# Research of software development technique of enabling dynamic updating

Yuuki Abe (410002)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 9, 2006

**Keywords:** dynamic update,state transition diagram, SPIN, LTL.

## Background and Purpose

In recent years, ubiquitous environment is ready. In this environment, it is required that the software which offers service operates permanently. But some situations that the stop of software is not avoided exists in these software. There is an updating work of software as one of them. The software updating is a work required in order to correct a bug, extend a function and strengthen security. Since service stops while doing this work, the quality of service deteriorates. Furthermore, if the system which exists in all places is updated manually, immense personnel expenses will be applied. These pose a problem when improving ubiquitous environment.

Then, the dynamic updating technique attracts attention. In here, dynamic updating is technical which can shift to a new system safely without terminating a system. In order to establish tha dynamic updating methods, it is necessary to clarify the following methods.

1. discovery technique of the right point which fault does not generate even if it shifts.
2. The realistic mounting technique for resuming from the discovered point.

The technique 1 proposed by this research, having assumed that the technique 2 was already realized.

## Approach

When proposing a technique 1, the most difficult thing is discovery of "the right point". The reason is because the definition of "rightness" is not clear and it is difficult to look for the point which can be resumed from vast state space, and it requires great cost. Here, the point which can be resumed is a point which can shift without terminating a system, although it stops temporarily at the time of updating.

Then, in order to propose the technique which does not require great cost, we limited the point which can be resumed until we could use the state transition diagram. By limiting those points, we become possible looking for the point be resumed in limited state space. Furthermore, since state space is limited, we can use a model cheker SPIN. we proposed the technique 1 using the state transition diagram and SPIN. Above "rightness" is that the following three faults do not occur at the time of updating.

- System stops or hangs up.
- System operates an unjust value.

We placed some assumption when advancing this research. They are shown below.

- System is mounted as the state transition diagram.
- An execution state can be taken out from the old system under operation.

## Proposed technique

We proposed the gradual inspection technique which judges "rightness" stated for the foregoing paragraph. In proposing a technique, we added the information on constraints of state and services to the state transition diagram. The constraint of state is set of conditions realized while the

object in a system stays in certain state. The service is operation of a system useful for a user. The gradual judgment technique using these two infomation which was shown below.

- Narrow down a candidate using constraints of a state.
- Deadlock inspection of a system.
- Specification inspection by the LTL formula.

Resumption from a state in which a system operates an unjust value is prevented at Step 1. We inspect whether a system stops or hangs up at Step 2. We check whether disadvantageous profit arises to a user at Step 3 and then we can judge "rightness".

## Performance evaluation and View

The following items are guranteed when all inspect is passed.

- A system does not operate an unjust value after updating.
- At the time of updating or after updating, a deadlock does not occur in a system after updating.
- The new system fulfills the specification of the old system.
- At the time of updating, service does not fall out and Duplication offer of the service is not made.

The greatest advantage of this technique is that cost is sharply reducible. However, since judgment is too severe, this technique has the fault which overlooks the point which should be able to be resumed. The rule for easing the judgment standard is required of the grade which does not lose an advantage. Moreover, this technique has restriction that a new system has variables, services and external events equivalent to updating before as a fault. In order to confirm this technique more, it is necessary to compensate the two above-mentioned faults.

Finally, it is necessary to propose a technique mounts a system as a state transition diagram and a technique shifts a system dynamically in order to apply this technique actually.