

## MPRI 2.18.2: Solutions for Quiz 2

### 1 Safety

#### Safety of an implementation

The set of runs of an implementation  $I$  is trivially *prefix-closed*: every prefix of a run of  $I$  is also a run of  $I$ .

Suppose that all *finite* runs of  $I$  are *safe* (with respect to some safety property  $P$ ). We want to show that even *infinite* runs of  $I$  are also in  $P$ .

Let  $\sigma$  be any infinite run of  $I$ . Let  $\sigma_1, \dots, \sigma_k, \dots$  be prefixes of  $\sigma$ , where  $\sigma_i, i = 1, 2, \dots$ , has length  $i$ . By our assumption, every  $\sigma_i$  is in  $P$ . Since  $P$  is limit-closed,  $\sigma = \lim_{i \rightarrow \infty} \sigma_i$  is also in  $P$ .

#### Checking safety

We want to argue that to check that a safety property  $P$  is violated, we can look for a *finite* run.

Indeed, consider a run  $\sigma \notin P$ . If  $\sigma$  is finite we are done: for every extension  $\sigma'$  of  $\sigma$ , we have  $\sigma' \notin P$  (otherwise,  $P$  is not prefix-closed).

Let  $\sigma$  be infinite. Suppose, by contradiction, that  $\sigma$  has no unsafe prefixes. Then, by limit-closedness of  $P$ , we get that  $\sigma$  (as the infinite limit of these safe prefixes) is safe—a contradiction.

#### Determining safety

Given a property  $P$ , we want to construct  $S$ , a safety property, and  $L$ , a liveness property, such that  $P = S \cap L$ .

$S$  can be constructed as a *prefix- and limit-closure* of  $P$ , defined as  $P$  plus all prefixes and limits of runs in  $P$ :

$$S = \{\sigma : \exists \sigma' \in P, \sigma \text{ is a prefix of } \sigma'\} \cup \{\sigma : \exists \sigma_1, \sigma_2, \dots \in P, \forall i, \sigma_i \text{ is a prefix of } \sigma_{i+1}, \sigma = \lim_{i \rightarrow \infty} \sigma_i\}$$

By construction,  $S$  is prefix- and limit-closed.

We define  $L$  as the *largest possible set* that gives  $P$  under intersection with  $S$ :

$$L = P \cup \neg S$$

Recall that a liveness property must contain extensions of *all* possible runs: something good should always be able to happen eventually. In this sense, it is better to make  $L$  as large as possible.

By construction,  $S \cap L = P$ .

It remains to show that  $L$  is indeed a liveness property, i.e., for every finite  $\sigma$ , there exists  $\sigma' \in L$ , an extension of  $\sigma$ .

Consider any  $\sigma \notin L$ . By the definition of  $L$ ,  $\sigma \in S - P$ , and, by the definition of  $S$ ,  $\sigma$  is either a finite prefix of a run in  $P$  or an infinite limit of a sequence of runs in  $P$ . Since,  $\sigma$  is finite, we derive that an extension of  $\sigma$  is in  $P$ .

## 2 Liveness

First of all, we observe that wait-freedom (WF) is a subset of every other property in the table, i.e., WF is the strongest liveness property in the set.

Consider obstruction-freedom (OF) and lock-freedom (LF) and take any run  $\sigma \in LF$ . LF is an independent property, so it guarantees progress to some process in all runs, while OF only guarantees progress if some process runs in isolation (for sufficiently long). Therefore, every run in LF is also in OF. Further, any run in which no process ever runs in isolation, e.g., in which processes run one-by-one in the round-robin order, but no process makes progress is, *trivially*, in OF, not in LF. Thus,  $LF \subsetneq OF$ .

Here we use standard logical reasoning. Consider a set of runs defined as follows:

$$P = \{\sigma : A\sigma \Rightarrow B\sigma\},$$

i.e.,  $P$  consists of all runs  $\sigma$ , such that if  $\sigma$  satisfies  $A$ , then it satisfies  $B$ . Then any run that *does not* satisfy  $A$  is *trivially* in  $P$ .

For example, consider the property: “I like all fruits, but if it is an apple, then I only like red ones.” Then if you give me an orange, I should like it.

Similarly, when deadlock-freedom says: “if every process is correct, then some process makes progress”, a run in which not every process is correct, is trivially deadlock-free.

The remaining relations can be established in this way (check, e.g., slide 47 of the second lecture).