quantity, low and high buy and sell price, respec. date (incl. hhmm) of day (hour and min.) from and day (etc.) to a buy or sell order is valid.
   - A stock trasnaction for a given stock s is possible
     - ⋆ if there is a set of buy orders, bs and a set of sell orders ss for that stock
     - ⋆ (elements of both bs and ss contain all the information listed above)
     - ⋆ such that the sum of the buy order quantities of bs equals or "slightly" exceeds the sum of the sell order quantities of ss and
     - ⋆ such that the actual trading price p is below any bp_{hi} in bs and above any sp_{lo} in ss.
   - An actual transaction need just satisfy the above.
   - Thus the choice of trading is nondeterministic.

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

The "Narrow Bridge"

- Michael Jackson suggests
  - ⋆ Designate as few phenomena as seems reasonable (the "narrow bridge").
  - ⋆ Define "the rest" based on this "narrow bridge" (to reality).
- The designations are then "lifted"
  - ⋆ to immediate, or "direct" definitions,
  - ⋆ that is, from values to types.
- From direct definitions one can then bring in further abstracted, that is, abstract, conceptual definitions (like route).

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

Refutable Assertions (RAs)

Introductory Examples

- Small examples:
  - ⋆ *A railway line connects exactly two stations.*
  - ⋆ Implications of the above RA are other RAs:
  - ⋆ *There are at least two train stations in a railway net.*
  - ⋆ *There is at least one railway line in a railway net.*
  - ⋆ *A train station is connected to at least one railway line.*
- Possible refutations:
  - ⋆ Is it likely to have only one station?
  - ⋆ Is it likely to have isolated stations?

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

General

- By a refutable assertion we mean
  - ⋆ a claim (a proposition, a predicate)
  - ⋆ which may be shown to be false.
- Refutable assertions are usually expressed
  - ⋆ as propositions
  - ⋆ or as predicates.

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

Further Refutable Assertion Examples

1. **A Refutable Transportation Assertion:**
   - Consider traffic: the continuous movement of vehicles along segments and across junctions of a net.
   - Assume
     - ⋆ at least two such vehicles,
     - ⋆ that each segment is directed, and
     - ⋆ that each such segment allows only traffic in one direction and
     - ⋆ that each such segment is like a single traffic lane.
   - A refutable assertion is now:
     - ⋆ *Two vehicles moving down the same segment,*
     - ⋆ *hence in the same direction,*
     - ⋆ *cannot change "in front/behind" position with respect to one another along that segment.*

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

2. **Another Refutable Transportation Assertion:**
   - Consider train traffic fully adhering to a time table modulo 24 hours.
   - Assume
     - ⋆ that all trains are on time.
   - A refutable assertion is now: *over any 24 hour interval*
     - ⋆ *the number of trains flowing into a station*
     - ⋆ *minus the number of trains ending their journey at that station*
     - ⋆ *plus the number of trains beginning their journey at that station*
     - ⋆ *equals the number of trains leaving that station.*
   - We should like to see the above assertion
     - ⋆ to be provable, as a domain theorem,
     - ⋆ under the given assdumptions.

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

3. **A Refutable Market Assertion:**

- Under the following assumptions
  - ⋆ the market encompasses all consumers, retailers, wholesalers and producers (including import and expot of merchandise) and
  - ⋆ returned merchandise is never resold,
- we postulate the following refutable assertions
  - ⋆ *at most the merchandise produced can be sold,*
  - ⋆ *if all merchandise is*
    - ◇ *(eventually) sold,*
    - ◇ *and none is returned*

    and
    - ◇ *is traded at higher prices between one ("downstream") pair of traders* (s/b)
    - ◇ *than between the immediate "upstream" pair of traders* $(s'/b'$, *where* $b' = s)$,
    - ◇ *then, excluding trading expenses, profit is generated.*

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

4. **A Refutable A Financial Industry Assertion:**

- Under the assumption that
  - ⋆ monies are not lost (in sense of "on the floor")
  - ⋆ and bank account balances are not tampered with
- we can express the following assertion:
  - ⋆ *Every transaction preserves an invariant between a banks's cash registers and its accounts.*
  - ⋆ You may wish to formulate this invariant:
    - ◇ Please consider repayment of loans,
    - ◇ interest on loans and yields on deposits,
    - ◇ etcetera, when formulating this refutable assertion.

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

Summary

- We have covered MJ's notion of
  - ⋆ **designations**
    - ◇ **names**
    - ◇ **recognition rules**
  - ⋆ **definitions**,
    - ◇ **names**
    - ◇ and **definition body**

  and the notion of a "narrow bridge:
    - ◇ **fewest possible designations**
    - ◇ in **favour of definitions**.
  - ⋆ and **refutable assertions**:
    - ◇ propositions or predicates
    - ◇ that appears to hold
    - ◇ but for which one must accept that they are one day shown not to hold.

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

Lecture Summary

- We have covered two axes of description:
  - ⋆ A concept of entities, functions, events and behaviours, and
  - ⋆ MJ's concepts of designations, definitions and refutable assertions.
- Any one description conforms to both sets of concept:
  - ⋆ weaves them into a narrative
  - ⋆ together with concepts to be covered in the next, the 3rd, lecture:
    - ◇ namely along the axis of domain facets
      - ○ intrinsics
      - ○ support technololgies
      - ○ management & organisation
      - ○ rules & regulations
      - ○ scripts
      - ○ human behaviour

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

⋆ as well as with concepts not covered in thise series of seminars:
  ◇ those of the axes of
    ◦ statics and dynamics
    ◦ tangibility
    ◦ temporality: hard and soft
    ◦ spatiality, i.e., dimensionality
    ◦ discreteness, continuity and chaos
    ◦ *&c.*
  ◇ See Vol. 3, Chap. 10 of my wonderful book!

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

Topic 3
Domain Facets

An Example

3. Domain Facets

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

Documents, A Domain Example
Originals, Copies and Versions

- There are documents.
- Documents are either
  ⋆ created,
  ⋆ edited or
  ⋆ copied.
- One can claim that a document is either
  ⋆ an original, or
  ⋆ an edited version, for short, a version, of a document, or
  ⋆ a copy of a document.

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

- One can claim that a document can either
  ⋆ only (say: "most recently") be an original, or
  ⋆ only (say: "most recently") be an edited document (i.e., a version), or
  ⋆ only (say: "most recently") be a copy of a document.

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

- The pragmatic intention of documents is to embody document content.
- We leave the notion of document content undefined.
- There is information.
- Information is either document content, or the absence of such.
- We use the special literal *void* to designate absence of content.
- To create a document needs no document content.
- From a document one can observe its most recent information.

-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

type
  D, oD, eD, cD, C, E
  I == void | C
value
  create: **Unit** $\rightarrow$ oD
  edit: E $\times$ D $\rightarrow$ eD
  copy: D $\rightarrow$ cD

  is_oD: D $\rightarrow$ **Bool**
  is_eD: D $\rightarrow$ **Bool**
  is_cD: D $\rightarrow$ **Bool**

+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

axiom
  ∀ d:D •
    is_oD(d)∨is_eD(d)∨is_cD(d) ∧
    is_oD(d)⇒∼is_eD(d)∧∼is_cD(d) ∧
    is_eD(d)⇒∼is_oD(d)∧∼is_cD(d) ∧
    is_cD(d)⇒∼is_oD(d)∧∼is_eD(d) ∧ ... or, which is the same:
  ∀ d:D,e:E •
    is_oD(create()) ∧ ∼is_eD(create()) ∧ ∼is_cD(create()) ∧
    is_cD(copy(d)) ∧ ∼is_oD(copy(d)) ∧ ∼is_cD(edit(e,d))
    is_eD(edit(e,d)) ∧ ∼is_oD(edit(e,d)) ∧ ∼is_cD(edit(e,d))
value
  obs_I: D → I
axiom
  obs_I(create()) = void ∧
  ∀ d:D • is_oD(d) ⇒ obs_I(copy(d)) = void

-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

Annotations:

- The sectioning literal **type** designates that the following text (up to a next sectioning literal) introduces abstract and concrete type definitions. An abstract type definition is like a sort.
  - ⋆ *D, oD, eD, cD, C* and *E* introduces the sorts of documents, original documents, edited documents, document copies, document contents and document editing. (We shall not elaborate further on *E* till Sect. on page 189.
  - ⋆ The equation *I* == *void* | *C* defines document information as either being *void* or *C*. (We are not here telling you what *void* means.) The alternatives of *U* == *V* | *W* | *X* | *Y* ... are, by the == constructor., being defined as disjoint types.

+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 sectioning literal **value** designates that the following text (up to a next sectioning literal) introduces values of defined types. Six such values are introduced. We see from their types (... $\rightarrow$ ...) that they are all function values.
  - ⋆ *create* designates the create function. It is of type $\mathbf{Unit} \rightarrow oD$. Thus it takes no arguments (designated by the value literal $\mathbf{Unit}$) and yields an original document.
  - ⋆ *edit* designates the editing function. It is of type $E \times D \rightarrow eD$. Thus it takes two arguments: some editing value and a document and yields an edited document.
  - ⋆ *copy* designates the copy function. It is of type $D \rightarrow cD$. Thus it takes one argument, a document and yields a document: the copied document. The function signature says nothing about "what happened" to the input argument. As we shall see, it is still there, "somewhere".[6]

[6] Adding 3 and 7, yielding 10, does not, in any way, destroy or influence 3 and 7.

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

- ⋆ *is_oD* designates a predicate observer function. It is a type $D \rightarrow \mathbf{Bool}$. If the document is an original then truth is yielded, otherwise falsity.
- ⋆ *is_eD* designates a predicate observer function. It is a type $D \rightarrow \mathbf{Bool}$. If the document is an edited version of a document then truth is yielded, otherwise falsity.
- ⋆ *is_cD* designates a predicate observer function. It is a type $D \rightarrow \mathbf{Bool}$. If the document is a copy then truth is yielded, otherwise falsity.

The functions are all postulated. They are claimed to exist. They are not defined. Instead their properties will be revealed through axioms.

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

- The sectioning literal **axiom** designates that the following text (up to a next sectioning literal) introduces a number of properties — typically over the types and values introduced before these axioms.
  - ⋆ The clause $\forall$ *a:A* • "reads": *for all values a of type A it is the case that*. In RSL all quantifications are typed.
  - ⋆ The proposition *is_oD(d)*$\vee$*is_eD(d)*$\vee$*is_cD(d)* $\wedge$ "reads" *a document d is either an original or an edited version or a copy, and ... .*
  - ⋆ The proposition *is_oD(d)*$\Rightarrow\sim$*is_eD(d)*$\wedge\sim$*is_cD(d)* "reads" *if a document is an original then it is neither an edited version or a copy, and ... .*
  - ⋆ The proposition *is_oD(create())* $\wedge \sim$*is_eD(create())* $\wedge \sim$*is_cD(create())* "reads" *for all documents and editing values, the value resulting from a proper create operation is an original and is not a edited version and is not a copy.*
  - ⋆ The predicate $\forall$ *d:D,e:E* • *is_eD(edit(e,d))* $\wedge \sim$*is_oD(edit(e,d))* etcetera "reads" *a document that has been properly edited is an edited version and is not an original and is not a copy.*

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

- The signature *obs_I: D* $\rightarrow$ *I* expresses a an observer function which from a document observes its information.
- The axioms *obs_I(create())* $=$ *void* and $\forall$ *d:D* • *is_oD(d)* $\Rightarrow$ *obs_I(copy(d))* $=$ *void* expresses that copies of copies of ... of copies of originals still have no proper information content.

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

Editing and Versions

- Editing a document modifies its information.
- An edited document is a version of the document from which it was edited.
- Editing a document does not amount to establishing a new document.
- From an edited document one can observe
  - ⋆ the information immediately before it was most recently edited, and
  - ⋆ how that information was edited, i.e., the resulting content.

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

- One way of modelling the edit function is by means of two functions:
  - ⋆ a forward editing function and
  - ⋆ a backward, "undo" editing function.
- The forward editing function
  - ⋆ takes an information argument and delivers an information result.
- The backward editing function
  - ⋆ takes an information argument and delivers an information results.
- The backward editing function is the inverse of the forward editing function.

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

```
type
  E′ = FE × BE
  FE,BE = I → I
  E = {|(fe,be):E • ∀ i:I • be(fe(i))=i |}
value
  obs_E: D ~→ E
axiom
  obs_E(create()) = chaos ∧
  ∀ d:D,e,(fe,be):E
    obs_E(edit(e,d)) = e ∧
    obs_I(edit((fe,be),d)) = fe(obs_I(d)) ∧
    obs_I(d) = be(obs_I(edit((fe,be),d))) ∧
    obs_E(copy(edit(e,d))) = e ∧ ... /∗ induction ∗/
```


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

Annotations:

- *E′* is a concrete type. It is defined as the Cartesian of two types: *FE* and *BE*.
- Both *FE* and *BE* are total functions from information to information.
- *E* is the subtype of *E′* which constrains the backward editing function *be:BE* to be an inverse of the forward editing function *fe:FE*.
- *obs_E* is a partial observer function. It applies to documents.
- From an original document one cannot observe any editing functions: *obs_E(create())* = **chaos**.
- From edited documents (whether since copied) one can (still) observe the editing functions.
- The parenthesised clauses: (whether since copied) and (still) are not expressed by *obs_E(copy(edit(e,d)))* = *e*, but intimated by the ellipses clause ... — to be formalised below.

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

Document Traces

- From a document one can observe its immediate predecessor document.
- An original document has no predecessor.
- A copy, d_c of a document, d, had d as its immediate predecessor document.
- An edited document, also called a version,, d_e of a document, d, had d as its immediate predecessor document.
- And so on, "ad finitum", till the original document is encountered.
- Let us call the document from which an edited version arises for the master document.
- And let us call document from which a copy is made also for the master document.
- Thus the predecessor documents are masters wrt. the successors.

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

value
obs_Pre: D $\xrightarrow{\sim}$ D
axiom
obs_Pre(create()) = **chaos** $\wedge$
$\forall$ d:D,e:E • obs_Pre(copy(d)) = d = obs_Pre(edit(e,d))

© Dines Bjørner, 2006
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

Annotations:

- From any document other than an original one can observe, *obs_Pre*, its predecessor.
- Thus *obs_Pre(create())* is not defined, that is, is **chaos**.
- For all documents and editing functions the predecessor of a *copy* of *d*, i.e., *copy(d)*, is *d*, and the predecessor of the *e* edited version, *edit(e,d)* of *d* is also *d*.

-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

Observations:

- We could decide, instead of making *obs_Pre* a partial function, to let *obs_Pre(create())* yield *create()*.
- Then *obs_Pre* would be a total function.
- And then *obs_Pre(copy(create()))* would be "the same" as *create()*.
- We shall review and modify our predecessor function, *obs_Pre*, later in this lectures.

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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 document trace is a history trail, i.e., a sequence of documents,
- from an original to the present document, whether a copy or a version
- such that
  - ⋆ the first document of the sequence is the document,
  - ⋆ the ith document in the sequence is the predecessor of the $i-1$st document in the sequence, and hence such that
  - ⋆ the last document in the sequence is the original.
- Thus one can establish the full history that any document has undergone since the creation of its "ultimate predecessor".

value
obs_doc_trace: D → D*
obs_doc_trace(d) ≡
  if is_oD(d) **then** ⟨d⟩ **else** ⟨d⟩⁀obs_doc_trace(obs_Pre(d)) **end**

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

Annotations:

- We name the document trace function *obs_doc_trace* since it is really an observer function (it is being "defined" solely in terms of, in this case one observer function).
- The document trace of an original document is the singleton sequence of that document.
- The document trace of a copy or an edited version (*d*) is the prefix concatenation of the singleton sequence of that document (*d*) with the document trace of the predecessor document of *d*.
- Termination is guaranteed since only a finite number of copies and edits can have taken place on any document.

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

We can now complete the induction part of the axiom above *obs_E(copy(edit(e,d))) = e ∧ ....*

axiom
∀ d:D ·
  ∀ i:**Nat** · i ∈ **inds** obs_doc_trace(d) ⇒
    is_eD(obs_doc_trace(d)(i)) ⇒
      ∀ j:**Nat** · j ∈ **inds** obs_doc_trace(d) ∧ j<i ∧
        ∀ k:**Nat** · k ∈ {j,i−1} ∧ is_cD(obs_doc_trace(d)(k)) ⇒
          obs_E(obs_doc_trace(d)(i)) = obs_E(obs_doc_trace(d)(k))

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

Annotations:

- For all documents
- and for all indices, *i*, into the trace of such doucments
- if the *i*'th document of that trace is an edited version
- then for all lower indices *j*, before *i*,
- if all documents (*obs_doc_trace(d)(k)*) of the trace properly *j* and *i−1* are copies,
- then we can observe in these copies the same editing value.

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

Annotated Original Documents

- We modify the *copy* function and the notion of an original document, *od:oD*.
- We now annotate original document by a trace of "has been copied" markers.
- The document resulting from *create()* has an empty such trace.
- The document resulting from *copy(create())* has a singleton trace of one "has been copied" marker.
- Each additional copying of a marked original adds one "has been copied" marker to the trace.
- Two original documents which differ only in number of "has been copied" markers are otherwise considered the same original.

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

type
  $\mathsf{hbc\_Mark} == \mathsf{hbc}$
value
  $\mathsf{obs\_hbc\_Marks}\colon \mathsf{oD} \to \mathsf{hbc\_Mark}^*$
axiom
  $\mathsf{obs\_hbc\_Marks(create())} \equiv \langle\rangle \wedge$
  $\forall\ \mathsf{od{:}oD} \cdot \mathsf{obs\_hbc\_Marks(copy(od))} = \langle\mathsf{hbc}\rangle \frown \mathsf{obs\_hbc\_Marks(od)}$

value
  $\mathsf{disregard\_Marks}\colon \mathsf{D} \to \mathsf{D}$
  $\mathsf{disregard\_Marks(d)}$ **as** d'
    $\mathsf{obs\_hbc\_Marks(d')} = \langle\rangle \wedge \mathsf{obs\_Pre(d)} = \mathsf{obs\_Pre(d')}$
  $\mathsf{differ\_by\_1\_Mark}\colon \mathsf{D} \times \mathsf{D} \to \mathbf{Bool}$
  $\mathsf{differ\_by\_1\_Mark(d,d')} \equiv$
    $\mathsf{obs\_hbc\_Marks(d)} = \mathbf{tl}\ \mathsf{obs\_hbc\_Marks(d')} \wedge$
    $\mathsf{disregard\_Marks(d)} = \mathsf{disregard\_Marks(d')}$

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

Annotations:

- *hbc_Mark* names a concrete type. Its only value is *hbc*. *hbc* is not further defined.
- *obs_hbc_Marks* is an observer function. It applies to original documents and yields a possibly empty list of *hbc:hbc_Marker** of *hbc* markers.
- The list of *hbc* markers of a fresh, "virgin" original is empty.
- The list of *hbc* markers of any original that has been copied (once or more) has one more *hbc* marker than the original from which it was copied.
- We can view a document without its "bass been copied" marks. That is the function of the *disregard_Marks* function.
- Two documents are, in a sense, the same if they differ only by one or more marks.

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

- We now redefine the predecessor observer function.

value
  $\mathsf{obs\_Pre}\colon \mathsf{D} \xrightarrow{\sim} \mathsf{D}$
axiom
  $\mathsf{obs\_Pre(copy(d))} = \mathsf{d} \wedge$
  $\forall\ \mathsf{d{:}D,e{:}E} \cdot$
    $\mathsf{obs\_Pre(edit(e,d))} = \mathsf{d} \wedge$
  $\forall\ \mathsf{od{:}oD} \cdot$
    $\mathsf{obs\_hbc\_Marks(od)} = \langle\rangle \Rightarrow \mathsf{obs\_Pre(od)} = \mathbf{chaos} \wedge$
    /* the above is the same as */ $\mathsf{obs\_Pre(create())} = \mathbf{chaos} \wedge$
    $\mathsf{obs\_Pre(copy(od))} = \mathsf{od}$

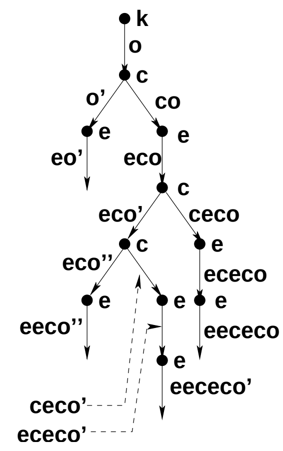
- Later we shall augment the "has been copied" marker with location and time of copying.

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

Document Family Trees

- Each document creation may give rise to a whole set of documents:
  - ⋆ copies of documents (for each copy a new document arises while the document from which it was copied basically remains), and
  - ⋆ edited versions of documents (for each version the number of documents remain the same).
- Given an original document one can establish the family tree of documents descending from the originally created document.

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



o is original
o' is o after copying o
co is copy of o
eo' is edited version of o'
eco is edited version of co
eco' is eco after copying eco
ceco is copy of eco
eco' is eco after copying eco
ceco' is copy of eco'
ececo is edited version of ceco
ececo' is edited version of ceco'
eececo is edited version of ececo
eececo' is edited version of ececo'

Figure 6.9: A document family tree

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

- A document family tree consists of nodes and stems (i.e., branches).
- Nodes, other than the root node, designate operations performed on documents.
- The root node designates the "moment" before "creation"!
- Stems designate documents.
- A node, other than the root node, has one input stem and, for any node, one or two output stems.
- The input stem of a node is (also) said to be incident upon that node,
- and to designate the predecessor document of the new document resulting from the node operation.

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

- The output stem is, or the output stems are said to emanate from the node.
- The root node designates the create operation.
- Any other node designates either an edit or a copy operation.
- If a node designates an edit operation then it has one output stem and that stem designates the edited version of the document designated by the stem incident upon the edit node.

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

- If a node designates a copy operation then it has two output stems:
  - ⋆ one of these stems designate the (input) document designated by the stem incident upon the copy node
  - ⋆ while the other stem designates the copy of that (input) document.
- Finally a document family tree ends in leaves which are stems, i.e., documents.
- From any stem in a document tree one can establish the unique path of stems from that stem back to the original document designated by the stem emanating from the root node.

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

- Such a path is a document trace.
- As for the general, i.e., abstract concept of trees one can speak of subtrees.
  - ⋆ If a stem is incident upon a node, then that node is the sub-root of a subtree which we shall here call a document tree (as distinguished from a document family tree).
  - ⋆ A (sub-)root of a document [family]tree[7] may have one or two subtrees, i.e., document trees: one of the (sub-)root designates the [create] (edit) [8] operation, two if it designates the copy operation.

[7] The phrase: *(sub-)root of a document [family]tree* reads as follows: *root of a document family tree or sub-root of a document tree.*
[8] The phrase: *(sub-)root designates the [create] (edit)* reads as follows: *root designates the create or sub-root designates the edit.*

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

```
type
  DFT′ = mkCreate() × oD × DT
  DFT = {|dft:DFT′ • wfDFT(dft)|}
  DT == nil | ET | CT
  ET = mkET(mkEdit(efns:(fe:FE,be:BE)),(ed:eD,dt:DT))
  CT = mkCT(mkCopy(),(d:D,dt:DT),(cd:cD,dt′:DT))

value
  wfDFT: DFT′ → Bool
  wfDFT(_,od,dt) ≡
    case dt of
      nil → true,
      _   → wfDT(dt)(od)
    end
```


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

```
wfDT: DT → D → Bool
wfDT(dt)(d) ≡
  case dt of
    nil → true,
    mkET((fe,be),(ed,dt′))
      → preEpost((fe,be),d,ed) ∧ wfDT(dt′)(ed),
    mkCT(mkCopy(),(d′,dt′),(cd,dt″))
      → preCpost(d,d′) ∧ wfDT(dt′)(d′) ∧ wfDT(dt″)(cd)
  end

preEpost: E × D × eD → Bool
preEpost((fe,be),d,ed) ≡ ...
  /∗ see postcondition of the edit function on page 191 ∗/

preCpost: D × D → Bool
preCpost(d,d′) ≡ disregard_Marks(d′)=d
```

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

Annotations:

- *DFT′* defines the Cartesian of not necessarily well-formed document tree.
- *mkCreate(), oD* and *DT* are the types of the components of the document tree.
- *mkCreate()* is strictly speaking not necessary, but is introduced so that all nodes possess an operation designator.
- *oD* designates the stem amanating from the *mkCreate()* node.
- *DT* designates the possibly emty sub-tree "attached" to the stem, i.e., upon which the stem may be incident.
- *DT* is thus either *nil* (i.e., the stem is a leaf) or is an edit tree *et:ET* or a copy tree *ct:CT*.

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

- An edit tree *mkET(mkEdit(efns:(fe:FE,be:BE)),(ed:eD,dt:DT))* has sub-root node *mkEdit(efns:(fe:FE,be:BE))* and one sub-tree *(ed:eD,dt:DT)*.
  - ⋆ The sub-root node designates the editing functions *mkEdit(efns:(fe:FE,be:BE))*.
  - ⋆ The forward editing function *fe* "works" on the document of the stem incident upon this sub-root node.
  - ⋆ The backward editing function *be* "works" on the document of [the edited version stem *ed:eD*] emanating from this sub-root node.
  - ⋆ *dt:DT* designates a possible sub-tree of the stem emanating from this sub-root node.

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

- A copy tree *mkCT(mkCopy(),(d:D,dt:DT),(cd:cD,dt′:DT))* has sub-root node *mkCopy()* and two sub-trees *(d:D,dt:DT)* and *(cd:cD,dt′:DT)*.
  - ⋆ The sub-root node designates the copy function *mkCopy()*.
  - ⋆ One (here shown as "the left") sub-tree *(d:D,dt:DT)* designates the document *d:D* being copied, hence "carried" forward, and its sub-tree *dt:DT*.
  - ⋆ One (here shown as "the right") sub-tree *(cd:cD,dt′:DT)* designates the document copy *cd:cD*, and its sub-tree *dt′:DT*.

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

- A number of constraints must be satisfied for a document history tree, *dft*, to be proper, i.e., to be well-formed *wfDFT(dft)*.
  - ⋆ We can ignore the Cartesian *mkCopy()* component of *dft*.
  - ⋆ If the sub-tree component *dt* is *nil* then the whole document history tree is well-formed.
  - ⋆ Otherwise the well-formedness of *dft* is the well-formedness of *dt* in the context of the incident document *od*.

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

- The well-formedness *wfDT(dt)(d)* of a sub-tree *dt* in the context of an incident document *d* is likewsie defined by cases:
  - ⋆ If *dt* is *nil* then well-formedness is guaranteed.
  - ⋆ If *dt* is an edit sub-tree *mkET((fe,be),(ed,dt′))* then well-formedness is a conjunction of
    - ◇ the edit pre/post condition *preEpost((fe,be),d,ed)* explained earlier, and
    - ◇ the well-formedness of the version document sub-tree *dt′*.

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

- ⋆ If *dt* is a copy sub-tree *mkCT(mkCopy(),(d′,dt′),(cd,dt″))* then well-formedness is a conjunction of
  - ◇ the copy pre/post condition *preCpost(d,d′)* where *d* is the document being copied — and after copying,
  - ◇ the well-formedness of the master[9] document sub-tree *wfDT(dt′)(d′)*, and
  - ◇ the well-formedness of the copied document sub-tree *wfDT(dt″)(cd)*.

[9] We shall move this notion way back, towards the front of this lectures: the master document is the document being copied.

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

Document Family States

- A state of a document family tree is a breadth-first set of stems of the tree.
- A breadth-first set of stems of a document family tree is one whose stems belong to distinct paths.
- Fig. 6.10 shows 11 states of a document family tree.

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

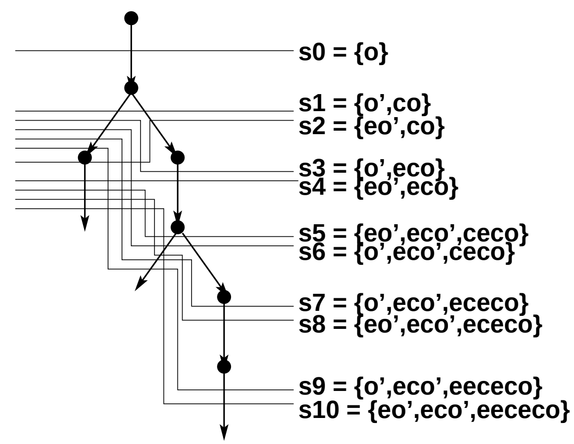


Figure 6.10: Document family states

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

- The idea is that there is an initial state, here s0, of the tree,
- and that there is a final state, here s10, of the tree.
- The initial state, here s0, designates the initial, i.e., the original document.
- The final state, here s10, designates a notion of final documents.
- A final state means that no further operations are to be performed on members of a set of documents. ("Case closed.")
- Please note that the final state of any document family tree is unique — as is the initial state.
- Please also note that a void document, i.e., a copy of a copy of ... a copy of an original document may be a final document.[10]

-761-51-1275, Fax: +81-761-51-1149 E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[10] The reader may feel uncomfortable having such void copies "floating" around, seemingly to no effect. But that is the cost of not imposing constraints that would otherwise impose what we consider unnatural limitations on what can be done to documents.

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

- Intermediate states designate possible collections of non-final documents.
- Thus a non-final state has one or more successor states.
- Usually there may be several ways of making state transitions from the initial state to the final state.
- Possible sequences of states are indicated by:

$$s0 \mapsto s1 \mapsto s3 \mapsto s6 \mapsto s7 \mapsto s9,$$
$$s0 \mapsto s1 \mapsto s2 \mapsto s4 \mapsto s8 \mapsto s10.$$

- From a document family tree we can compute all states and all possible initial to final state sequences.

+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

type
$\Sigma = \{|\sigma{:}\text{D-}\mathbf{set}\cdot\sigma\neq\{\}|\}$
value
States: DFT $\rightarrow \Sigma$-**set**
Traversal: DFT $\rightarrow \Sigma^*$

States(dft) $\equiv$ ...
Traversal(dft) $\equiv$ ...

-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

Document Community

- By a document community we mean a set of uniquely identified document family trees.

type
Did
DoCo = Did $\underset{m}{\rightarrow}$ DFT

- No two states of (two) distinctly named document family trees share states, i.e., have one or more documents in common.

value
wfDoCo: DoCo $\rightarrow$ **Bool**
wfDoCo(doco) $\equiv$ ...

+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

Discussion of First Model of Document Intrinsics

- There seems to be a number of problems with the model so far:
  - ⋆ Documents, whether manifest by humans senses (such as paper documents) or by technical/scientific apparata (such a MS Word, LaTeX (.tex) files, portable document format (.pdf) files or postcript (.ps)files) always have a unique location in space.
  - ⋆ Operations on documents occur at certain times and these operations may, or may not "take time to perform".
  - ⋆ Finally we did not mention any notion of document identity: two documents which differ in some way (location, time of application of, say, most recent operation, content, etc.) can be claimed to have unique, i.e., distinct indentities.
- We will, in the next two sections propose concrete models of locations and time of operation invocation.

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

A Concrete Model of Locations

- We introduce a spatial notion of location.
- Mathematically we consider a location to be a dense point set equipped with some "neighbourhood" (or "infinitisimally close" predicate).
- No two otherwise distinct documents can occupy overlapping locations.
- Thus all distinct documents of a document family state occupy distinct, non-overlapping locations.
- And similarly for document communities.
- We now extend our simplistic model of document intrinsics.

+81-761-51-1275, Fax: +81-761-51-1149 | © Dines Bjørner, 2006 | 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

- From documents we can now observe their location.
- When creating or copying a document a single location is provided.
- The original document being created "receives" the given location.
- The document copy being established likewise "receives" the given location. The document from which the copy was made retains its location.
- The document resulting from an edit retains the location of the document being edited.
- We finally add a new operation on documents: Moving a document from one location to another, therefrom distinct location.
- The move shall result in the location of the moved document changing from what it was before the move to the given location.
- We shall, when now considering the create, copy, edit and move operations not consider whether the implied locations may interfere with locations of other documents of a family or community.

+81-761-51-1275, Fax: +81-761-51-1149 | © Dines Bjørner, 2006 | 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
value
  $=$: L $\times$ L $\rightarrow$ **Bool**
  infinitesimally_close: L $\times$ L $\rightarrow$ **Bool**
axiom
  $\forall$ l,l′:L $\cdot$ infinitisimally_close(l,l′) $\Rightarrow$ l$\neq$l′
  $\forall$ l,l′,l″:L $\cdot$ l′$\neq$l″ $\wedge$
    infinitesimally_close(l,l′)$\wedge$infinitisimally_close(l,l″) $\Rightarrow$
      infinitesimally_close(l′,l″) ...

+81-761-51-1275, Fax: +81-761-51-1149 | © Dines Bjørner, 2006 | 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
  create: L → oD
  copy: D × L → D × cD
  edit: E × D → eD
  move: D × L $\xrightarrow{\sim}$ D, **pre**: move(d,l): obs_L(d)≠l
  obs_L: D → L
axiom
  ∀ l:L,e:E ·
    obs_L(create(l)) = l ∧
    let (d′,cd) = copy(d,l) **in**
    preCpost′(d,d′) ∧ obs_L(cd)=l **end** ∧
    let ed = edit(e,d) **in** obs_L(ed)=obs_L(d) **end** ∧
    obs_L(move(d,l)) = l

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

A Basic Concrete Model of Time

- We introduce a temporal notion of time.
- Mathematically we consider time to be a linear dense point ordering.
- Each document operation: create, copy, edit and move occurs at a specific time (and lasts no time).
- We now extend our simplistic model of document intrinsics.
- From documents we can now observe the time of their last operation.
- When creating, copying, editing and moving a document a single time is provided.
- The original document being created "receives" the given time.

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

- The document copy being established likewise "receives" the given time. The document from which the copy was made retains its time.
- The document resulting from an edit "receives" the given time.
- The move shall result in a moved document marked with the given time.
- We shall, when now considering the create, copy, edit and move operations not consider whether the implied times are coincident with times of other documents of other the same family or other families.
- Previous documents of any documents retain their times of operation applications.

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

type
  T
value
  obs_T: D → T
  create: L × T → oD
  copy: D × L × T → D × cD
  edit: E × D × T → eD
  move: D × L × T $\xrightarrow{\sim}$ D, **pre**: move(d,l): obs_L(d)≠l
axiom
  ∀ t:T,e:E ·
    obs_T(create(__,t)) = t ∧
    let (d′,cd) = copy(d,__,t) **in**
    preCpost′(d,d′) ∧ obs_T(cd)=t **end** ∧
    let ed = edit(e,d,t) **in** obs_T(ed)=t **end** ∧
    obs_T(move(d,l,t)) = t

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

Located and Timed Documents

- We wish to record that for every document that has been copied the fact that it has been copied: time and place.

value
has_been_copied: D → **Bool**
when_where_copied: D $\tilde{\to}$ L×T
otherwise_the_same: D×D → **Bool**
axiom
∀ d:D •
~has_been_copied(d) ≡ when_where_copied(d)=**chaos** ∧
∀ l:L,t:T •
let (c′,cd) = copy(d,l,t) **in**
has_been_copied(d′) ∧ when_where_copied(d′)=(l,t) ∧
otherwise_the_same(d,d′) **end**

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

Time and Space (Locations)

- No document can at the same time be in two different locations:

axiom
∀ d,d′:D •
let (l,t) = (obs_L(d),obs_T(d)),(l′,t′) = (obs_L(d′),obs_T(d′)) **in**
(t=t′ ∧ l=l′ ≡ d=d′) ∧ (t=t′ ∧ l≠l′ ≡ d≠d′) **end**

Unique Document Identifiers

- Given that creation and copying times and locations are unique we can introduce a notion of unique document identifications.
- For a document family that is simple enough:

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

type
Uid
value
obs_Uid: D → Uid
axiom
let od = create() **in**
let uid = obs_Uid(d) **in**
∀ d:D, e:E, t:T, l:L •
let dt = doc_trace(d) **in** dt(**len** dt)=od ⇒
∀ i:**Nat** • i ∈ **inds** dt ⇒
is_oD(dt(i)) ⇒ obs_Uid(dt(i))=uid ∧
is_eD(dt(i)) ⇒ obs_Uid(dt(i))≠uid ∧
is_cD(dt(i)) ⇒ obs_Uid(dt(i))≠uid
end end end

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

- For a community we need to distnguish two originals by their distinct document family identifiers.
- That is: The Uid is some concoction of a document family identifier, a ocopy or edit operation time and a copy or edit operation location.

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

Business Processes

- We briefly overview a few business processes:
  - ⋆ Air Traffic
  - ⋆ Freight Logistics
  - ⋆ Harbours
  - ⋆ Financial Service Industry

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

Air Traffic Business Processes

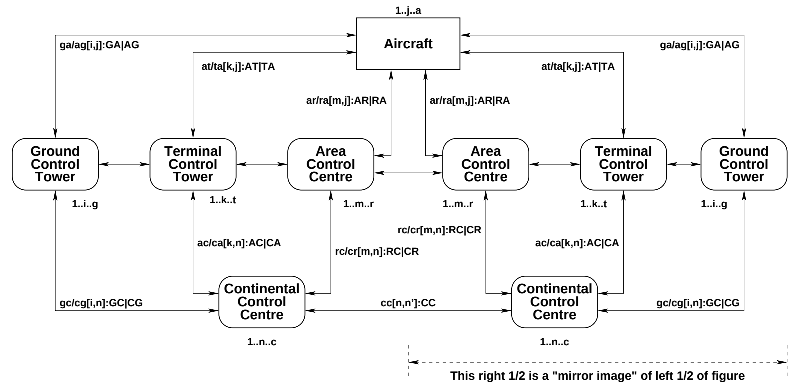


Figure 7.11: An air traffic behavioural system abstraction

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

- The main business process behaviours of an air traffic system are the following:
  - ⋆ the aircraft,
  - ⋆ the ground control towers,
  - ⋆ the terminal control towers,
  - ⋆ the area control centres and
  - ⋆ the continental control centres
- (Fig. 7.11 on the facing page).

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

- We describe each of these behaviours separately:
  - ⋆ *Aircraft*
    - ◇ get permission from ground control towers to depart;
    - ◇ proceed to fly according to a flight plan (an entity);
    - ◇ keep in contact with area control centres along the route,
    - ◇ (upon approach) contacting terminal control towers from which they, simplifying, get permission to land; and
    - ◇ upon touchdown, changing over from terminal control tower to ground control tower guidance.

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

⋆ *The ground control towers,*

- ◇ on one hand, take over monitoring and control of landing aircraft from terminal control towers;
- ◇ and, on the other hand, hand over monitoring and control of departing aircraft to area control centres.
- ◇ Ground control towers, on behalf of a requesting aircraft, negotiate with destination ground control tower and (simplifying) with continental control centres when a departing aircraft can actually start in order to satisfy certain "slot" rules and regulations (as one business process).
- ◇ Ground control towers, on behalf of the associated airport, assign gates to landing aircraft, and guide them from the spot of touchdown to that gate, etc. (as another business process).

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

⋆ *The terminal control towers*

- ◇ play their major role in handling aircraft approaching airports with intention to land.
- ◇ They may direct these to temporarily wait in a holding area.
- ◇ They — eventually — guide the aircraft down, usually "stringing" them into an ordered landing queue.
- ◇ In doing this the terminal control towers take over the monitoring and control of landing aircraft from regional control centres,
- ◇ and pass their monitoring and control on to the ground control towers.

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

⋆ *The area control centres* handle aircraft flying over their territory:

- ◇ taking over their monitoring and control
  - ○ either from ground control towers,
  - ○ or from neighbouring area control centres.
- ◇ Area control centres shall help ensure smooth flight,
  - ○ that aircraft are allotted to appropriate air corridors, if and when needed (as one business process),
  - ○ and are otherwise kept informed of "neighbouring" aircraft and weather conditions en route (other business processes).
- ◇ Area control centres hand over aircraft
  - ○ either to terminal control towers (as yet another business process),
  - ○ or to neighbouring area control centres (as yet another business process).

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

⋆ *The continental control centres*

- ◇ monitor and control, in collaboration with
  - ○ regional and ground control centres,
- ◇ overall traffic in an area comprising several regional control centres (as a major business process),
- ◇ and can thus monitor and control whether contracted (landing) slot allocations and schedules can be honoured,
- ◇ and, if not, reschedule these (landing) slots (as another major business process).

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

- From the above rough sketches of behaviours the domain engineer then goes on to describe
  - ⋆ types of messages (i.e., entities) between behaviours,
  - ⋆ types of entities specific to the behaviours, and
  - ⋆ the functions that apply to or yield those entities.

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

Freight Logistics Business Processes

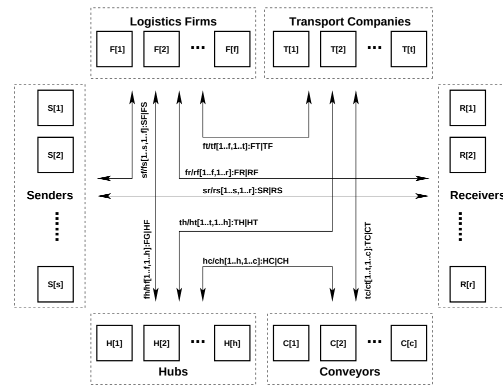


Figure 7.12: A freight logistics behavioural system abstraction

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

- The main business process behaviours of a freight logistics system are the following:
  - ⋆ the senders of freight,
  - ⋆ the logistics firms which plan and coordinate freight transport,
  - ⋆ the transport companies on whose conveyors freight is being transported,
  - ⋆ the hubs between which freight conveyors "ply their trade",
  - ⋆ the conveyors themselves and
  - ⋆ the receivers of freight
- A detailed description for each of the freight logistics business process behaviours listed above should now follow: ...

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

Harbour Business Processes

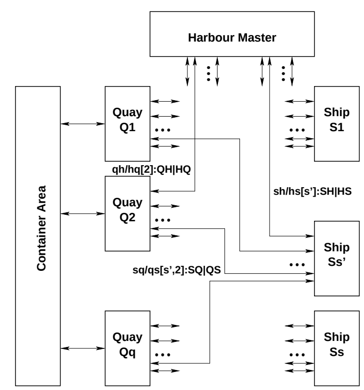


Figure 7.13: A harbour behavioural system abstraction

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

- The main business process behaviours of a harbour system are the following:
  - ⋆ the ships who seek harbour to unload and load cargo at a harbour quay,
  - ⋆ the harbourmaster who allocates and schedules ships to quays,
  - ⋆ the quays at which ships berth and unload and load cargo (to and from a container area) and
  - ⋆ the container area which temporarily stores ("houses") containers
- (Fig. 7.13 on the preceding page).

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

- There may be other parts of a harbour:
  - ⋆ a holding area for ships
    - ◇ to wait before being allowed to properly enter the harbour and be berthed at a buoy or a quay,
    - ◇ or for ships to rest before proceeding; as well as
  - ⋆ buoys at which ships may be anchored while
    - ◇ unloading and loading.
- We shall assume that the course student can properly complete an appropriate, realistic harbour domain.
- A detailed description for each of the harbour business process behaviours listed above should now follow.
- We leave this as an exercise to the reader to complete.

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

Financial Service Industry Business Processes

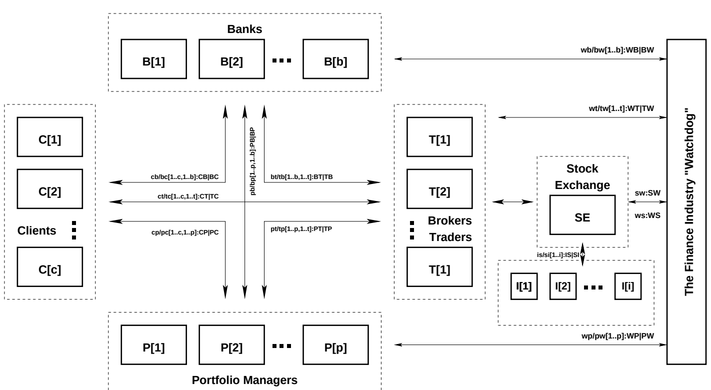


Figure 7.14: A financial behavioural system abstraction

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

- The main business process behaviours of a financial service system are the following:
  - ⋆ clients,
  - ⋆ banks,
  - ⋆ securities instrument brokers and traders,
  - ⋆ portfolio managers,
  - ⋆ (the, or a, or several) stock exchange(s),
  - ⋆ stock incorporated enterprises and
  - ⋆ the financial service industry "watchdog".
- We rough-sketch the behaviour of a number of business processes of the financial service industry.

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

- ⋆ Clients engage in a number of business processes:
  - ◇ they open, deposit into, withdraw from, obtain statements about, transfer sums between and close demand/deposit, mortgage and other accounts;
  - ◇ they request brokers to buy or sell, or to withdraw buy/sell orders for securities instruments (bonds, stocks, futures, etc.); and
  - ◇ they arrange with portfolio managers to look after their bank and securities instrument assets, and occasionally they reinstruct portfolio managers in those respects.

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

- ⋆ Banks engage with clients, portfolio managers, and brokers and traders in exchanges related to client transactions with banks, portfolio managers, and brokers and traders, as well as with these on their own behalf, as clients.
- ⋆ Securities instrument brokers and traders engage with clients, portfolio managers and the stock exchange(s) in exchanges related to client transactions with brokers and traders, and, for traders, as well as with the stock exchange(s) on their own behalf, as clients.

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

- ⋆ Portfolio managers engage with clients, banks, and brokers and traders in exchanges related to client portfolios.
- ⋆ Stock exchanges engage with the financial service industry watchdog, with brokers and traders, and with the stock listed enterprises, reinforcing trading practices, possibly suspending trading of stocks of enterprises, etc.
- ⋆ Stock incorporated enterprises engage with the stock exchange: They send reports, according to law, of possible major acquisitions, business developments, and quarterly and annual stockholder and other reports.
- ⋆ The financial industry watchdog engages with banks, portfolio managers, brokers and traders and with the stock exchanges.

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

Discussion

- An essence of the examples is not the specific diagrams shown,
- but that one can indeed draw such behavioural rough sketches.
- These can include
  - ⋆ square or rounded boxes designating behaviours;
  - ⋆ single- or, as here shown, double-ended arrows, designating the possibility of typed communication of messages (say over channels);
  - ⋆ the (entity) typing of these messages;
  - ⋆ and so on.

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

- Another essence of the examples is hence
  - ⋆ that there is a diagrammatic language of behaviours,
  - ⋆ and that this language has textual counterparts — say in the form of `CSP` or `RSL/CSP`.
- Other diagrammatic forms might be chosen, depending on properties not revealed in the above examples.
- These other forms might be Petri nets,
- message or live sequence charts, or, for example,
- statecharts.

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

- Furthermore, the examples
  - ⋆ are sketchy,
  - ⋆ but they provide an immediate, constructive start
  - ⋆ to the arduous task of carefully and painstakingly describing a domain.
- In all examples we have sketched the suggested arrays of channels and their types (as sorts).
  - ⋆ These are just suggestions.
  - ⋆ Interactions between behaviours are then modelled in terms of messages communicated over these channels.
  - ⋆ But such models are just that: there is no obligation on the part of any, subsequent software design to implement channels as something anywhere similar to channels!

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

- To describe domains fully satisfactorily requires
  - ⋆ at least the full complement of principles, techniques and tools
  - ⋆ covered in all chapters of Vols. 1 and 2,
  - ⋆ as well as in all the chapters up to and including all of the present chapter in this volume!

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

Intrinsics

- Railways, although they have many “players and actors” revolve around some core notions: the rail net and trains on these.
- Overlapping groups of players and actors (i.e., stakeholders), hence different perspectives, in general, have a core of common entities and phenomena.
- We refer to this core as *the intrinsics of the domain.*

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

Principle of Domain Intrinsic

From the outset of describing a domain:

- Analyse it with respect to its intrinsic phenomena and concepts.
- Focus on describing these first.
- Make sure that the descriptions of subsequently described domain facets are subordinated descriptions of the domain facets

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

Overall Principles

- Each stakeholder group typically has its view of a domain.
- Different stakeholder groups may thus have different views of their — otherwise shared — domain.
- In developing a description of the domain intrinsics we must first develop one description per stakeholder group.
- Then, in some step of development, reconcile possible domain description inconsistencies and conflicts.
- To do so systematically we first need to form a basis,
- the intrinsics,
- which is common to all subsequent facets.

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

Intrinsics

By domain *intrinsics* we shall understand

- those phenomena and concepts of a domain which are basic to any of the other facets (listed earlier and treated, in some detail, below),
- with such domain intrinsics initially covering at least one specific, hence named, stakeholder view
- In the next many examples we show typical fragments of rough-sketch or narrative descriptions —
- such as the software developer has to construct when creating a domain description.

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

Railway Net Intrinsics

We narrate and formalise three railway net intrinsics.

- From the view of *potential train passengers*
  - ⋆ a railway net consists of lines, stations and trains.
  - ⋆ A line connects exactly two distinct stations.
- From the view of *actual train passengers*
  - ⋆ a railway net — in addition to the above —
  - ⋆ allows for several lines between any pair of stations
  - ⋆ and, within stations, provides for one or more platform tracks from which to embark or alight a train.

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

- From the view of *train operating staff*
  - ⋆ a railway net — in addition to the above —
  - ⋆ has lines and stations consisting of suitably connected rail units.
  - ⋆ A rail unit is either a simple (i.e., linear, straight) unit, or is a switch unit, or is a simple crossover unit, or is a switchable crossover unit, etc.
  - ⋆ Simple units have two connectors. Switch units have three connectors. Simple and switchable crossover units have four connectors.
  - ⋆ A path (through a unit) is a pair of connectors of that unit.
  - ⋆ A state of a unit is the set of paths, in the direction of which a train may travel. A (current) state may be empty: The unit is closed for traffic.
  - ⋆ A unit can be in either one of a number of states of its state space.

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

- *Potential train passengers:*

scheme N0 =
  class
    type
      N, L, S, Sn, Ln
    value
      obs_Ls: N $\rightarrow$ L-**set**, obs_Ss: N $\rightarrow$ S-**set**
      obs_Ln: L $\rightarrow$ Ln, obs_Sn: S $\rightarrow$ Sn
      obs_Sns: L $\rightarrow$ Sn-**set**, obs_Lns: S $\rightarrow$ Ln-**set**
    axiom
      ...
  end

© Dines Bjørner, 2006

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

- *Actual train passengers:*

scheme N1 = **extend** N0 **with**
  class
    type
      Tr, Trn
    value
      obs_Trs: S $\rightarrow$ Tr-**set**, obs_Trn: Tr $\rightarrow$ Trn
    axiom
      ...
  end

© Dines Bjørner, 2006

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

- *Train operating staff:*

scheme N2 = **extend** N1 **with**
  class
    type
      U, C
      P′ = U $\times$ (C$\times$C)
      P = {| p:P′ • **let** (u,(c,c′))=p **in** (c,c′)$\in \cup$ obs_Ω(u) **end** |}
      Σ = P-**set**
      Ω = Σ-**set**
    value
      obs_Us: (N|L|S) $\rightarrow$ U-**set**
      obs_Cs: U $\rightarrow$ C-**set**
      obs_Σ: U $\rightarrow$ Σ
      obs_Ω: U $\rightarrow$ Ω
    axiom
      ...
  end

© Dines Bjørner, 2006

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

- Different stakeholder perspectives,
- not only of intrinsics, as here,
- but of any facet,
- leads to a number of different models.
- The name of a phenomenon of one perspective, that is, of one model,
- may coincide with the name of a "similar" phenomenon of another perspective, that is, of another model, and so on.
- If the intention is that the "same" names cover comparable phenomena, then the developer must state the comparison relation.

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

Comparable Intrinsics

We claim that the concept of nets, lines and stations in the three models above must relate. The simplest possible relationships are to let the third model be the common "unifier" and to mandate

- that the model of nets, lines and stations of the *potential train passengers* formalisation is that of nets, lines and stations of the *train operating staff* model; and
- that the model of nets, lines, stations and tracks of the *actual train passengers* formalisation is that of nets, lines, stations of the *train operating staff* model.

Thus the third model is seen as the definitive model for the stakeholder views initially expressed.

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

- In general the relationships to be expressed between different stakeholder models require more elaborate expressions.
- To express these formally, in RSL, we make use of RSL's *scheme* facility.
  - ⋆ More elaborate stakeholder schemes can be expressed by *extending* basic (i.e., intrinsic) schemes *with* additional types, values and axioms.
  - ⋆ The *hiding* facility of schemes can likewise be used to express different, but commensurate models.

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

- In the above description such things as lines, stations and units, including their particular kind (linear, switch, etc.) are phenomena, that is, they can be pointed to.
- Such things as connectors and paths could be considered either phenomena or concepts.
- Unit states and unit state spaces, including the idea of open and closed units, will here be considered concepts.
- The above example is only indicative.
- Much care must be taken to ensure that a description is consistent and complete.
- Care must also be taken to not describe phenomena or concepts that more properly belong to some other facets, as covered next.
- Identifying and describing intrinsics is also an art!

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

• Intrinsics of Switches

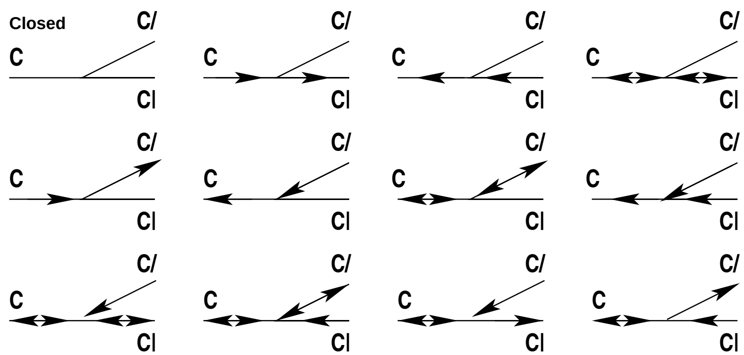


Figure 8.15: Possible states of a rail switch

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

- The intrinsic attribute of a rail switch is that it can take on a number of states.
- A simple switch $({}^{c_|}Y_c^{c_/})$ has three connectors: $\{c, c_|, c_/\}$. c is the connector of the common rail from which one can either "go straight" $c_|$, or "fork" $c_/$.
- So we have that a possible state space of such a switch could be ω_{g_s} :

$$\begin{array}{l}\{\{\},\\ \{(c,c_|)\},\{(c_|,c)\},\{(c,c_|),(c_|,c)\},\\ \{(c,c_/)\},\{(c_/,c)\},\{(c,c_/),(c_/,c)\},\{(c_/,c),(c_|,c)\},\\ \{(c,c_|),(c_|,c),(c_/,c)\},\{(c,c_/),(c_/,c),(c_|,c)\},\{(c_/,c),(c,c_|)\},\{(c,c_/),(c_|,c)\}\}\end{array}$$

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

- The above models a general switch ideally.
- Any particular switch ω_{p_s} may have $\omega_{p_s} \subset \omega_{g_s}$.
- Nothing is said about how a state is determined:
  - ⋆ who sets and resets it,
  - ⋆ whether determined solely by the physical position of the switch gear,
  - ⋆ or also by visible or virtual (i.e., invisible, intangible) signals up or down the rail, away from the switch.

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

Conceptual Versus Actual Intrinsics

- In order to bring an otherwise seemingly complicated domain across to the reader,
- one may decide to present it piecemeal:
  - ⋆ First, one presents the very basics, the fewest number of inescapable entities, functions and behaviours.
  - ⋆ Then, in a step of enrichment, one adds a few more (intrinsic) entities, functions and behaviours.
  - ⋆ And so forth.
  - ⋆ In a final step one adds the last (intrinsic) entities, functions and behaviours.

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

- In order to develop what initially may seem to be a complicated domain,
- one may decide to develop it piecemeal:
  - ⋆ We basically do as for the presentation steps:
  - ⋆ Steps of enrichments —
  - ⋆ from a big lie, via increasingly smaller lies, till one reaches a truth!

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

Conceptual Intrinsics: Freight Transport

- The very essence of freight transport is:
  - ⋆ Entities: Senders, freight, “the system of transport”, and receivers.
  - ⋆ Functions:
    - ◇ submitting an item of freight for transport, and
    - ◇ receiving an item of freight having been transported.
  - ⋆ Behaviour: Being transported.

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

type
  Sndr, Frei, Rcvr
value
  submit: Sndr × Frei → System → System
  receiv: Rcvr → System → System × Frei
  transport: System → System

Observe that we have said nothing, really, about “the system of transport.

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

Actual Intrinsics: Freight Logistics

- We now elaborate on “the system of transport” alluded to earlier.
  - ⋆ The system entities are: harbours, bills of lading, ships and ship routes (from harbours to harbours).
    - ◇ We assume that there is no need to detail what are harbours, ships and ship routes.
    - ◇ A bill of lading is a document, say attached to a piece of freight, which stipulates properties of the freight (sender, receiver, origin of transport, destination of transport and route of transport: sequence of harbours and ships, sailing times, etc.).

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

⋆ The system functions are:

- ⋄ submit a piece of freight to a harbour (of origin) indicating a receiver and a harbour of destination, and obtaining a bill of lading;
- ⋄ load a piece of freight from a harbour to a ship, as prescribed by that freight's bill of lading;
- ⋄ unload a piece of freight from a ship to a harbour, as prescribed by that freight's bill of lading;
- ⋄ fetching, by a receiver, a piece of freight from a destination harbour, as prescribed by that freight's bill of lading.

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

⋆ A system behaviour could be the sequence of one submission, one or more pairs of loadings and unloadings, ended by one fetch.

- ⋄ The above behaviour has abstracted "away" any notion of sailings,
- ⋄ i.e., of actual movement!

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

Freight Logistics

```
type
  Sndr, Sndr_Na, Frei, Rcvr, Rcvr_Na,
  Harb, H_Na, Ship, S_Na, System, BoL
  Dest = H_Na
value
  obs_Harbs: System → Harb-set
  obs_HNa: Harb → H_Na
  obs_Route : BoL → (H_Na × S_Na)*
  obs_Dest : BoL → HNa
  obs_RcvrNa : BoL → Rcvr_Na
  obs_RcvrNa : Rcvr → Rcvr_Na

  submit: Sndr × Frei × Dest → System → BoL
  load: Frei × BoL × Ship × Harb → Ship × Harb
  unload: BoL × Ship × Harb → Ship × Harb × Frei
  receiv: Rcvr → Harb → System → Frei × BoL
  transp: System → System
```


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

The formalisation, as does the narrative, only rough-sketches some intrinsics of freight logistics.

- We leave the two versions, the virtual and the "more realistic", further undefined.
- Both descriptions were kept in the form of rough sketches.
- The latter can take being further refined, i.e., made more precise.

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

Discussion

- The intrinsics become part of every one of the next facets.
- From an algebraic semantics point of view these latter are extensions of the above.
- We have presented a story of intrinsics as truthfully as we could.
  - ⋆ To decide on what is intrinsics and what is not is an art — it is a matter of choice, hence of style.
  - ⋆ There is no clear-cut criterion according to which a line of separation between intrinsics and nonintrinsics can be drawn.

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

Utter Barebones Intrinsics

- It was implied above that an absolute barebones intrinsics of railways was the atomic trains and the rail net abstracted to atomic lines and atomic stations.
- Similarly one could claim that an absolute barebones intrinsics of a hospital system was the atomic patients, atomic medical staff and atomic beds. Without the beds the first two kinds of entities would pass only for a physician's office.
- And similarly one could claim that an absolute barebones intrinsics for air traffic would be the aircraft, the airports and the air space.
- And so on.

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

- The reason we bring this concept of *utter barebones intrinsics* up is three-fold.
  - ⋆ First, the domain engineer must "think very hard" in trying to isolate, identify and capture the, or an utter barebones intrinsics of a domain.
  - ⋆ Secondly, the "more frugal" the domain engineer has been in selecting the utter barebones entities, functions, events and behaviours, the more time that domain engineer has to care about properly extending that utter barebones intrinsics with the remaining domain facets covered next.
  - ⋆ Thirdly, by "forcibly" trying to isolate an utter barebone intrinsics the domain engineer is actually trying to establish a scientific basis for the domain. The domain describer is more of a researcher than an engineer. This is basically untrodden land: few have tried to formulate domain descriptions let alone intrinsics, and very few, if any may have attempted to identify the utter barebones of a domain.
- We claim that it is a prerequisite for good domain descriptions to have tried to discover utter barebones intrinsics.

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

Support Technologies

- Technology is meant to support human activities.
- Usually technology replaces human actions one to one, i.e., rather directly.
- (That is, for one human action kind there is usually a substitute technology.)
- In other instances technology radically transforms the ways in which things are done.
- Hence:

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

When describing a domain:

- analyse it with respect to its support technology phenomena and concepts — the subject of this lecture;
- focus on possibly describing these separately; and
- make sure that descriptions of other described domain facets are commensurate with possibly multiple, alternative descriptions of domain support technologies

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

Overall Principles

- Earlier we implied that a switch may take on a number of states:
- linking, into paths, suitable pairs of connectors, or none.
- But how such states came about was abstracted (away).

By domain *support technology* we shall understand

- ways and means of implementing certain observed phenomena

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

- The above characterisation is deliberately loose.
- It is so, so that we are not, later, constrained by a too tight characterisation.
- Therefore it is important to illustrate the idea,
- so as to aid the student's intuition,
- and thus enable proper identification and description of support technologies.

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

Railway Support Technology

We give a rough sketch description of possible rail unit switch technologies.

- In "ye olde" days, rail switches were "thrown" by manual labour, i.e., by railway staff assigned to and positioned at switches.
- With the advent of reasonably reliable mechanics, pulleys and levers[11] (and steel wires), switches were made to change state by means of "throwing" levers in a cabin tower located centrally at the station (with the lever then connected through wires etc., to the actual switch).
- This partial mechanical technology then emerged into electromechanics, and cabin tower staff was "reduced" to pushing buttons.
- Today, groups of switches, either from a station arrival point to a station track, or from a station track to a station departure point, are set and reset by means also of electronics, by what is known as interlocking (for example, so that two different routes cannot be open in a station if they cross one another).

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

- It must be stressed that the above is just a rough sketch.
- In a proper narrative description the software (cum domain) engineer must describe, in detail, the subsystem of electronics, electromechanics and the human operator interface (buttons, lights, sounds, etc.).
- An aspect of supporting technology includes recording the state-behaviour in response to external stimuli.
- We give an example.

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

Probabilistic Rail Switch Unit State Transitions

- Figure 9.16 intends to model the probabilistic (erroneous and correct) behaviour of a switch when subjected to settings (to switched (*s*) state) and resettings (to direct (*d*) state).
- A switch may go to the switched state from the direct state when subjected to a switch setting *s* with probability *psd*.

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

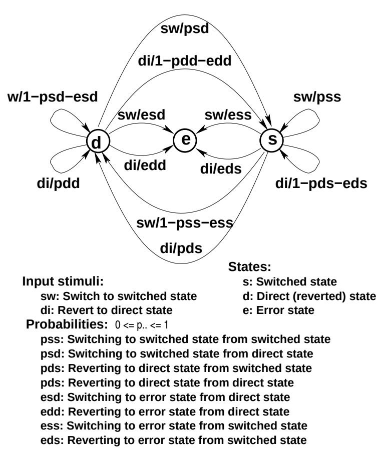


Figure 9.16: Probabilistic state switching

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

Another example shows another aspect of support technology:

- Namely that the technology must guarantee certain of its own behaviours,
- so that software designed to interface with this technology,
- together with the technology, meets dependability requirements.

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

Railway Optical Gates

- Train traffic (itf:iTF), intrinsically, is a total function over some time interval, from time (t:T) to continuously positioned (p:P) trains (tn:TN).
- Conventional optical gates sample, at regular intervals, the intrinsic train traffic.
- The result is a sampled traffic (stf:sTF).
- Hence the collection of all optical gates, for any given railway, is a partial function from intrinsic to sampled train traffics (stf).
- We need to express quality criteria that any optical gate technology should satisfy — relative to a necessary and sufficient description of a *close*ness predicate.

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

- For all intrinsic traffics, *itf*, and for all optical gate technologies, *og*, the following must hold:
  - ⋆ Let *stf* be the traffic sampled by the optical gates.
  - ⋆ For all time points, *t*, in the sampled traffic,
  - ⋆ those time points must also be in the intrinsic traffic,
  - ⋆ and, for all trains, *tn*, in the intrinsic traffic at that time,
  - ⋆ the train must be observed by the optical gates, and
  - ⋆ the actual position of the train and the sampled position must somehow be checkable to be close, or identical to one another.

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

Railway Optical Gate Technology Requirements

type
$\quad \text{T, TN}$
$\quad \text{P} = \text{U}^*$
$\quad \text{NetTraffic} == \text{net:N} \;\; \text{trf:(TN} \underset{m}{\rightarrow} \text{P)}$
$\quad \text{iTF} = \text{T} \rightarrow \text{NetTraffic}$
$\quad \text{sTF} = \text{T} \underset{m}{\rightarrow} \text{NetTraffic}$
$\quad \text{oG} = \text{iTF} \xrightarrow{\sim} \text{sTF}$
value
$\quad [\,\text{close}\,]\ \text{c: NetTraffic} \times \text{TN} \times \text{NetTraffic} \xrightarrow{\sim} \mathbf{Bool}$
axiom
$\quad \forall\ \text{itt:iTF, og:OG} \cdot \mathbf{let}\ \text{stt} = \text{og(itt)}\ \mathbf{in}$
$\quad\quad \forall\ \text{t:T} \cdot \text{t} \in \mathbf{dom}\ \text{stt} \cdot$
$\quad\quad\quad \text{t} \in \mathcal{D}\ \text{itt} \wedge \forall\ \text{Tn:TN} \cdot \text{tn} \in \mathbf{dom}\ \text{trf(itt(t))}$
$\quad\quad\quad\quad \Rightarrow \text{tn} \in \mathbf{dom}\ \text{trf(stt(t))} \wedge \text{c(itt(t),tn,stt(t))}\ \mathbf{end}$

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

Checkability is an issue of testing the optical gates when delivered for conformance to the *close*ness predicate, i.e., to the axiom.

Air Traffic Control (ATC)

We refer to the business process description of ATC.

- The particular decomposition of air traffic control into the domain described, the ground, terminal, area and continental (monitoring and) control centres, represents but one composition of technologies.
  - ⋆ The pragmatics, i.e., the assumptions underlying that combined ground, terminal, area and continental control centre support technology is that all monitoring and control was to take place from the ground.

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

- Future technologies, easily implementable today, facilitate the following alternative "sum total" technologies:
  - ⋆ Most, if not all, of the human guidance that today takes place at these control centres can be automated and physically moved
    - ⋄ either to fixed space-positioned satellites,
    - ⋄ or to each aircraft itself.
  - ⋆ Intermediate support technologies shall then feature solutions that are intermediary to the present and the future support technologies.

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

Methodological Consequences

Support Technology

- The *support technologies* model of a domain is a partial specification, hence all the usual abstraction and modelling principles, techniques and tools apply. More specifically,
- support technologies (st:ST) "implement" intrinsic contexts and states: $\theta_i : \Theta_i$ in terms of "actual" contexts and states: $\theta_a : \Theta_a$:

type
Θ_i, Θ_a
ST $= \Theta_i \rightarrow \Theta_a$
axiom
$\forall$ sts:ST-**set**, st:ST $\cdot$ st $\in$ sts $\Rightarrow \forall\, \theta_i{:}\Theta_i,\ \exists\, \theta_a{:}\Theta_a \cdot$ st$(\theta_i) = \theta_a$

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

- The formal requirements can be narrated:
  - ⋆ Let Θ_i and Θ_a designate the spaces of intrinsic and actual-world configurations (contexts and states).
  - ⋆ For each intrinsic configuration model — that we know is support technology assisted —
  - ⋆ there exists a support technology solution,
  - ⋆ that is, a total function from all intrinsic configurations to corresponding actual configurations.
- If we are not convinced that there is such a function then there is little hope that we can trust this technology

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

- Support technology is not a refinement, but an extension.
- Support technology typically introduces considerations of
  - ⋆ technology accuracy — reliability ⋆
  - ⋆ fault tolerance — availability ⋆
  - ⋆ accessability — safety ⋆
- Axioms characterise members of the set of support technologies (sts).
- An example axiom was given in the optical gate example.

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

Support Technology

The *support technology* principle is relative to all other domain facets.

- It expresses that one must first describe essential intrinsics.
- Then it expresses that support technology is any means of implementing concrete instantiations
  - ⋆ of some intrinsics,
  - ⋆ of some management and organisation,
  - ⋆ and/or of some rules and regulations,
  - ⋆ and so on

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

- Generally the principle states that one must always be on the look out for and inspire new support technologies.
- The most abstract form of the principle is: *What is a support technology one day becomes part of the domain intrinsics a future day.*

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

Management & Organisation

- It is a basic characteristic of human-made systems
- that they are managed by humans
- and that their management and the managed are structured in organisational structures.
- This lecture is about how we model this facet.

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

When describing a domain:

- analyse it with respect to its management and organisation phenomena and concepts — the subject of this lecture;
- focus on possibly describing these separately; and
- make sure that descriptions of other described domain facets are commensurate with possibly multiple, alternative descriptions of domain management and organisation

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

Overall Principles

- Activities of some (application) domains are made up by the actions of many people.
- It is therefore common to organise these into levels of management and many groups of "floor", i.e., nonmanagement staff.
- Railway systems are usually characterised by highly structured management organisations, and rules and regulations set up by upper echelons of management to be followed by lower levels and by ground staff and users.

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

Train Monitoring, I

- In China, as an example, rescheduling of trains occurs at stations and involves telephone negotiations with neighbouring stations ("up and down the lines").
- Such rescheduling negotiations, by phone, imply reasonably strict management and organisation (M&O). This kind of M&O reflects the geographical layout of the rail net.

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

Management

By domain *management* we shall understand such people (such decisions)

- who (which) determine, formulate and thus set standards (cf. rules and regulations, a later lecture topic) concerning
  - ⋆ strategic, tactical and operational

  decisions;
- who ensure that these decisions are passed on to (lower) levels of management, and to floor staff;
- who make sure that such orders, as they were, are indeed carried out;
- who handle undesirable deviations in the carrying out of these orders cum decisions;
- and who "backstop" complaints from lower management levels and from floor staff

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

Organisation

By domain *organisation* we shall understand

- the structuring of management and nonmanagement staff levels;
- the allocation of
  - ⋆ strategic,
  - ⋆ tactical and
  - ⋆ operational

  concerns to within management and nonmanagement staff levels;
- and hence the "lines of command":
  - ⋆ who does what, and
  - ⋆ who reports to whom,
    - ◇ administratively and
    - ◇ functionally

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

Railway Management and Organisation: Train Monitoring, II

- Certain (lowest-level operational and station-located) supervisors are responsible for the day-to-day timely progress of trains within a station and along its incoming and outgoing lines, and according to given timetables.
- These
  - ⋆ supervisors
  - ⋆ and their immediate (middle-level) managers (see below for regional managers)
- set guidelines (for local station and incoming and outgoing lines)
  - ⋆ for the monitoring of train traffic,
  - ⋆ and for controlling trains that are either ahead of or behind their schedules.

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

- By an incoming and an outgoing line we mean part of a line between two stations, the remaining part being handled by neighbouring station management.
- Once it has been decided, by such a manager, that a train is not following its schedule, based on information monitored by nonmanagement staff,
- then that manager directs that staff:
  - ⋆ to suggest a new schedule for the train in question, as well as for possibly affected other trains,
  - ⋆ to negotiate the new schedule with appropriate neighbouring stations, until a proper reschedule can be decided upon, by the managers at respective stations,
  - ⋆ and to enact that new schedule.
- A (middle-level operations) manager for regional traffic, i.e., train traffic involving several stations and lines, resolves possible disputes and conflicts.

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

- The above, albeit rough-sketch description, illustrated the following management and organisation issues:
  - ⋆ There is a set of lowest-level (as here: train traffic scheduling and rescheduling) supervisors and their staff.
  - ⋆ They are organised into one such group (as here: per station).
  - ⋆ There is a middle-level (as here: regional train traffic scheduling and rescheduling) manager (possibly with some small staff),
  - ⋆ organised with one such per suitable (as here: railway) region.
  - ⋆ The guidelines issued jointly by local and regional (...) supervisors and managers imply an organisational structuring of lines of information provision and command.

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

A Conceptual Analysis, I

- People staff enterprises, the components of infrastructures with which we are concerned, i.e., for which we develop software.
- The larger these enterprises — these infrastructure components — the more need there is for management and organisation.
- The role of management is roughly twofold:

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

- ⋆ first, to perform strategic, tactical and operational work, to set strategic, tactical and operational policies — and to see to it that they are followed.
- ⋆ The role of management is, second, to react to adverse conditions, that is, to unforeseen situations, and to decide how they should be handled, i.e., conflict resolution.

- Policy setting should help nonmanagement staff operate normal situations — those for which no management interference is thus needed.
- And management "backstops" problems: management takes these problems off the shoulders of nonmanagement staff.

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

- To help management and staff know who's in charge wrt. policy setting and problem handling, a clear conception of the overall organisation is needed.
  - ⋆ Organisation defines lines of communication within management and staff, and between these.
  - ⋆ Whenever management and staff has to turn to others for assistance they usually, in a reasonably well-functioning enterprise, follow the command line: the paths of organigrams — the usually hierarchical box and arrow/line diagrams.

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

Methodological Consequences, I+II

Management and Organisational

- The *management and organisation* model of a domain is a partial specification; hence all the usual abstraction and modelling principles, techniques and tools apply. More specifically,
- management is a set of predicates, observer and generator functions which either parameterise other, the operations functions, that is, determine their behaviour, or yield results that become arguments to these other functions

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

Conceptual Analysis, II

- To relate classical organigrams to formal descriptions we first show such an organigram (Fig. 10.17),
- and then we show schematic processes which — for a rather simple scenario — model managers and the managed!

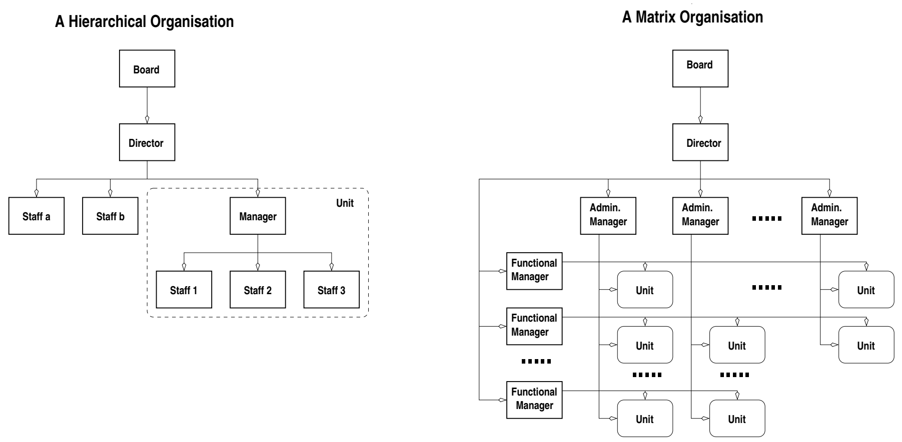


Figure 10.17: Organisational structures

- Based on such a diagram, and modelling only one neighbouring group of a manager and the staff working for that manager we get
  - ⋆ a *system* in which one manager, *mgr*, and many staff, *stf*, coexist or work concurrently, i.e., in parallel.
  - ⋆ The *mgr* operates in a context and a state modelled by ψ.
  - ⋆ Each staff, *stf(i)* operates in a context and a state modelled by *s*σ*(i)*.

Conceptual Model of a Manager-Staff Relation, I

type
$\mathsf{Msg}, \Psi, \Sigma, \mathsf{Sx}$
$\mathsf{S\Sigma} = \mathsf{Sx} \ \overrightarrow{m}\ \Sigma$
channel
$\{\ \mathsf{ms}[\,\mathsf{i}\,]{:}\mathsf{Msg} \mid \mathsf{i}{:}\mathsf{Sx}\ \}$
value
$\mathsf{s}\sigma{:}\mathsf{S\Sigma},\ \psi{:}\Psi$

$\mathsf{sys}{:}\ \mathbf{Unit} \rightarrow \mathbf{Unit}$
$\mathsf{sys}() \equiv \|\ \{\ \mathsf{stf(i)(s}\sigma\mathsf{(i))} \mid \mathsf{i{:}Sx}\ \}\ \|\ \mathsf{mgr}(\psi)$

- In this system
  - ⋆ the manager, *mgr*,
    - ◇ (1) either broadcasts messages, *msg*, to all staff via message channel *ms[i]*. The manager's concoction, *mgr_out*(ψ), of the message, *msg*, has changed the manager state.
    - ◇ Or (2) is willing to receive messages, *msg*, from whichever staff *i* the manager sends a message. Receipt of the message changes, *mgr_in(i,msg)*(ψ), the manager state.
  - ⋆ In both cases the manager resumes work as from the new state.
  - ⋆ The manager chooses — in this model — which of thetwo things (1 or 2) to do by a so-called nondeterministic internal choice ($\sqcap$).

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

Conceptual Model of a Manager-Staff Relation, II

$$
\begin{array}{l}
\quad \mathsf{mgr}\!: \Psi \rightarrow \mathbf{in,out}\ \{\ \mathsf{ms}[\,\mathsf{i}\,] \mid \mathsf{i{:}Sx}\ \}\ \mathbf{Unit} \\
\quad \mathsf{mgr}(\psi) \equiv \\
(1)\ \ (\mathbf{let}\ (\psi',\mathsf{msg}) = \mathsf{mgr\_out}(\psi)\ \mathbf{in} \\
\quad\ \ \| \ \{\ \mathsf{ms}[\,\mathsf{i}\,]!\mathsf{msg} \mid \mathsf{i{:}Sx}\ \}\ ;\ \mathsf{mgr}(\psi')\ \mathbf{end}) \\
\quad\ \ \prod \\
(2)\ \ (\mathbf{let}\ \ \psi' = [\!]\ \{\mathbf{let}\ \mathsf{msg} = \mathsf{ms}[\,\mathsf{i}\,]?\ \mathbf{in} \\
\quad\ \ \mathsf{mgr\_in}(\mathsf{i},\mathsf{msg})(\psi)\ \mathbf{end} \mid \mathsf{i{:}Sx}\ \}\ \mathbf{in}\ \mathsf{mgr}(\psi')\ \mathbf{end})
\end{array}
$$

$$
\begin{array}{l}
\mathsf{mgr\_out}\!: \Psi \rightarrow \Psi \times \mathsf{MSG}, \\
\mathsf{mgr\_in}\!: \mathsf{Sx} \times \mathsf{MSG} \rightarrow \Psi \rightarrow \Psi
\end{array}
$$

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

- And in this system,
  - ⋆ staff *i, stf(i)*,
    - ◇ (1) either is willing to receive a message, *msg*, from the manager, and then to change, *stf_in(msg)(σ)*, state accordingly,
    - ◇ or (2) to concoct, *stf_out(σ)*, a message, *msg* (thus changing state) for the manager, and send it *ms[i]!msg*.
  - ⋆ In both cases the staff resumes work as from the new state.
  - ⋆ The staff member chooses — in this model — which of thetwo “things” (1 or 2) to do by a nondeterministic internal choice ($\prod$).

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

Conceptual Model of a Manager-Staff Relation, III

$$
\begin{array}{l}
\quad \mathsf{stf}\!: \mathsf{i{:}Sx} \rightarrow \Sigma \rightarrow \mathbf{in,out}\ \mathsf{ms}[\,\mathsf{i}\,]\ \mathbf{Unit} \\
\quad \mathsf{stf}(\mathsf{i})(\sigma) \equiv \\
(1)\ \ (\mathbf{let}\ \mathsf{msg} = \mathsf{ms}[\,\mathsf{i}\,]?\ \mathbf{in}\ \mathsf{stf}(\mathsf{i})(\mathsf{stf\_in}(\mathsf{msg})(\sigma))\ \mathbf{end}) \\
\quad\ \ \prod \\
(2)\ \ (\mathbf{let}\ (\sigma',\mathsf{msg}) = \mathsf{stf\_out}(\sigma)\ \mathbf{in}\ \mathsf{ms}[\,\mathsf{i}\,]!\mathsf{msg};\ \mathsf{stf}(\mathsf{i})(\sigma')\ \mathbf{end})
\end{array}
$$

$$
\begin{array}{l}
\mathsf{stf\_in}\!: \mathsf{MSG} \rightarrow \Sigma \rightarrow \Sigma, \\
\mathsf{stf\_out}\!: \Sigma \rightarrow \Sigma \times \mathsf{MSG}
\end{array}
$$

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

- Both manager and staff processes recurse (i.e., iterate) over possibly changing states.
- The management process nondeterministically, external choice, “alternates” between “broadcast”-issuing orders to staff and receiving individual messages from staff.
- Staff processes likewise nondeterministically, external choice, alternate between receiving orders from management and issuing individual messages to management.
- The conceptual example also illustrates modelling stakeholder behaviours as interacting (here *CSP*-like) processes.

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

DTU

Discussion

- The domain models of management and organisation eventually find their way into requirements and, hence, the software design —
- for those cases in which the requirements are about computing support of management and its organisation.
- Support in the solution of the recursive equations of the earlier stakeholder example may be offered in the form of constraint-satisfaction solvers.

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

DTU

- These may partially handle logic characterisations of the strategic and tactical management functions.
- They might then do so in the form of computerised support of message passing between the various management groups (of, for example, that stakeholder example), as well as of the generic example of the present part.

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

DTU

Rules & Regulations

- Railway systems, for example, are characterised by large varieties of rules for appropriate behaviour of:
  - ⋆ trains,
  - ⋆ train dispatch,
  - ⋆ monitoring and control,
  - ⋆ supporting technology,
  - ⋆ and hence of humans at all levels.
- This is also true for most other systems that we might care to consider.

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

DTU

- When rules are broken regulations take effect:
  - ⋆ Humans may be disciplined,
  - ⋆ and activities of the domain may be adjusted.

When describing a domain:

- analyse it with respect to its rules and regulations phenomena and concepts — the subject of this lecture;
- focus on possibly describing these separately; and
- make sure that the descriptions of other domain facets are commensurate with possibly multiple, alternative descriptions of domain rules and regulations

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

Overall Principles

- Earlier, when we dealt with management and organisation, it was hinted that management may issue certain guidelines.
- We now look at a special class of these.

Rule

By a domain *rule* we shall understand

- some text (in the domain) which prescribes how people or equipment are expected to behave when dispatching their duty, respectively when performing their function

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

Regulation

By a *domain regulation* we shall understand

- some text (in the domain) which prescribes what remedial actions are to be taken when it is decided that a rule has not been followed according to its intention
- Rules are like one part of a law: *Thou shalt!*
- Regulations are like another part of a law: *If you break this law "thou" can expect the following punishment!*

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

- Rules and regulations are set
  - ⋆ by enterprises,
  - ⋆ by equipment manufacturers,
  - ⋆ by enterprise associations,
  - ⋆ by [government] regulatory agencies,
  - ⋆ and by society (the latter in the form of laws).
- Adherence to rules is likewise monitored by these or similar institutions.
- Enforcement of (i.e., the imposition of what is specified in) regulations is similarly ensured by these or similar institutions.

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

Trains at Stations

- Rule:
  - ⋆ In China the arrival and departure of trains at, respectively from, railway stations is subject to the following rule:
  - ⋆ *In any three-minute interval at most one train may either arrive to or depart from a railway station.*
- Regulation:
  - ⋆ *If it is discovered that the above rule is not obeyed*, then there is some regulation which prescribes administrative or legal management and/or staff action, as well as some correction to the railway traffic.

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

Trains Along Lines

- Rule:
  - ⋆ In many countries railway lines (between stations) are segmented into blocks or sectors. The purpose is to stipulate that if two or more trains are moving along the line, then:
  - ⋆ *There must be at least one free sector (i.e., without a train) between any two trains along a line.*
- Regulation:
  - ⋆ *If it is discovered that the above rule is not obeyed*, then there is some regulation which prescribes administrative or legal management and/or staff action, as well as some correction to the railway traffic.

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

- It is, as for all other domain facets, crucially important that rules and regulations are captured and precisely described —
- as we often shall find that requirements of software
  - ⋆ either assume these rules to hold,
  - ⋆ or expect such rules to be enforced.

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

Methodological Consequences

Rules and Regulations

- There are, abstractly speaking, usually three kinds of languages involved wrt. (i.e., when expressing) rules and regulations (respectively when invoking actions that are subject to rules and regulations).
  - ⋆ Two languages, Rules and Reg, exist for describing rules, respectively regulations; and
  - ⋆ one, Stimulus, exists for describing the form of the [always current] domain action stimuli.

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

- A syntactic stimulus, *sy_sti*, denotes a function, *se_sti:STI:* $\Theta \rightarrow \Theta$, from any configuration to a next configuration
- A syntactic rule, *sy_rul:Rule,* has as its semantics, its meaning, *rul:RUL,*
  - ⋆ a predicate over current and next configurations, $(\Theta \times \Theta) \rightarrow$ **Bool**,
  - ⋆ where these next configurations have been caused, by the stimuli. These stimuli express:
  - ⋆ If the predicate holds then the stimulus will result in a valid next configuration.

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

Conceptual Model of Rules, 1

type
Stimulus, Rule, Θ
STI = $\Theta \rightarrow \Theta$
RUL = $(\Theta \times \Theta) \rightarrow$ **Bool**
value
meaning: Stimulus $\rightarrow$ STI
meaning: Rule $\rightarrow$ RUL

valid: Stimulus $\times$ Rule $\rightarrow \Theta \rightarrow$ **Bool**
valid(sy_sti,sy_rul)(θ) $\equiv$ meaning(sy_rul)(θ,(meaning(sy_sti))(θ))

valid: Stimulus $\times$ RUL $\rightarrow \Theta \rightarrow$ **Bool**
valid(sy_sti,se_rul)(θ) $\equiv$ se_rul(θ,(meaning(sy_sti))(θ))

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

- A syntactic regulation, *sy_reg:Reg* (related to a specific rule), stands for, i.e., has as its semantics, its meaning,
  - ⋆ a semantic regulation, *se_reg:REG*,
  - ⋆ which is a pair.
  - ⋆ This pair consists of
    - ◇ a predicate, *pre_reg:Pre_REG*, where *Pre_REG* $= (\Theta \times \Theta) \rightarrow$ **Bool**,
    - ◇ and a domain configuration-changing function, *act_reg:Act_REG*, where *Act_REG* $= \Theta \rightarrow \Theta$,
    - ◇ that is, both involving current and next domain configurations.

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

  - ⋆ The two kinds of functions express:
    - ◇ If the predicate holds,
    - ◇ then the action can be applied.
- The predicate is almost the inverse of the rules functions.
- The action function serves to undo the stimulus function.

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

Conceptual Model of Regulations, 2

type
Reg
Rul_and_Reg = Rule $\times$ Reg
REG = Pre_REG $\times$ Act_REG
Pre_REG = $\Theta \times \Theta \rightarrow$ **Bool**
Act_REG = $\Theta \rightarrow \Theta$
value
interpret: Reg $\rightarrow$ REG

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

- The idea is now the following:
  - ⋆ Any action of the system, i.e., the application of any stimulus,
    - ⋄ may be an action in accordance with the rules,
    - ⋄ or it may not.
  - ⋆ Rules therefore express whether stimuli are valid or not in the current configuration.
  - ⋆ And regulations therefore express whether they should be applied, and, if so, with what effort.

-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

- More specifically,
  - ⋆ there is usually, in any current system configuration, given a set of pairs of rules and regulations.
  - ⋆ Let *(sy_rul,sy_reg)* be any such pair.
  - ⋆ Let *sy_sti* be any possible stimulus.
  - ⋆ And let θ be the current configuration.
  - ⋆ Let the stimulus, *sy_sti*, applied in that configuration result in a next configuration, θ', where $\theta' =$ *(meaning(sy_sti))*(θ).
  - ⋆ Let θ' violate the rule, $\sim$*valid(sy_sti,sy_rul)*(θ),
  - ⋆ then if predicate part, *pre_reg*, of the meaning of the regulation, *sy_reg*, holds in that violating next configuration, *pre_reg*$(\theta,$*(meaning(sy_sti))*$(\theta))$,
  - ⋆ then the action part, *act_reg*, of the meaning of the regulation, *sy_reg*, must be applied, *act_reg*(θ), to remedy the situation.

+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

Conceptual Model of Rules and Regulations, 3

```
axiom
 ∀ (sy_rul,sy_reg):Rul_and_Regs ·
  let se_rul = meaning(sy_rul),
      (pre_reg,act_reg) = meaning(sy_reg) in
   ∀ sy_sti:Stimulus, θ:Θ ·
    ∼valid(sy_sti,se_rul)(θ)
      ⇒ pre_reg(θ,(meaning(sy_sti))(θ))
        ⇒ ∃ nθ:Θ · act_reg(θ)=nθ ∧ se_rul(θ,nθ)
  end
```

-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

- It may be that the regulation predicate fails to detect applicability of regulations actions.
- That is, the interpretation of a rule differs, in that respect, from the interpretation of a regulation.
- Such is life in the domain, i.e., in actual reality

+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

- We have given an outline of the basic conditions under which a set of rules and regulations must be designed.
- Whether they are, in actual life, designed, by people, and to be interpreted and followed by people, as described here is not for us to decide.
- Such concerns are the prerogatives of business process reengineering and domain requirements
- We will cover such concerns in later lectures.

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

Rules and Regulation Languages

- We have outlined the basic properties any set of rules and regulations must imply in a properly functioning organisation.
- The axioms prescribed above are abstract.
- They also apply, inter alia, to natural language expressions of rules and regulations.
- It would be nice if rules and regulations could be formalised.
- Then, given an appropriate model of the domain, one might be able to analyse the consistency and completeness of rules and regulations with respect to the domain model.

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

- It is inside the scope, but outside the span of these lectures to bring in — as of 2006 — research material on this subject.
- In other words: Expect it to come, one day, probably couched in terms of some modal logics of knowledge and belief, and/promise and commitment, etc.

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

- Essentially, the issues are:
  - ⋆ first, to design and use languages (one or more, *Rul, Reg*),
  - ⋆ with proper, possibly modal constructs,
  - ⋆ for expressing rules and regulations.
  - ⋆ Second, we need to compile such expressions of rules and regulations.
  - ⋆ Finally, we need to let a computer check "all the time" whether stimuli (whether human or otherwise generated) might cause
  - ⋆ transitions that may result in violations of the rules.

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

Principles and Techniques

Principles: Rules and Regulations

Domains are governed by rules and regulations: by laws of nature or edicts by humans.

- Laws of nature
  - ⋆ can be part of intrinsics,
  - ⋆ or can be modelled as rules and regulations constraining the intrinsics.
- Edicts by humans
  - ⋆ usually change,
  - ⋆ but are normally considered part of an irregularly changing context,
  - ⋆ not a recurrently changing state.

Modelling techniques follow these principles

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

Techniques: Rules and Regulation

- *Rules and regulations,* in the domain, are therefore domain-modelled
  - ⋆ by abstract or concrete syntaxes of syntactic rules,
  - ⋆ by abstract types of denotations and
  - ⋆ by semantics definitions, usually in the form of axioms or denotation-ascribing functions.

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

- Such rules and regulations modelling must allow for conflicts between rule and regulation interpretations:
  - ⋆ that rules are interpreted to state that a next configuration is not valid,
  - ⋆ while a regulation (applicability) predicate does not hold.
- Stimuli, without here going into details, may be modelled by nondeterministic external events, i.e., CSP-like inputs

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

Reminder

We remind the reader of the principle stated at the outset of this lecture on domain rules and regulations:

When describing a domain:

- analyse it with respect to its rules and regulations phenomena and concepts — the subject of this lecture;
- focus on possibly describing these separately; and
- make sure that the descriptions of other domain facets are commensurate with possibly multiple, alternative descriptions of domain rules and regulations

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

Human Behaviour

- Let us consider the staff of any enterprise, any place of work, whether private or public.
  - ⋆ Some go about doing their job **conscientiously: diligently** carrying out tasks as expected.
  - ⋆ Other staff unconsciously sometimes forget: are sometimes a bit **sloppy** in the dispatch of duties.
  - ⋆ Yet other staff set themselves lower standards for the pursuit of their assignments: they are **slovenly delinquent** in completing their work.
  - ⋆ Finally it may be that some staff are **outright criminal** in doing their work: They misappropriate funds or steal from the warehouse, etc.

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

- A whole spectrum of quality thus characterises human work.

When describing a domain,

- analyse it with respect to its human behaviour phenomena and concepts.
- Focus on possibly describing these separately.
- Make sure that descriptions of other described domain facets are commensurate with possibly multiple, alternative descriptions of domain human behaviours

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

Overall Principles

Principles: Human Behaviour

By domain *human behaviour* we shall understand

- any of a quality spectrum of carrying out assigned work:
  - ⋆ from *careful, diligent* and *accurate,*

  via

  - ⋆ *sloppy* dispatch, and
  - ⋆ *delinquent* work,

  to

  - ⋆ outright *criminal* pursuit

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

- In describing a domain it is important to try capture salient features of what it means to be a human worker:
  - ⋆ being *careful, diligent* and *accurate,*
  - ⋆ being unintentionally *sloppy,*
  - ⋆ being intentionally *delinquent,*
  - ⋆ being outright *criminal*

  and, if describable, any shade in-between.
- How
  - ⋆ one describes that,
  - ⋆ and how one, i.e., the software developer, utilises such descriptions
- are covered in more detail later in this lecture.

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

Banking — or Programming — Staff Behaviour

- Let us assume a bank clerk, "in ye olde" days, when calculating, say mortgage repayments:
  - ⋆ We would characterise such a clerk as being *diligent,* etc., if that person carefully follows the mortgage calculation rules, and checks and double-checks that calculations "tally up", or lets others do so.
  - ⋆ We would characterise a clerk as being *sloppy* if that person occasionally forgets the checks alluded to above.

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

  - ⋆ We would characterise a clerk as being *delinquent* if that person systematically forgets these checks.
  - ⋆ And we would call such a person a *criminal* if that person intentionally miscalculates in such a way that the bank (and/or the mortgage client) is cheated out of funds which, instead, may be diverted to the cheater.

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

- Let us, instead of a bank clerk, assume a software programmer charged with implementing an automatic routine for effecting mortgage repayments:
  - ⋆ We would characterise the programmer as being *diligent* if that person carefully follows the mortgage calculation rules, and throughout the development verifies and tests that the calculations are correct with respect to the rules.
  - ⋆ We would characterise the programmer as being *sloppy* if that person forgets certain checks and tests when otherwise correcting the computing program under development.
  - ⋆ We would characterise the programmer as being *delinquent* if that person systematically forgets these checks and tests.
  - ⋆ And we would characterise the programmer as being a *criminal* if that person intentionally provides a program which miscalculates the mortgage interest, etc., in such a way that the bank (and/or the mortgage client) is cheated out of funds.

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

Shopping — Overall Consumer Behaviour

- A consumers goods market consists of
  - ⋆ consumers, retailers, wholesalers, producers and delivery services.
- We focus just on possible consumer behaviours:
  - ⋆ (i) a consumer inquires, with a retailer, as to availability, price, and delivery terms, of some merchandise.
  - ⋆ (ii) The retailer responds with zero, one or more offers.
  - ⋆ (iii) The consumer may decide to ignore the offers, or the consumer may select one of the offers, or the consumer may order something that was not in the set of offers.

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

- ⋆ (iv) The retailer may confirm an order, whereupon delivery takes place and an invoice is sent.
- ⋆ (v) The consumer may decide to return the merchandise unpaid, or even paid!
- ⋆ (vi) Or the consumer may keep the merchandise and may ignore the invoice, or may pay it, or may pay some other "fictive" (i.e., nonexisting) invoice.
- ⋆ (vii) The consumer may then decide to return the merchandise for repair or for claims.

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

Shopping — Overall Consumer Behaviour

```
type
  Σ
  Choice == inq | ord | acc | ret | pay | cla | ign
  CR == Inq(..)|Ord(..)|Acc(..)|Pay(..)|Cla(..)|Ign(..)
  RC == Ofr(..)|Del(..)|Inv(..)|..
channel
  cr:CR, rc:RC
```


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

```
value
  consumer: Σ → out cr in rc  Unit
  consumer(σ) ≡
c0  (let cho == inq⌈⌉ord⌈⌉acc⌈⌉ret⌈⌉pay⌈⌉cla⌈⌉ign in
c1   let σ′ =
c2     case cho of
c3       inq → let (σ″,i) = .. in cr!i ; σ″ end
c4       ord → let order = .. in cr!order end
c5       acc → if .. then let (σ″,a) .. in cr!a ; σ″ end else σ end
c6       ret → if .. then let (σ″,r) = .. in cr!r ; σ″ end else σ end
c7       pay → if .. then let (σ″,p) = .. in cr!c ; σ″ end else σ end
c8       cla → if .. then let (σ″,c) = .. in cr!c ; σ″ end else σ end
c9       ign → σ
c10    end
c11  consumer(σ′) end end)
```


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

```
     ⌈⌉
s1  (let res = rc ? in
s2   let σ′ =
s3     case res of
s4       Ofr(..) → handle_ofr(res)(σ),
s5       Del(..) → handle_del(res)(σ),
s6       Inv(..) → handle_inv(inv)(σ),
s7       .. → ..
s8     end in
s9  consumer(σ′) end end)
```

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

- We narrate in detail the informal points (i–vii) above.
- The consumer function has two internally nondeterministically chosen alternatives.
  - ⋆ Either the initiative is on the side of the consumer (i.e., 'client' mode, shown using "c" prefixed line labels);
  - ⋆ or the consumer "passively" awaits response from the retailer (i.e., 'server' mode, shown using "s" prefixed line labels).

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

- (c) As a client the consumer nondeterministically internally, i.e., of her own free will, chooses between doing any of the actions
  - ⋆ (c3) inquire about merchandise,
  - ⋆ (c4) order merchandise ,
  - ⋆ (c5) accept delivery of merchandise believed to have been delivered ,
  - ⋆ (c6) return merchandise believed to have been delivered,
  - ⋆ (c7) pay for merchandise believed to have been delivered,
  - ⋆ (c8) claim refund on supposedly faulty merchandise believed to have been delivered, or
  - ⋆ (c9) ignore whatever goes on!
- Any of these actions (the last is, in effect, a nonaction) does, indeed, leave a side effect, a remembrance, in the mind of the consumer, hence a state change, from *state* to *state′* ((c1)).

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

- (s) As a server the consumer
  - ⋆ awaits a response from the retailer.
  - ⋆ If none is forthcoming, the consumer "deadlocks"!
  - ⋆ If a response is forthcoming, it is either
    - ◇ (s4) an offer, possibly prompted by an earlier consumer inquiry — but not necessarily. It could be an "own initiative" by the retailer, or
    - ◇ (s5) a delivery (etc.),
    - ◇ (s6) an invoice (etc.),
    - ◇ (s7) or other!
  - ⋆ In any case, a new state (s2) results.
- The consumer resumes being a consumer in a new state resulting from either her own initiatives, or from externally prompted actions (c11), resp. (s9).

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

- In the above example we are deliberately leaving many things unspecified (..).
- The point is that we are not so much interested — in this section — in those (..) things.
- We are interested in modelling, in describing, the vagaries of consumers.
- These uncertainties, these unpredictable wanderings, were fully described by the nondeterministic choice
- and by the fact that after the outputs (!) the consumer "recursed" being a consumer without awaiting responses from the retailer.
- It was also shown in our not defining, yet, the *handle_xyz(..)* clauses.

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

Shopping — Detailed Consumer Behaviour

- We left some open points in the earlier example.
- We shall use these to illustrate other aspects of human behaviour, its informal and formal descriptions.
- We start by singling out the treatment of a consumer-initiated initiative, like making an inquiry (c3).

c3 $\quad$ inq $\rightarrow$ **let** $(\sigma''$,i$)$ = .. **in** cr!i ; σ'' **end**

- To (c3) we add the "missing" information about how we form (i.e., "compute") the information (i.e., data) that goes into an inquiry.

c3 $\quad$ inq $\rightarrow$ **let** $(\sigma''$,i$)$ = mki(σ) **in** cr!i ; σ'' **end**
mki: $\Sigma \rightarrow$ Inq Σ

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

- In the formula above we have referred to the action of human "gathering" the information that goes into an inquiry by the cryptic function name *mki*.
- To *make* an *i*nquiry we assume that the consumer refers to whatever sense impressions that person may have, and we model that ("whatever sense impressions that person may have") as part of that person's state.
- Hence the gathering action operates on the state and updates it with the fact that the person (whose state it is) has contemplated and formed an inquiry.
- We leave the description of *mki* open.
- Leaving it open also leaves it open to interpretation.
- Anything is allowed that forms an inquiry and possibly changes the state.
- This "openness" models the vagaries of human behaviour.
- The case for all other consumer-initiated actions directed at the retailer is similar to that of the inquiry action in respect of acting upon and communicating information.

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

- We now treat the case of retailer-initiated interactions.
- Let us consider the consumer's reaction to a retailer offer response.

s4 $\quad$ Ofr(..) $\rightarrow$ handle_ofr(res)(σ)

- We refer to this reaction by *handle_ofr*.
- As for the making of an inquiry (etc.), this action is not being further described, other than saying:
  - ⋆ It is any action that somehow records,
  - ⋆ in the consumer's state, i.e., mind, or jotted down on a piece of paper,
  - ⋆ say stuck to a kitchen notice board,
  - ⋆ the fact that approximately "such and such" an offer was received.

value
handle_ofr: Ofr $\rightarrow \Sigma \rightarrow \Sigma$

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

- No further action is described.
- In particular, the perhaps expected reaction of the consumer "immediately firing off" an order, or a declination of the offer is not described.
- Any such possible reaction is modelled by the
  - ⋆ internal nondeterministic choices of the
  - ⋆ client actions of the consumer:
  - ⋆ The consumer may, sooner or later or even never
  - ⋆ select or choose an order reply.
  - ⋆ And that order reply may relate, "through" the *mko* action (c4, not shown),
  - ⋆ to the *Of fer response* (s4).

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

Methodological Consequences

- Commensurate with the above, humans interpret rules and regulations differently,
- and not always "consistently" — in the sense of repeatedly applying the same interpretations.

type
  Action = $\Theta \xrightarrow{\sim} \Theta$-**infset**
value
  hum_int: Rule → Θ → RUL-**infset**
  action: Stimulus → Θ → Θ
  hum_beha: Stimulus × Rules → Action → $\Theta \xrightarrow{\sim} \Theta$-**infset**
  hum_beha(sy_sti,sy_rul)(α)(θ) **as** θset
    post
      θset $= \alpha(\theta) \wedge$ action(sy_sti)(θ) $\in \theta$set
      $\wedge\ \forall\ \theta'$:Θ•$\theta' \in \theta$set $\Rightarrow \exists$ se_rul:RUL•se_rul $\in$ hum_int(sy_rul)(θ)$\Rightarrow$se_rul(θ,θ')

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

- The above is, necessarily, sketchy:
  - ⋆ There is a possibly infinite variety of ways of interpreting some rules.
  - ⋆ A human, in carrying out an action, interprets applicable rules and chooses one which that person believes suits some (professional, sloppy, delinquent or criminal) intent.
  - ⋆ "Suits" means that it satisfies the intent,
    - ◇ i.e., yields **true** on the pre/post-configuration pair,
    - ◇ when the action is performed —
    - ◇ whether as intended by the ones who issued the rules and regulations or not.
  - ⋆ We do not cover the case of whether an appropriate regulation is applied or not

Tel.: +81-761-51-1275, Fax: +81-761-51-1149 | E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner
© Dines Bjørner, 2006

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

- The above-stated axioms express how it is in the domain,
- not how we would like it to be.
- For that we have to establish requirements.
- This is the subject of late lectures.

Tel.: +81-761-51-1275, Fax: +81-761-51-1149 | E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner
© Dines Bjørner, 2006

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

Human Behaviour and Knowledge Engineering

- Domain engineering aims at making precise our understanding of the entities, functions, events and behaviours of the observable phenomena and the intellectual concepts of the domain.
- By *knowledge* we shall, in the narrow context of knowledge engineering, understand that which a human (or a machine, i.e., an agent) knows or believes or assumes or commits with respect to (*knowledge, beliefs, promises* or *commitments* of) another agent.
- By *knowledge engineering* we shall understand the formulation (whether informal or formal) of such knowledge.

Tel.: +81-761-51-1275, Fax: +81-761-51-1149 | E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner
© Dines Bjørner, 2006

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

- Knowledge engineering is thus concerned with understanding relations between two or more agents' knowledge (etcetera) about one another with respect to the following issues:
  - ⋆ what does an agent know about what another agent knows or believes;
  - ⋆ which (things) does an agent promise another agent who may then commit or promise other or similar things to yet other agents;
  - ⋆ and so on.
- The subject of knowledge engineering is of importance when we model human behaviour
- but we shall not in this book venture into this very important field of computer and computing science.

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

Discussion

- Please observe the difference between the version of *meaning* under the rules and regulations facet, and the present version.
  - ⋆ The former reflected the semantics as intended by the stakeholder who issued the rules and regulations.
  - ⋆ The latter reflects the professional or the sloppy or the delinquent or the criminal semantics as intended by the similarly "qualified" staff which carries out the rule-abiding or rule-violating actions.
- Please also observe that we do not here exemplify any regulations.

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

Reminder

We remind the reader of the principle stated at the outset of this lecture on domain human behaviour:

When describing a domain,

- analyse it with respect to its human behaviour phenomena and concepts.
- Focus on possibly describing these separately.
- Make sure that descriptions of other described domain facets are commensurate with possibly multiple, alternative descriptions of domain human behaviours

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

Lecture Summary

Overview

- It's been a long lecture.
- First a long example: Documents and we rushed through that!
- Then Business Processes.
- And finally Domain Facets:
  - ⋆ Intrinsics
  - ⋆ Support Technologies
  - ⋆ Management & Organisation
  - ⋆ Rules & Regulations
  - ⋆ (Scripts — whic we skipped)
  - ⋆ Human Behaviour
- There may be other facets.

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

Four Axes of Description

- Four kinds of descriptive features have to be woven together:
  - ⋆ Entities, Functions, Events, Bahviours
  - ⋆ Designations, Definitions, Refutable Assertions
  - ⋆ Business Processes
  - ⋆ Intrinsics, Support Technologies, Management & Organisation, Rules & Regulations, Scripts, Human Behaviour

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

Topic 4

A Glimpse of Requirements Engineering

A Fifth Example: Good Governance

4, A Glimpse of Requirements Engineering

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

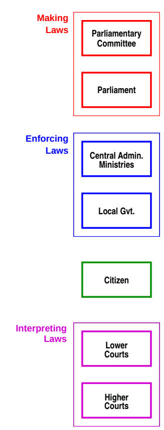
Closing

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

Example Public Government & Documents

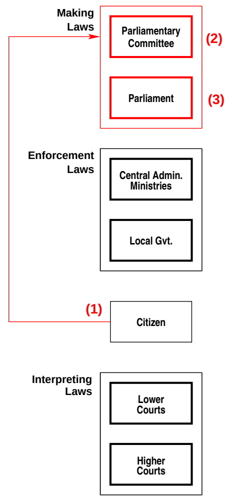
An Informal View of Public Government

- Public government, in this seminar, consists of
  - ⋆ the **lawmakers:** Parliament
  - ⋆ the **law enforcers:** Central and local government
  - ⋆ and the **law interpreters:** Judiciary system
- **Citizens** interact with all three branches of government.



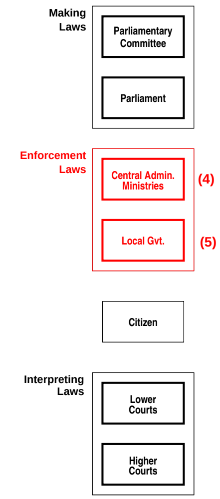
Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292
DTU

1. Citizens through the process of debate provoke their parliament to discuss societal problems.
2. A parliament committee discusses a specific societal problem.
3. Their deliberations are "sent" as a law proposal to parliamment which debates the issue and passes some law.



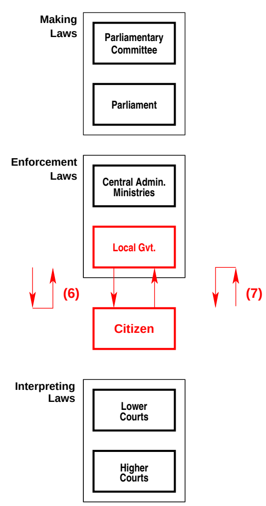
Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292
DTU

4. The law is passed on to an appropriate ministry (of the central government) and that ministry formulates basic rules & regulations for how local governments shall administrate uses of the law.
5. The local governments makes provisions for handling the law locally.



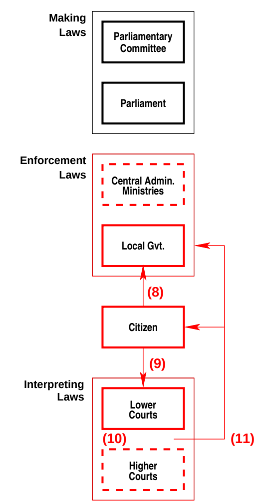
Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292
DTU

6. The citizen is either
   - contacted by the local government
   - and asked to report on some issue (tax, traffic violation, or other),
   - and the citizen replies.
7. or the citizen
   - contacts the local government
   - in order to apply for something (passport, pension benefits, ot other)
   - And the local government replies.



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

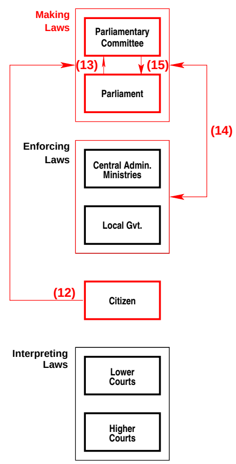
8. The citizen is either accepts the dicision of local government,
9. or the citizen
   - does not accept the dicision,
   - and complains to the courts.
10. The "due process of law" takes place.
11. Eventually the judiciary system hands down a decision
   - either in favour of the citizen,
   - or in favour of the governement,
   - or both!



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

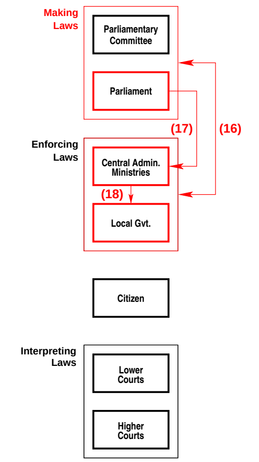
Flow of Documents in Public Administration

12. Citizens may direct a problem petition to parliament — in the form of a document signed by many citizens.
13. Parliament decides to "do something" (or not to do anything) about the problem. A response document is produced.
14. A designated parliament committee requests an appropriate ministry to prepare some "background" document.
15. The parliament committee passes discussion and a law proposal documents to parliament.



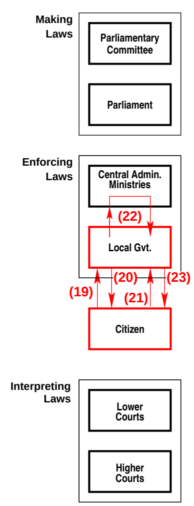
Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

16. Parliament requests further "background" documents from the central administration, and receives these.
17. Parliament debates the law proposal and passes a law, which, as a document is sent to the appropriate ministry for further handling — and otherwise published in the law gazette.
18. The ministry and its departments, i.e., the central administration, formulates procedures for the enforcement of the law and sends these, as documents to local administrations.



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

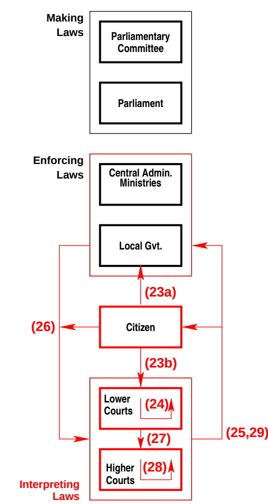
19. A citizen applies for some permission, that is, an application document is sent to a local administration — or a citizen breaks the law (symbolised with the virtual arrow from citizen to a local authority).
20. The local administration sends a receipt (a citation) document, possibly forwards further documents to be filled in, and gives a conditional date by which a decision can be expected.
21. The citizen sends in the possibly further requested documents.
22. The local administration communicates various documents related to the case to/from other public government offices.
23. And finally the citizen receives a response document.



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

23. The citizen
    (a) either sends an acceptance document to the local administration,
    (b) or rejects it, informing the local administration of this, and directs a complaint at the law courts.
24. The first instance law court deliberates (i.e., documents are produced),
25. a decision is sent to the citizen and the local admin.,
26. Either the local administration or the citizen both accepts the decision and further actions are curtailed, or at least one of them appeals the decision.
27. Lower court decision documents are passed on to a higher court.

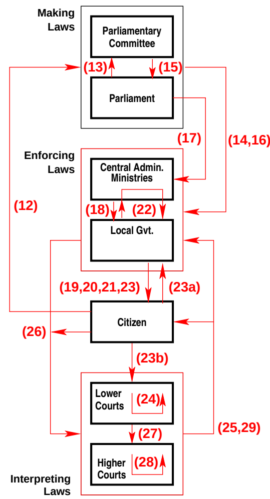
28.–29. And steps (24–25) are repeated till a final decision is passed.



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

Summary of Documents

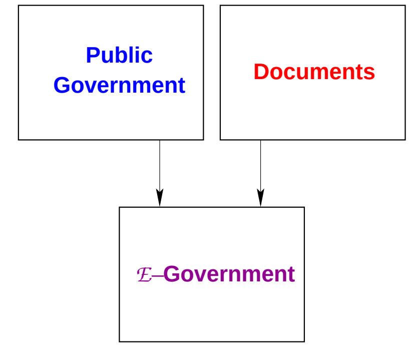
12. Citizen petition
13. Parliament response
14. Background briefing
15. Subcommittee discussion and law proposal
16. Further background briefing
17. Law and record of paliament debate
18. Handling procedures and forms
19. Citizen application (or "breakin law event")
20. Local authority reply (or citation)
21. Citizen response to local authority reply
22. Public admin. docs. handling citizen request or infringement
23. "Final" local authority reply/decision
    (a) Citizen acceptance or rejection
    (b) Citizen lawsuit
24. Lower law court handling
25. Lower law court decision
26. Citizen and public administration reaction
27. Transfer of lower law court dcosuments
28. Higher law court handling
29. Higher law court decision (final, final)



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

Documents — A Closer Analysis

- We present a "story" of documents that is a bit different from what you may be used to.
- The reason is that we are building up, towards the end of this seminar, to a "story" on computers, communication and documents.
- Our "story" on documents is also "completely" independent of our previous "narration" of public government.
- Again there is a reason: towards the end of this seminar we merge the "story" on documents with the "narration" of public government into the subject of $\mathcal{E}$-Government.



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

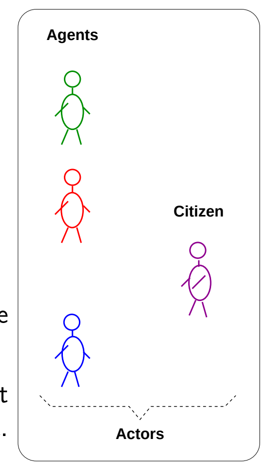
Overview of Document Issues

- **Document Operations:**
  Documents are created, are edited, and can be read, copied, moved, can be the basis for searchees and calculations, and can be shredded — by actors.
- **Document Authorisation:**
  Actors have varying degrees of creation, editing, reading, copying, distribution and shredding authority.
- **Document History:**
  Document may reveal their creation, editing, reading, copying distribution, search & calculation history — who did what, when, where!
- **Document Licensing:**
  Unauthorised actors must be prevented from performing designated operations on documents. We achieve this indirectly by introducing and enforcing a regime of licensing based on authorisation.

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

Actors: Citizens and Agents

- Document operations are performed by **actors**.
- **Actors** are either **agents** or **citizens**,
- An **agent** is
  - ⋆ either a person working for a branch of public government,
  - ⋆ or is that branch of public government.
- Of course **citizens** may be agents in some other context,
- that is, a **citizen** is a person interacting, not as an agent, with agents of public government.

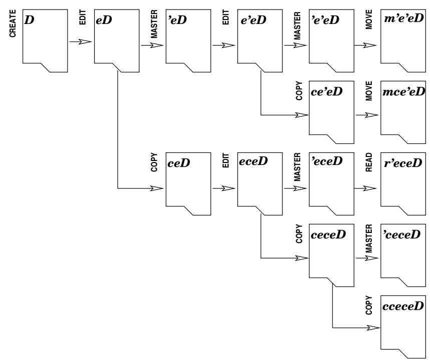


Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

Document Operations

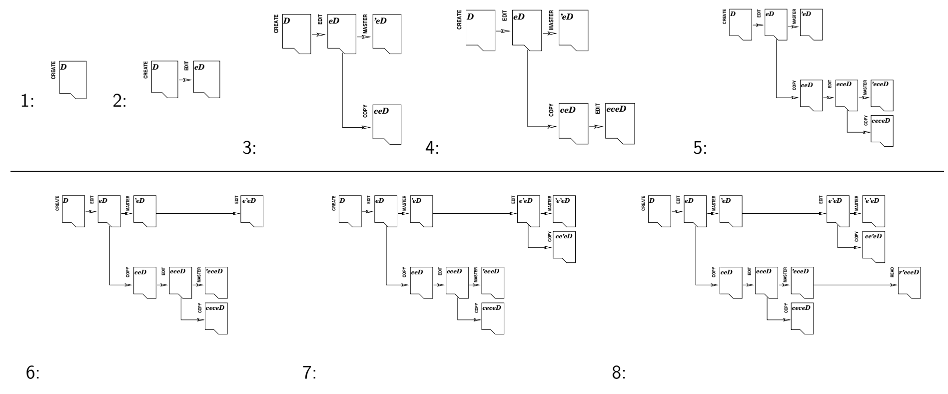
- Document operations are performed by **actors**.

30. Documents can be **created**.
31. Documents can be **edited**.
32. Documents can be **read**!
33. Documents can be **copied**.
34. Documents can be **moved**.
35. Documents can be **shredded** (not shown).



- An **actor** can at most be performing one operation at a time.
- Documents are "marked" by the **time** and **location** of the operation and by the identity of the performing **actors**.
- Together the **time, location** and **actor identity** forms a **unique document identification**.

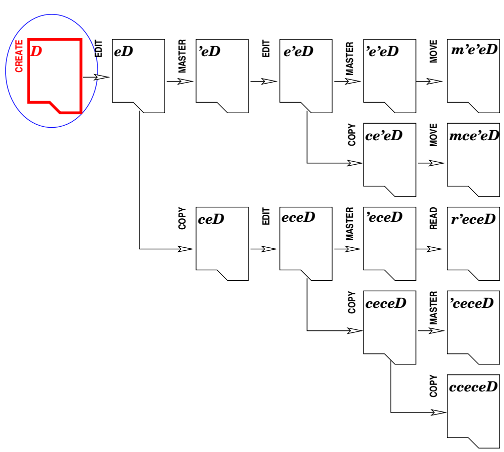
Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292



- A sequence of document operations:
- 1:create, 2:edit, 3:copy, 4:edit, 5:copy, 6:edit, 7:copy, 8:read

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

30. Documents can be **created**.

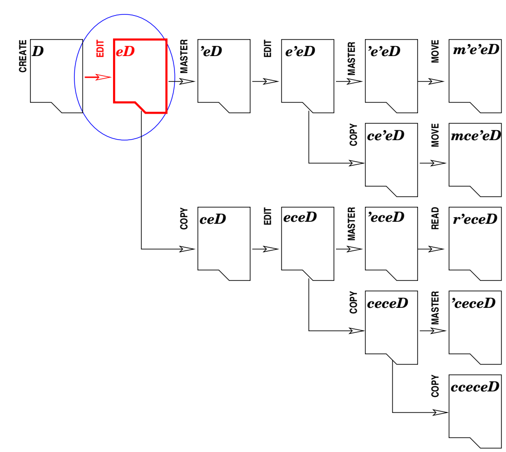


- Created documents contain no substantial information
- other than administrative information about
  - ⋆ time and
  - ⋆ location of creation,
  - ⋆ identity of actor who created the document.

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

31. Documents can be **edited**.

- Edited documents are **versions** of the document on the basis of which they were edited.
- Edited documents contain substantial information.
- One can read documents while editing them!
- One cannot copy, move or shred documents during editing.
- An edited document is different from the document input.
- The difference amounts to the changed text, time and location of edit, and identity of editing actor.

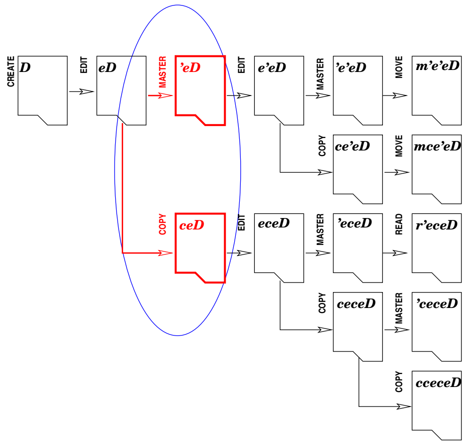


Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

32. Documents can be **copied**.

- As a result the **master** "goes on" to exist
- and a copied, **"the copy"**, document is constructed.
- One cannot edit, move, read or shred the master or the copy documents while copying.
- The location and time of copying is the same for both master and copy.

To **audially communicate**, i.e., to **tell** (speak about) a document (content) to other listeners is the same as **copy**ing it.

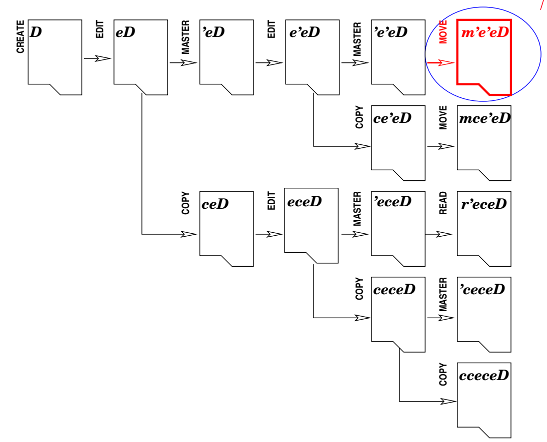


Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

33. Documents can be **moved**.

- They are physically moved from one **agent (location)** to another distinct **agent (location)**.
- The document "is almost" the same before start and after end of move, only location has changed.
- Documents cannot be copied, edited, read or shredded while being moved.

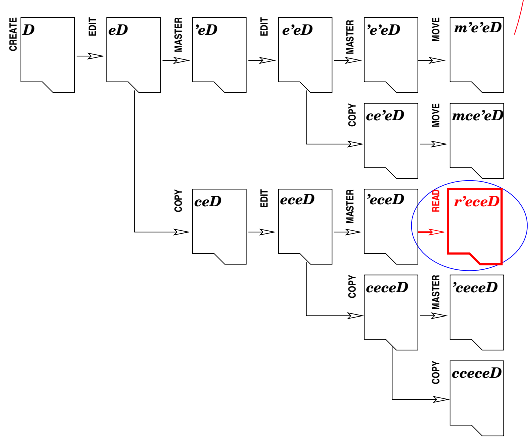
Instead of **moved** we shall sometimes use the term **distributed**.



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

34. Documents can be **read**!

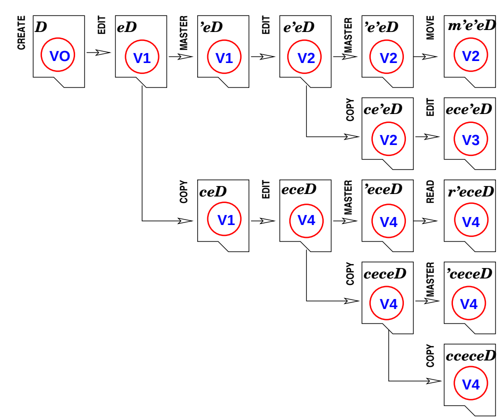
- One cannot edit, copy, move or shred document while only reading them.
- Reading leaves the document unchanged — except that it has now been read, at some time and at some location, by some actor.



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

Document Family and Document Versions

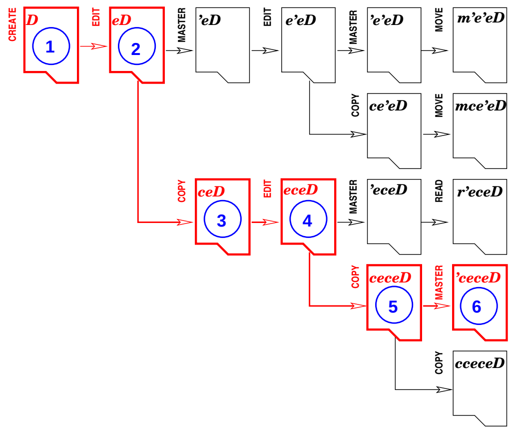
- **Document Family**
  - ⋆ The structure to the right designates one document family.
  - ⋆ Every create gives rise to a document family.
  - ⋆ It may grow (copying) and shrink (shredding).
- **Document Version**
  - ⋆ A "just" create document has version 0.
  - ⋆ Every edit of a document creates a new version of that "same" document.
  - ⋆ All other operations leave the version attribute unchanged.
- (Let us not be bothered by how version numbers are generated!)



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

Document History

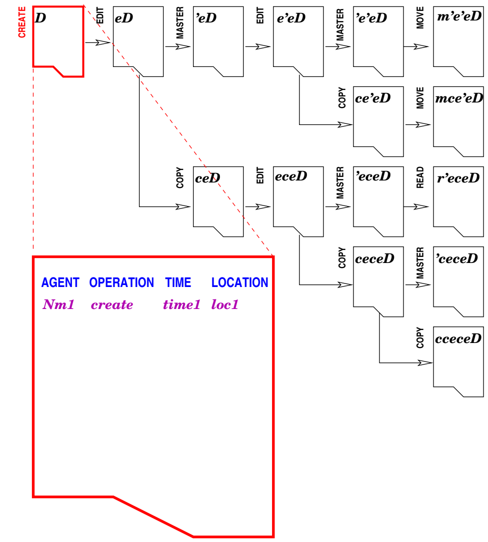
- From a document we can, "in theory", **trace its unique past**.
- In reverse order of operations:
  - **6** Take the lower right MASTER.
  - **5** It was most recently the BASIS for a **copy**ing.
  - **4** Before that it was the BASIS for an earlier **copy**ing.
  - **3** Before that it was the RESULT of a **copy**ing.
  - **2** Before that it was an **edit**ed version
  - **1** of a **create**d document.



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

1 Create

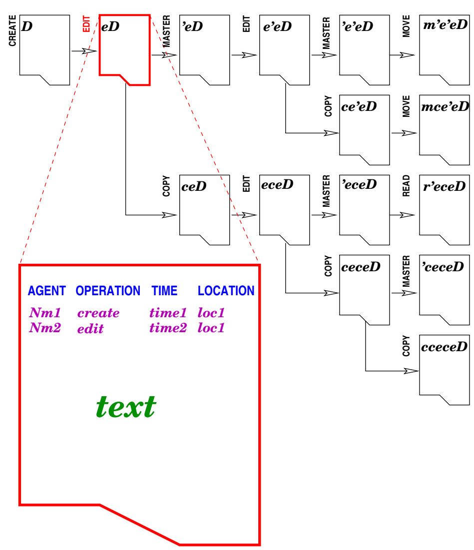
- An actor named **Nm1**
- performs operation **create**
- at time **time1**
- on location **loc1**.
- A document is created with just about the only information you see in the lower left corner to the right:



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

2 Edit

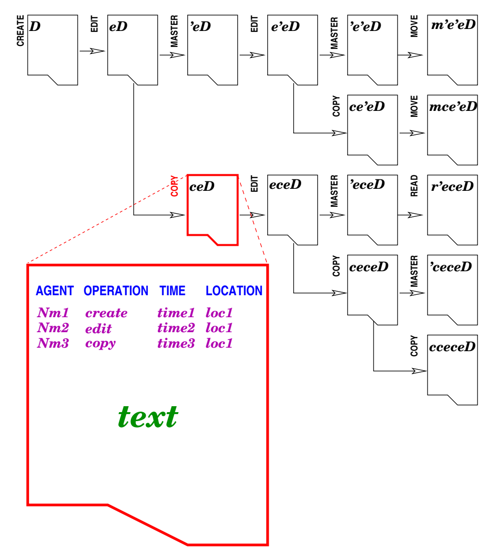
- An actor named **Nm2**
- performs operation **edit**
- at time **time2**
- on location **loc1**
- Document *D* is extended with text **text** into document *eD*.



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

3 Copy

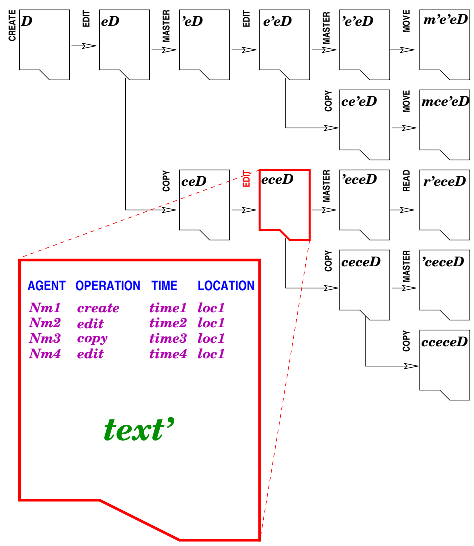
- An actor named **Nm3**
- performs operation **copy** (on *eD* and we focus on the 'copy')
- at time **time3**
- on location **loc1**.
- Document *eD* text **text** remains unchanged but is referred to as *ceD*.



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

4 Edit

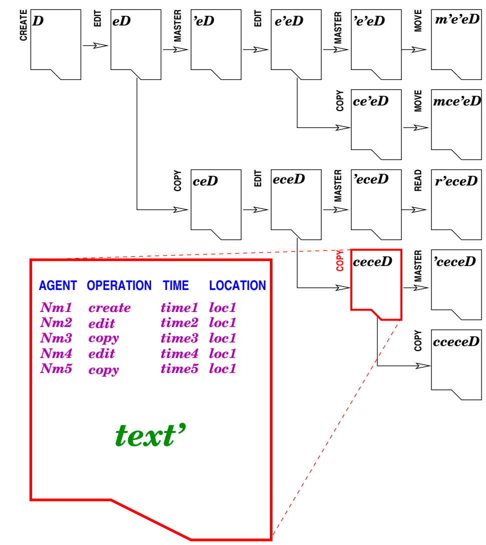
- An actor named **Nm4**
- performs operation **edit**
- at time **time4**
- on location **loc1**.
- Document *ceD* text **text** is changed into document *eceD* **text'**.



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

5 Copy

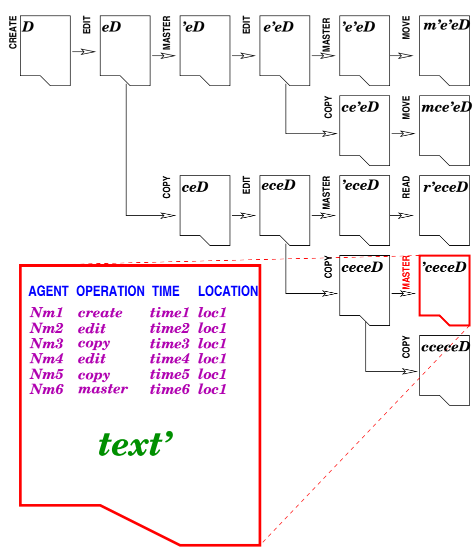
- An actor named **Nm5**
- performs operation **copy** (on *eceD* and we focus on the 'copy' *ceceD*)
- at time **time5**
- on location **loc1**.
- Document *ceceD* text **text'** remains unchanged.



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

6 Master

- An actor named **Nm6**
- performs operation **copy** (on *ceceD* and we focus on the 'master' *'ceceD*)
- at time **time6**
- on location **loc1**
- Document *'ceceD* text **text'** remains unchanged.



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

Document Authorisation

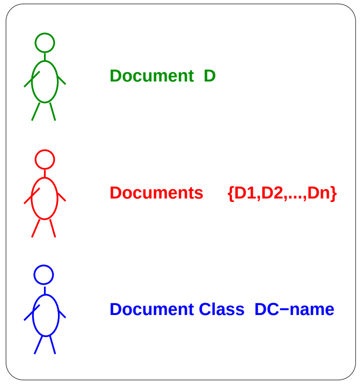
Rationale for Authorisation

- We explain the need for introducing a concept that we shall call 'authorisation'.
  - ⋆ Some documents may contain information that not all **actor**s should be aware off.
  - ⋆ For an **actor** to be allowed to perform an operation
    - ◇ upon (create or edit or copy or read or move or shred) a document
    - ◇ that **actor** must be so authorised (by some **agent**).
  - ⋆ **Authorisation** can be in the orm of a **license**, a **permit**, to perform an **operation** on some entity, as here, a **document**.

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

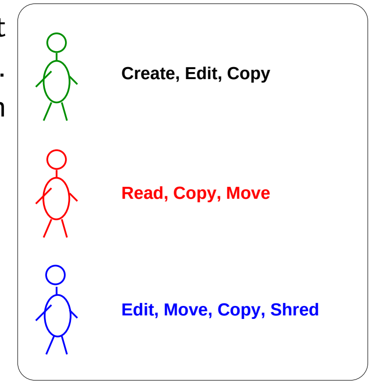
Authorisation of Actors

- Actors can be authorised with respect to (wrt.)
  - ⋆ one specific document whose identity will then be given, or wrt.
  - ⋆ a finite, identified set of documents, or wrt.
  - ⋆ a potentially indefinite class of documents, so we have to introduce a notion of a document class.
  - ⋆ (An example class of documents could be the class of all social security application forms [based on same template]. More on this later.)



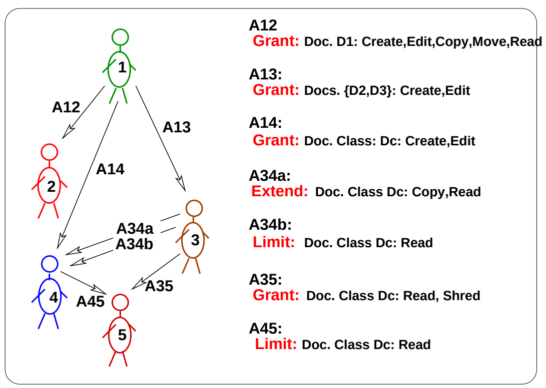
Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

- Actors can, within the designated set of such documents, be authorised wrt. which operations can be performed on these documents:
  - ⋆ **create,**
  - ⋆ **edit,**
  - ⋆ **copy,**
  - ⋆ **search,**
  - ⋆ **move,**
  - ⋆ **read,**
  - ⋆ **shred and**
  - ⋆ **calculate.**



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

- Actors may be authorised to
  - ⋆ **grant** document handling authorisations to (other) actors,
  - ⋆ **extend** or **limit** previously (by others or by that same actor) granted such document handling authorisations, or
  - ⋆ outright **withdraw** such document handling authorisations altogether.



Granting, Extending and Limiting Licences

The problem of how to initialise the system of document handling authorisations is an interesting one — which we may have time to come back to later.

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

License Scripts

- A license script is a named text which is issued by one actor to another.
- The license specifies
  - ⋆ a grant,
  - ⋆ an extension,
  - ⋆ a limitation or
  - ⋆ a withdrawal
  - ⋆ of specified document operations
  - ⋆ on specified (licensed) documents.
- A license can also grant permission to issue further licenses.
- We give the grammar of a license script language <LSL>:

• License Language, A Grammar

<LSL> ::= <License>-set
<License> ::= <Grant> | <Extend> | <Limit> | <Withdraw> | <Grant>
<Grant> ::= <License_name: **actor** <Actor_name>
    grants operations <Operations>
    to actor <Actor_name>
    on documents <Documents>
<Extend> ::= **actor** <Actor_name>
    extend license <License_name>
    of actor <Actor_name>
    with operations <Operations>
<Limit> ::= **actor** <Actor_name>
    limit license <License_name>
    of actor <Actor_name>
    with operations <Operations>
<Withdraw> ::= **actor** <Actor_name>
    withdraw license <License_name>
    from actor <Actor_name>

<Grant> ::= **actor** <Actor_name>
    { **grants licensing right** <License>
    to actor <Actor_name> |
  /* or */ |
    withdraw license <License_name>
    from actor <Actor_name> }

<Actor_name> ::= [**not**] <Identifier>**-set** | **all**
<Operations> ::= [**not**] <Op_name> **-set**| **all**
<License_name> ::= /* some identifier */
<Documents> ::= **class** <Doc_Class_name> | <Doc_name>**-set**

• Example Licenses

ln1: **actor** a1 **grants operations** {op1,op2,...,opn}
    to actor a2 **on documents** {d1,d2,...,dm}

actor a3 **extend license** ln2 **of actor** a4 **with operations** {op$'$,op$''$,...,op$'''$}

actor a5 **limit license** ln3 **of actor** a6 **with operations** {op$a$,op$b$,...,op$w$}

actor a7 **withdraw license** ln4 **from actor** a8

actor a9 **grants licensing right**
    ln5: **actor** a10 **grants operations** {opx,opy,...,opz}
        to actor a11 **on documents** {da,db,...,dc}

actor a12 **withdraw license** ln6 **from actor** a13

Special Edit Operations

- We have hinted at only a very rudimentary **edit** operation.
  - ⋆ One that takes only one document and
  - ⋆ basically adds, modifies or deletes **text**.
- More general, in fact a whole family of **edit** operations are present in everyday handling of documents:
  - ⋆ **merge** of two documents into
    - ◇ a third, implying a **copy**ing and a **create** operation.
    - ◇ into one of the two documents, implying a **copy**ing and a simple **edit** operation.
  - ⋆ **split** of one document into two documents implying a copying and two **create** operations.
  - ⋆ *Etcetera*

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

A Document Class Concept

Examples

• General Public Administration Document Classes

Different branches of government work on and produce different classes of document:

- Parliamentary committees (PC)
  - ⋆ handle **societal background problem** documents and
  - ⋆ produce **committee discussion** and **law proposal** documents.

-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

• General Public Administration Document Classes — Continued

- Parliament (P)
  - ⋆ handles **committee discussion** and law proposal documents and
  - ⋆ produces **parliament discussion** and law documents.
- ...
- And law courts
  - ⋆ receive **law suit** documents,
  - ⋆ deliberate over **law court proceeding** documents and
  - ⋆ issue **verdicts** (i.e., documents).

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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 Public Administration Documents

• Taxation Document Classes

- A tax office
  - ⋆ issues **tax declaration template** documents and
  - ⋆ handles **tax declaration form**[12] documents.

• Traffic Police Documents

- A traffic police officer
  - ⋆ handles **traffic violation citation template** documents and
  - ⋆ issues **traffic violation citation forms** (i.e., documents).

-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
E-mail: bjorner@gmail.com; URL: http://www.jaist.ac.jp/~bjorner

[12] A form is a filled-in template document

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

• Budget and Account Documents

- An accountant
  - ⋆ handles **budget** documents,
  - ⋆ fills in **account template** and **account form** documents, and
  - ⋆ aggregates (calculate) over **account form** and **budget** documents to produce ...

+81-761-51-1275, Fax: +81-761-51-1149
© Dines Bjørner, 2006
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

Document Classes

• Generic Document Classes

- By the generic class of documents we understand a class of documents that is indeoendent of the specific application domain.
- We make the following generic classification:
  - ⋆ **General, unformatted, un-structured text documents.**
    Comment: No calculations can be done on such documents.
    Example: Any “spur-of-the-moment” note
  - ⋆ **Formatted, semi-structured text documents.**
    Comment: Trivial searches can be done over such documents.
    Example: Most public administration documents.
  - ⋆ **Speficially formatted, template-based document.**
    Comment: Non-trivial calculations can be done over such documents.
    Example: Most application and related documents.

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

• Document Classes

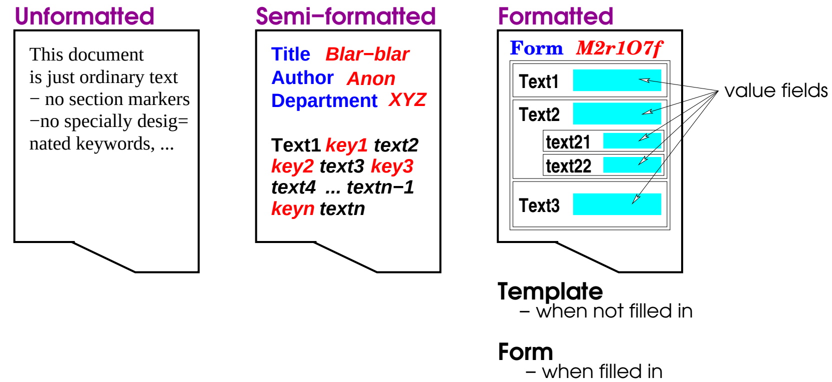


Figure 15.18: **Indication of Document Classes**

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

• Specific Government Document Classes

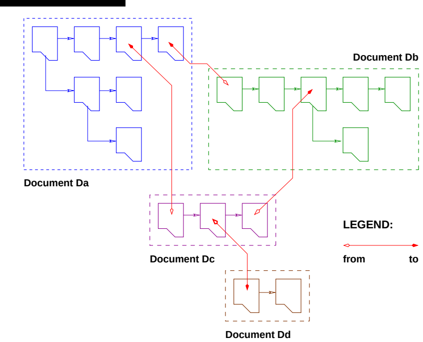
- For the application-specific category of public administration
  - ⋆ we suggest to let the class of government documents
  - ⋆ be determined by their relevance to specific laws or law proposals:[13]
- Some specific examples:
  - ⋆ Law proposal background doc.
  - ⋆ Law proposal discussion doc.
  - ⋆ Law.
  - ⋆ Law admin./handling doc.
  - ⋆ Law rules & reg. doc.
  - ⋆ Local admin. letter to citizen.
  - ⋆ Citizen reply to local admin. letter.
  - ⋆ Citizen complaint to law court.
  - ⋆ Law court inquiry doc.
  - ⋆ Law court decision.

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

Document [Cross–]References

- Documents
  - ⋆ in one family of documents
  - ⋆ may cross-refer to documents
  - ⋆ in another family of documents

  as shown to the right.
- Reasons seem obvious:
  - ⋆ chronologically “later” documents were
  - ⋆ derived in the context of knowledge of
  - ⋆ the chronologically “earlier” documents
  - ⋆ which can be made aware of the of the “later” uses.



Cross-references between documents of four document families

[13]— all other documents are simple administration documents found also in most other forms of administration.

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

• Examples of Document [Cross–]References

- Law proposal background doc. may refer to other laws.
- Law proposal discussion doc. may refer to background doc.
- Law usually refers to many other laws.
- Law admin./handling doc. usually refers to many other handling docs. and refers to the law.
- Law rules & reg. doc. refers to the law.
- Local admin. letter to citizen refers to the law.
- Citizen reply to local admin. letter refers to that letter.
- Citizen complaint to law court refers to local admin. letter and law.
- Law court inquiry doc. refers to citizen and local admin. letters and the law.
- Law court decision refers to the law and other law court decisions.

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

Document Calculations

- We can distinguish amongst different kinds of computations over documents.
  - ⋆ Document Identifier Searches:
    Example: Intra- and inter-document-family tracing.
  - ⋆ Attribute Searches:
    Example: Searches based on document attributes — incl. form numbers.
  - ⋆ Trivial Document “Syntactic Content” Searches:
    Example: Documents related to a specific agent or topic (a citizen, a law, or other). Searches look for text parts only.
  - ⋆ Non-trivial Document “Semantic Content” Searches:
    Example: Documents containing strongly formatted text parts, e.g., XML embedded and coded texts. Searches try to deduce meaning (“data mining”).
  - ⋆ Full-blown Calculations:
    Example: Tax calculations.

© Dines Bjørner, 2006

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

Summary of Document Attributes

These are the generic classes of document attributes.

- **document name**
- **document version number**
- **document classes**
  (generic and special)
- **history trace** of operations[a]
  (operation, location, time, actor)
- **reference to relevant license**

A unique document identifier can be calculated from the above.

[a] including calcuations

Doc. name:
Bjorner–e–macao
Doc. version:
version–number
Doc. class:
(gen–format,seminar)
Doc. history:
<(create,jaist,april30,db),
(edit,jaist,may2,db),
...
(edit,shanghai,may24,db),
(copy,macao,may31,lsc),
(read,macay,june1,...)>
License:
E–mail: Janowski–to–Bjørner

Document attributes

© Dines Bjørner, 2006

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

Actor Attributes

- **Unique Actor Identifier**
- **Actor Location**
- **Licenses**
  - ⋆ Current “Own” Licenses (i.e., work being pursued)
  - ⋆ Current Granted Licenses (i.e., work being managed)
- Which **Documents** (by reference)
  - ⋆ have be **Operated** upon
  - ⋆ at **Locations**
  - ⋆ and at **Times**

© Dines Bjørner, 2006

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

$\mathcal{E}^2\mathcal{G}$: $\mathcal{E}$ssential $\mathcal{E}$-$\mathcal{G}$overnment

- **Law**-based public administration handles, like any other public or private administration, "thousands" of kinds of "zillions" of documents.
- Of these we single out now, we focus only on those public government documents
  - ⋆ which are **based in law**,
  - ⋆ which ultimately **refer to laws**.
- That is we **do not** in the following consider such kinds of documents
  - ⋆ as procurement, (ordinary) budget, accounting, personnel, etc.
  - ⋆ documents whose handling is like in any other, not law-based administration, whether public or private.
- **Assumption**: **Paperless administration**!

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

The Meaning of $\mathcal{E}^2\mathcal{G}$

- So, by $\mathcal{E}$ssential $\mathcal{E}$-$\mathcal{G}$overnment we shall thus mean:
  - ⋆ Any electronic handling of documents, that is,
    - ◇ **planning,**
    - ◇ **preparation,**
    - ◇ **discussion,**
    - ◇ **communication,**
    - ◇ **decision,**
    - ◇ **etcetera**

    and which are based on and results in (possibly new, possibly edited) documents
  - ⋆ **such that these documents**
  - ⋆ **directly or indirectly**
  - ⋆ **refer to laws.**

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

From Domain to $\mathcal{E}^2\mathcal{G}$ Requirements

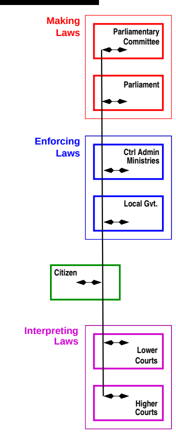
- To illustrate what "such electronic handling" might mean,
- we **systematically go through** the domain(s)
  - ⋆ of public government such as outlined in topic 1
  - ⋆ and of documents, such as outlined in topic 2
- in order to **decide** whether "such–and–such"
  - ⋆ agent (institution, i.e., branch of government) and citizen interactions,
  - ⋆ documents and document attributes,
  - ⋆ functionalities,
  - ⋆ "etcetera"
- **must** be **"made more–or–less electronic"**.

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

So Here We Go: Towards $\mathcal{E}^2\mathcal{G}$

• Which branches of government should be included in $\mathcal{E}^2\mathcal{G}$?

- One answer could be:
  - ⋆ All branches interfacing with citizens.
  - ⋆ The double–arrowed line indicates this.
  - ⋆ Within these branches we must list the relevant departments.
- Another answer could be: Only such and such a subset of the indicated branches. (We then omit some of the ↔s.)

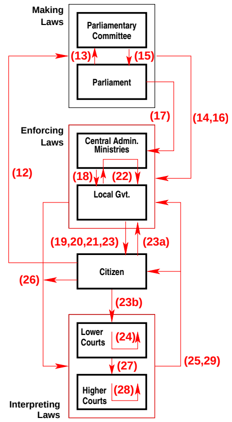


Japan Advanced Institute of Science & Technology
School of Information Sciences
1-1, Asahidai, Tatsunokuchi
Nomi, Ishikawa, Japan 923-1292

• Which document classes should be included in $\mathcal{E}^2\mathcal{G}$?

- One answer could be:
  - ⋆ All the (in this example) **18** (29-12+1) document classes implied by the **red** arrows in figure to the right.
  - ⋆ For each arrow-head we then list relevant document classes.
- Another answer could be: Only such and such a subset of the indicated document classes.

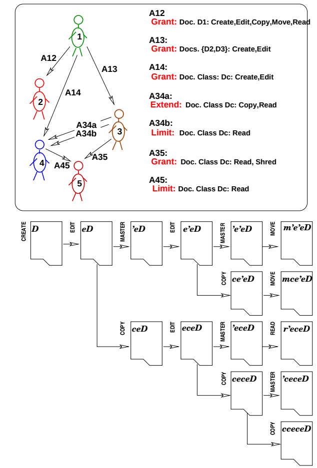
  (That is, we omit some of the → document classes.)



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

• Which authorisation on document classes should be $\mathcal{E}^2\mathcal{G}$ scripted?

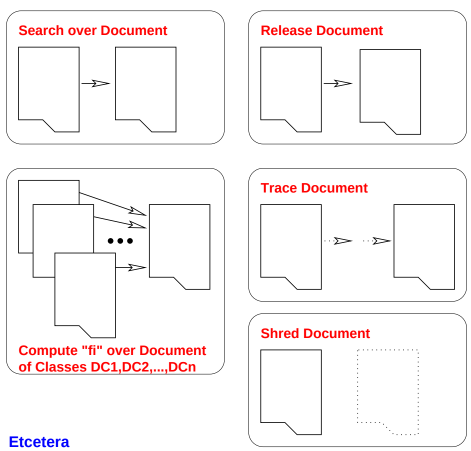
- For each selected document class
  - ⋆ scripts
  - ⋆ of zero, one or more authorisations need be designed
  - ⋆ and their instantiation wrt. specific documents
  - ⋆ must be computerised,
  - ⋆ as must the monitoring and control of the implied document family.



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

• Which new operations document classes should be $\mathcal{E}^2\mathcal{G}$ supported?

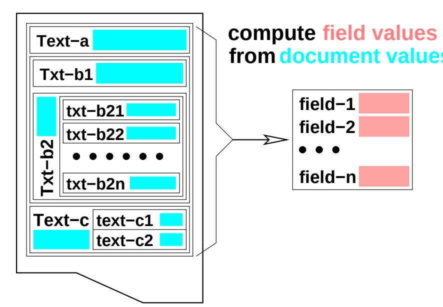
- For each selected document class
- as well as combinations of related document classes
- all conceivably $\mathcal{E}^2\mathcal{G}$ supported operations must be defined:
  - ⋆ All relevant **searches**.
  - ⋆ All relevant $n \geq 1$ **computations**.
  - ⋆ All **trace** functions.
  - ⋆ A new **release** operation.
  - ⋆ The **shred** operation.



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

• **More on $\mathcal{E}^2\mathcal{G}$ Document Computations (II)**

- One class of computations
  - ⋆ have the compuation be based on **values**
  - ⋆ of a possibly only partially **filled-in template** (= **form**).
  - ⋆ The computation would then yield, not necessarily a document, but
  - ⋆ new values that can serve as basis for further computations
  - ⋆ and possibly be fed to a repository of documents.
- Such computations
  - ⋆ presume design of templates (i.e., forms),
  - ⋆ and the implementation of the computations.

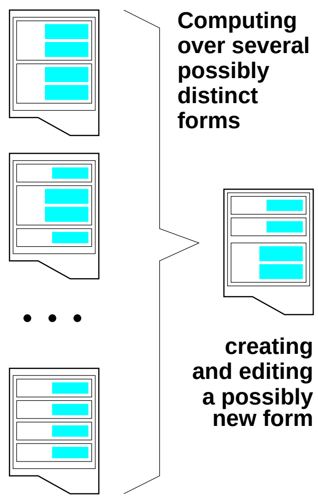


(Partially) Filled Template Form

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

• Yet More on $\mathcal{E}^2\mathcal{G}$ Document Computations (III)

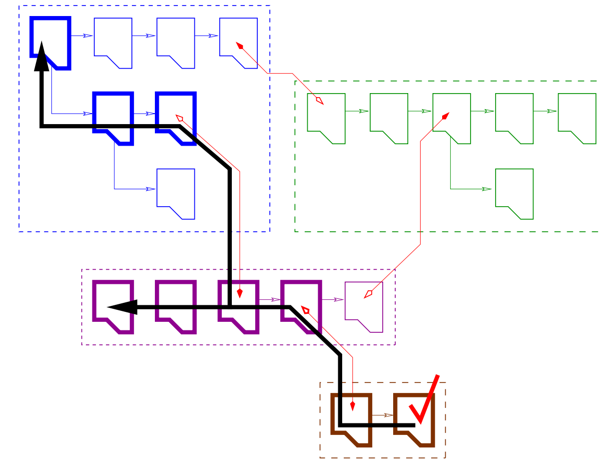
- Another class of computations
  - ⋆ collects data from several possibly distinct documents
  - ⋆ and produce an aggretated document.
- An example could be
  - ⋆ income and property tax returns
  - ⋆ of several tax payers
  - ⋆ aggregated into a community tax budget.
- The leftmost, i.e., the resulting document may be an edited (i.e., an update) version of one of the rightmost, i.e., input documents.



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

• Transparency Implies $\mathcal{E}^2\mathcal{G}$ Traceability

- Given a document,
  - ⋆ say the "bottom-right-most" $\surd$**-checked** document
  - ⋆ one may wish to trace all its "ancestor" documents.
  - ⋆ Such a trace may — as indicated — lead
  - ⋆ to several traces, that is,
  - ⋆ to sequences of document references.
- For an agent or a citizen such **traceability**
- implies **transparency** of public government.



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

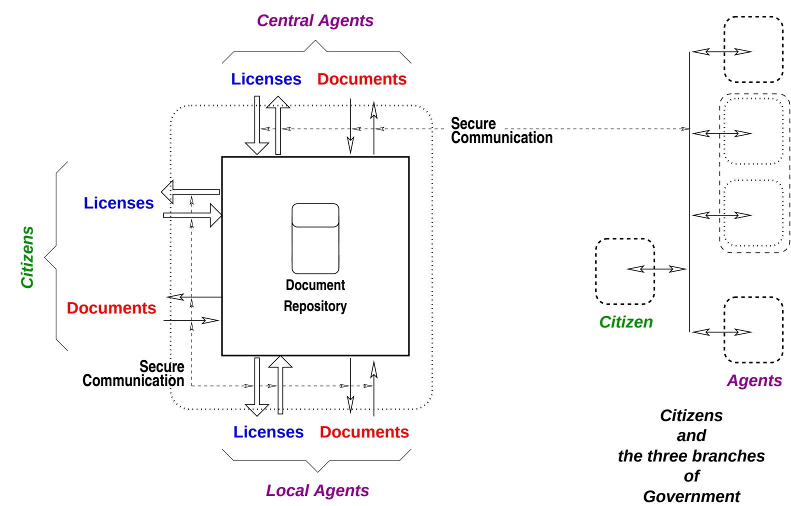
Summary of $\mathcal{E}^2\mathcal{G}$

First Summary

- So $\mathcal{E}$ssential $\mathcal{E}$-$\mathcal{G}$overnment, $\mathcal{E}^2\mathcal{G}$,
  - ⋆ assumes **paper-less** administration, i.e., all electronic documents and
  - ⋆ focuses of all/most such **document**-manifested actions
  - ⋆ which are **based in law**.
- Such documents entail:
  - ⋆ Which **branches** of public government are **included/excluded**?
  - ⋆ Which **document classes** are **included/excluded**?
  - ⋆ Which **authorisations**, and which **scripts** are **mandated**?
  - ⋆ Which **operations** on documents are **supported**?
  - ⋆ Which form of **traceability** is **supported**?

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

Second Summary of $\mathcal{E}^2\mathcal{G}$



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

End of Long Example

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

The Machine

Machine

- The machine is
  - ⋆ the software and
  - ⋆ the hardware

  to be procured and/or developed.

Environment = Domain

- What Michael Jackson calls the 'environment'
- we call the 'domain' (application domain).

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

Delineations

1. **Domain requirements**
   - are those requirements which can be expressed
   - by only using terms from the domain
     (and everyday, otherwise non-technical language).

   Domain requirements are thus "simply derived" from
   - the domain description
   - by reading it, together with requirements stakeholders
   - and, for basically each line of descripotion,
   - asking a number a number of questions and noting down the answers.

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

2. **Machine requirements**
   - are those requirements which can be expressed
   - by only using terms from the machine.

   Thus machine requirements, in essence, concerns
   - phenomena (and concepts)
   - **possessed only**
   - by the machine.

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

3. **Interface requirements**

- are those requirements which can be expressed
- by only using terms both from the domain and the machine.

Interface requirements thus concerns

- phenomena (and concepts) **shared** between
- the domain
- and the machine.

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

Domain Requirements

Domain Requirements Questions and Answers

- The questions are structured around the following domain-to-requirements operations:
  - ⋆ Projection
  - ⋆ Instantiation
  - ⋆ Determination
  - ⋆ Extension
  - ⋆ Fitting
  - ⋆ Completion
- From answers, by the requirements stakeholders,
  - ⋆ the domain requirements prescription document emerges.
- Imagine six phases of re-readings, one for each of the above operators.

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

[1] Projection

- A first reading asks the question:
  - ⋆ Which of the entity types, functions, events and behaviours
  - ⋆ that are described in the domain model
  - ⋆ do you wish to support, partially or fully by the machine?
- The $\mathcal{E}^2\mathcal{G}$ example
  - ⋆ shows a very informal projection
  - ⋆ of almost 100% of "the" domain description!

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

- Projection **examples**:
  - ⋆ **Transportation:** only rail nets
  - ⋆ **The Market:** only consumer/retailer relations
  - ⋆ **Financial Services:** only banking

[2] Instantiation

- A second reading asks the question:
  - ⋆ Which of the entity types, functions, events and behaviours
  - ⋆ that you have projected for machine support
  - ⋆ shall be made less generic, more specific?
- Instantiation **examples**:
  - ⋆ **Transportation nets:** Only the **Shinkansen** lines
  - ⋆ **Market:** Only the **Daiwa** stores
  - ⋆ **Financial Market:** Only **Citicorp**, and only in Japan
- Instantiation (normally) results in further type, function, event and behaviour constraints.

[3] Determination

- A third reading asks the question:
  - ⋆ Which of the entity types, functions, events and behaviours
  - ⋆ that you have projected and instantiated for machine support
  - ⋆ shall be made less “loose” and more deterministic?
- Determination **examples**:
  - ⋆ **Transportation:** commuter train achedules modulo n minutes
  - ⋆ **The Market:** adhere to inquiry, offer, reject/confirm, delivery, accept/reject, invoice, payment scenario
  - ⋆ **Financial Services:** (“algorithmically”) script all banking transactions

[4] Extension

- A fourth reading asks the question:
  - ⋆ Which of the entities, functions, events and behaviours
  - ⋆ that you did not describe in the domain
  - ⋆ because you decided that they are not feasible in the domain
  - ⋆ are made possibly feasible by a machine?
  - ⋆ And for those you so identify, please describe them.
- Extension **examples**:
  - ⋆ **Transportation:** n-intermediate transfer travel inquiries
  - ⋆ **The Market:** exhaustive inquiry search of all retailers
  - ⋆ **Financial Services:** daily/weekly optimisation of funds in demand/deposit and savings accounts and/or high/medium/low risk investments

[5] Fitting

- A fifth, or maybe an earlier, “zeroeth” reading asks the question:
  - ⋆ Which of the entities, functions, events and behaviours
  - ⋆ that you have projected, instantiated, “determinated” and extended for machine support
  - ⋆ may be sharable with other domain requirements
  - ⋆ developed elsewhere — not “officially” related to the present requirements?
  - ⋆ And for those you so identify, please develop an altogether new set of requirements.

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

- The question:
  - ⋆ Which of the entities, functions, events and behaviours
  - ⋆ that you have projected, instantiated, "determinated" and extended for machine support
  - ⋆ may be sharable with other domain requirements
  - ⋆ developed elsewhere — not "officially" related to the present requirements?
  - ⋆ And for those you so identify, please develop an altogether new set of requirements.
- Fitting **examples**:
  - ⋆ **Transportation:** Shared repository on rail and bus nets and time tables + base functions
  - ⋆ **The Market:** Shared repository on retailer/wholesaler/producer prices catalogues + base functions
  - ⋆ **Financial Services:** Shared repository on banking, portfolio, and brokerage clients

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

[6] Completion

- A sixt, possibky a "distributed infix" reading asks the question:
  - ⋆ Which of the entities, functions, events and behaviours
  - ⋆ that are described in the domain model
  - ⋆ have not been covered by the above five domain-to-requirements operations
  - ⋆ but need be putatively formulated as requirements?
- The answer follows!

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

Interface Requirements

- Interface requirements
  - ⋆ are those requirements which can be expressed
  - ⋆ by only using terms both from the domain and the machine.
- Interface requirements thus concerns
  - ⋆ phenomena (and concepts) **shared** between
  - ⋆ the domain
  - ⋆ and the machine.

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

Shared Phenomena and Concepts

- In order to rescribe proper interface requirements
- the requirements engineer need identify
  - ⋆ all the entity types, functions, events and behaviours
  - ⋆ of the domain description
  - ⋆ that must be replicated, not replaced, by the machine.
    - ◇ A shared phenomenon (concept) is thus "present"
    - ◇ both in the domain
    - ◇ and in the machine.
- All such shared phenomena and concepts shall be identified.

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

Interface Requirements Categories

- One can speak of four classes of interface requirements:
  - ⋆ Initialisation and Refreshment of Shared Phenomena and Concepts
  - ⋆ Man-machine Dialogue
  - ⋆ Physiological Implements
  - ⋆ Machine-machine Dialogue
- We will now survey each of these.

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

Initialisation and Refreshment of Shared Phenomena and Concepts

- **Initialisation:**
  - ⋆ All initial entity values, functions, events and "pre-canned" behaviours
  - ⋆ must be identified
  - ⋆ and their machine representation and initial "bulk" input
  - ⋆ must be prescribed.
- **Refreshment:**
  - ⋆ Need for frequency of updates of these entity values, functions, events and "evolving" behaviours
  - ⋆ must be identified
  - ⋆ and their sampled input must be prescribed.

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

- **Means:**
  - ⋆ Usually combinations of
    - ◇ man-machine and
    - ◇ machine-machine dialogues
    - ◇ and their physiological implementation

    need be defined.

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

Man-machine Dialogue

- Definition of user-machine interaction sequences
- wrt. each and every shared phenomenon and concept.

Physiological Implements

- Use of
  - ⋆ visual (graphics display, window, video clips, etc.)
  - ⋆ tactile (keyboard, mouse, screen pointer)
  - ⋆ audio (voice, sound)
  - ⋆ smell, ...

  "devices" (technologies) need be identified and defined.
- All of this wrt. each and every shared phenomenon and concept.

Machine-machine Dialogue

$\mathcal{E}$tcetera!

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

Machine Requirements

- Machine requirements
  - ⋆ are those requirements which can be expressed
  - ⋆ by only using terms from the machine.
- Thus machine requirements, in essence, concerns
  - ⋆ phenomena (and concepts)
  - ⋆ **possessed only**
  - ⋆ by the machine.

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

Categories of Machine Requirements

- We make a distinction between the following categories of machine requirements:
  - ⋆ Performance
  - ⋆ Dependability
  - ⋆ Maintenance
  - ⋆ Platform
  - ⋆ Documentation

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

Performance

- For each
  - ⋆ entity, function, event and behaviour, generic questions
  - ⋆ irrespective of the particulars of the domain,
  - ⋆ and concerning their resource consumption
    (how little, how much, statistics, probablity)

  must be asked and answered:
  - ⋆ **Time:** imply slower/faster machines
  - ⋆ **Space:** imply smaller/larger memories
  - ⋆ **Equipment:** imply less/more peripheral equipment

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

The "ilities": Dependability

- For each
  - ⋆ entity, function, event and behaviour, generic questions
  - ⋆ irrespective of the particulars of the domain,
  - ⋆ concerning their dependability
    (fault analysis, statistics, probablity)

  must be asked and answered:
  - ⋆ **Accessability:** implies "fair" scheduling
  - ⋆ **Availability:** implies time-sharing of resources
  - ⋆ **Safety and Reliability:** implies failure analysis and defensive design
  - ⋆ **Security:** implies intrusion analysis, authorisation, encryption, etc.
  - ⋆ Etc.

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

Maintenance

- For each
  - ⋆ entity, function, event and behaviour, generic questions
  - ⋆ irrespective of the particulars of the domain,
  - ⋆ concerning a spectrum of maintenance issues

  must be asked and answered:
  - ⋆ **Adaptive Maintenance:** adapting to changing base, middleware and/or user machine (e.g., software)
  - ⋆ **Corrective Maintenance:** bugs
  - ⋆ **Perfective Maintenance:** tuning performance (up/down)
  - ⋆ **Preventive Maintenance:** testing after updates

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

Platform

- For each
  - ⋆ entity, function, event and behaviour, generic questions
  - ⋆ irrespective of the particulars of the domain,
  - ⋆ concerning a spectrum of platform issues

  must be asked and answered:
  - ⋆ **Development Platform**
  - ⋆ **Demonstration Platform**
  - ⋆ **Execution Platform**
  - ⋆ **Maintenance Platform**

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

Documentation

- For each
  - ⋆ entity, function, event and behaviour, generic questions
  - ⋆ irrespective of the particulars of the domain,
  - ⋆ concerning a spectrum of documentation issues

  must be asked and answered:
  - ⋆ **Development Documents:** — see next slide!
  - ⋆ **Service Documents:** Installation, maintenance, ...
  - ⋆ **User Documents:** Reference, ...

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

- **Development Documents:**
  - ⋆ **Domain Engineering Documents:** informative, description, analytic (proofs, checks, tests; logbook)
  - ⋆ **Requirements Engineering Documents:** informative, prescription, analytic (proofs, checks, tests; logbook)
  - ⋆ **Software Engineering Documents:** informative, design models,analytic (calculatioms, proofs, checks, tests; logbook)

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

Etcetera

- "Classical", i.e., ad hoc software engineering
- names the following categories of requirements:
  - ⋆ functional, non-functional
  - ⋆ user and systems

  requirements.
- We fail to see a logic in the above categorisartion.
- Instead we offer:
  - ⋆ domain requirements,
  - ⋆ interface requirements, and
  - ⋆ machine requirements!
- I leave it up to you to try relate the former to the latter!

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

Lecture and Requirements Summary

- We have rough-sketched an **example** domain of government and requirements to e-government.
- And we have covered a novel approach to **requirements engineering**.
  - ⋆ It is based strongly on the results of proper, exhaustive domain engineering,
  - ⋆ and introduces the concepts of
    - ◇ domain requirements,
    - ◇ interface requirements, and
    - ◇ machine requirements!
  - ⋆ together with associated sets of
    - ◇ domain-to-domain-requirements principles, techniques and tools,
    - ◇ domain-to-interface-requirements principles, techniques and tools, and
    - ◇ machine requirements principles, techniques and tools!

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

Closing

Summary

- We are at road's end!
- We have covered **central issues of domain engineering**.
- We have given several **non-trivial-sized examples of domain descriptions**.
- Domain engineering is **a new** software engineering **discipline**.
- We have **related** domain engineering to requirements engineering.
- And we have thereby exemplified **a new kind** of requirements engineering.

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

Consequences

- Domain engineering **must precede** requirements engineering.
- Domain theories **must be established** by academic research.
- National public & private sector academia & industry groups
  - ⋆ have an **obligation to pursue professional** software development
  - ⋆ on the basis of the new domain engineering
  - ⋆ and the new kind of requirements engineering.

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

Thanks

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

Table of Contents:

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

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

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

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

© Dines Bjørner, 2006

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

© Dines Bjørner, 2006

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

© Dines Bjørner, 2006

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

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