A Refinement Planning Sheet

Shin NAKAJIMA

National Institute of Informatics
Tokyo, Japan
nkjm@nii.ac.jp

Five major IT companies[1] with an academic institute[2] in Japan formed a joint research group on formal methods, DSF (Dependable Software Forum), in December 2009. Its focus is to study feasibility of their use for the development of Enterprise Software, including Web-based business applications. After an initial survey, DSF adapted Event-B, VDM++, and SPIN for further study. Although VDM++ and SPIN have already been somewhat used in industry in Japan, Event-B/RODIN is new to most of the participating engineers. A series of seminar was given, and some of the obstacles for its use have been identified.

Roughly, three distinctive aspects are important to get accustomed with Event-B/RODIN; the language, refinement-based modeling, and proof methods. Most of the participating engineers have enough experience in software development and are highly motivated. They did not find much difficulty in writing Event-B descriptions, playing with set-theoretic notations. It is, of course, true that proof with RODIN requires some expertises, and turned out that further training would be needed. However, a major bottleneck to face with is a lack of a modeling method to include planning refinement steps. Starting from an initial machine model, refinement went in an ad-hoc manner to result in *spaghetti*. A methodological guideline for a prior sketch on refinement steps is called for.

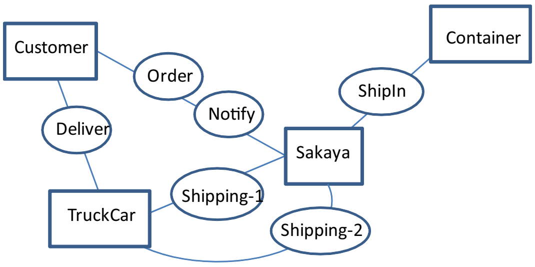
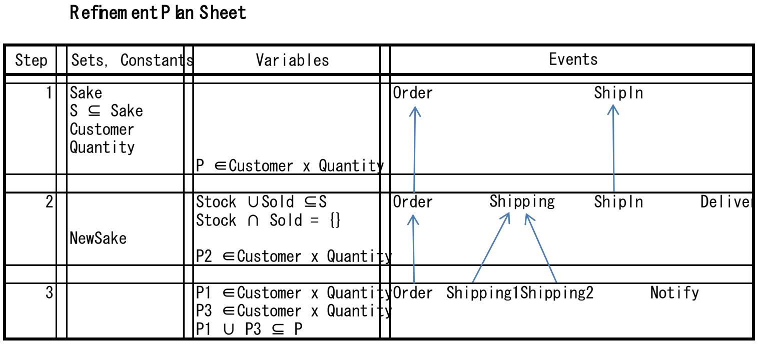


Fig. 1. Joint Action in Catalysis

Since the most engineers nowdays are familar with UML, such a guideline is desirable to share with notion of object-oriented modeling. Thus, Joint action in

[1] NTT-Data, Fujitsu, Hitachi, NEC, and Toshiba.
[2] National Institute of Informatics (NII).

Catalysis [1] is adapted to illustrate a first informal sketch. Its aim is to identify events from the problem space. In Figure 1, each oval is a joint action to work on the participating objects. The identified joint action becomes a candidate for a event. Further, dataflow diagram is used for analyzing how the events work on particular variables. The result is summarized in an Excel-based sheet presentation (Figure 2).



Refinem ent P lan Sheet

Step	Sets, Constants	Variables	Events
1	Sake $S \subseteq$ Sake Customer Quantity	$P \in$Customer x Quantity	Order ShipIn
2	NewSake	Stock $\cup$Sold $\subseteq$S Stock $\cap$ Sold = {} P2 $\in$Customer x Quantity	Order Shipping ShipIn Delive
3		P1 $\in$Customer x Quantity P3 $\in$Customer x Quantity P1 $\cup$ P3 $\subseteq$ P	Order Shipping1Shipping2 Notify

Fig. 2. An Example Sheet using Excel

A refinement planning sheet provides a sketch of what is introduced at each step. Newly defined Sets and some of the important Constants are depicted. Furtrher, variables together with a list of events defined at one particular refinement step are summarized. For example, in Figure 2, two events Order and ShipIn are introduced at the initial level, both may work on a variable P of type Quantity x Customer. Quanatity and Customer are sets introduced at this level. The sheet also shows that Shipping event at the second level is further refined into two decomposed eventts, Shipping-1 and Shipping-2. The event Order is refined at each step as variables to form state-space are detailed.

The sheet provides an overall plan for the refinement and easy to grasp how events are refined at each step. Engineers can concentrate themselves on working with RODIN without losing their ways. Last, a possible plug-in is planned to generate Event-B skelton from the refinement planning sheet.

References

1. D.F.D'Souza and A.C. Wills : *Objects, Components, and Frameworks with UML – The Catalysis Approach*, Addison-Wesley 1999.