Abstract

The specification of a simplified Network Service is given in CSP.

Because specifications of such services are notoriously difficult, it is especially pleasing that in this case the problem can be decomposed into several more easily achieved sub-specifications. This decomposition greatly improves the credibility of the overall specification.
1. Introduction

Problem 2 describes a simplified version of the ISO Network Service, and asks for a specification of it. The main simplifications are

Neither resets nor expedited data are described.

Each service access point (SAP) is limited to participation in only one connection at a time.

We discovered that the second simplification seemed to make the service harder rather than easier to specify; and so we chose instead to specify the simplified Network Service without that restriction. In fact, it was easiest to allow a SAP to participate in even an unbounded number of connections simultaneously.

We use CSP [11] as our specification language, and describe the allowable behaviour of the simplified network by constructing a process NETWORK whose traces are exactly the allowed sequences of network events.

1.1 Structure of the specification

We found it was possible to split the problem into three parts, which could be specified separately; by doing this, of course, the specification was made much less complex. The parts are:

Data transmission
SAP behaviour
Connection behaviour

Data transmission is the purpose of the network; all the complexities of connection establishment, for example, are just the means to that end. In this section we specify that all messages sent from one end of a connection arrive at the other end, in the order they were sent. We do in fact allow an unbounded number of messages to be in transit at any time (another simplifying assumption).

The specification of SAP behaviour covers the details of the way in which a SAP treats one end of a connection - e.g. that it must complete the connection protocol before sending or receiving data, and that it cannot send or receive data after it has (been) disconnected.

Finally, the specification of Connection behaviour covers the way in which events at one end of a connection relate to those at its other end - that a ConReq here appears eventually as a ConInd there, for example. (This really includes data transmission as a special case - so special, however, that we chose to describe it separately).

2. Data transmission

2.1 The alphabet of data events

The alphabet of data events is

$$DT = \text{SAPname} \times \{\text{DatReq, DatInd}\} \times \text{Data}$$

where SAPname is a set from which names of SAPs are drawn, and Data is some set of data elements that can be transmitted or received in a single request. We write

$$a.\text{DatReq}(d)$$

for a typical element of DT. a is the name of the SAP at which this event occurs, and d is the data transmitted.