On the Partial Correctness of the Alternating Bit Protocol

Attila Lakatos and Pál Tőke

One of the basic problems of the computer communication is to give a reliable data transmission on an unreliable data transmission service. In the layered architectures like TCP/IP and ISO OSI Reference Model the data link control and transport layeres are to solve this problem. There are several protocol designs which can be applied. The common basic principle in these protocols is the retransmission and acknowledgement for the messages sent in individual protocol data units. >From mathematical point of view the simplest form of the data transmission phase can be modeled by the alternating bit protocol which can be described by the following parallel program over an appropriate $\mathcal{L}_P$ first order logical language.

$$
\begin{array}{rl}
\Psi \equiv \textbf{initial} & nextinput = u_0 \wedge nr = 1 \wedge \\
 & \wedge\, ls = mn = a = 0; \\
\textbf{cobegin} & \\
\textbf{loop} & \\
\alpha_0 : & \\
 & \textbf{if } ls = a \textbf{ then} \\
 & ls := ls \oplus 1; d := nextinput \textbf{ fi}; \\
\alpha_1 : & \\
 & send(ls, d)\ to\ (mn, inf) \\
\textbf{end} & \\
\| & \\
\textbf{loop} & \\
\beta_0 : & \\
 & \textbf{if } mn = nr \textbf{ then} \\
 & nextoutput := inf; \\
 & nr := nr \oplus 1 \textbf{ fi}; \\
\beta_1 : & \\
 & send(nr \oplus 1)\ to\ (a) \\
\textbf{end} & \\
\textbf{coend} &
\end{array}
$$

The specification of the program is the following:

– $\alpha_1 \to \circ[\quad (mn, inf) = (ls, d) \vee$
$\qquad (mn, inf) = (error, error)]$
– $\alpha_1 \wedge P \to \circ P$
for every P-formula P
not containing *mn* and *inf*.
– $\beta_1 \to \circ(a = nr \oplus 1 \vee a = error)$
– $\beta_1 \wedge P \to \circ P$
for every P-formula P not
containing a-t.
– $\alpha_0 \wedge ls = a \wedge \quad nextinput = u_i \wedge ls = ls_0 \to$
$\qquad \circ(nextinput = u_{i+1} \wedge$
$\qquad ls = ls_0 \oplus 1 \wedge d = u_i)$
– $\alpha_0 \wedge P \to \circ P$
for every P-formula P not
containing *ls* and*d*.
– $\alpha_0 \wedge ls \neq a \wedge P \to \circ P$
for every P-formula P.
– $\beta_0 \wedge \quad mn = nr \wedge nr = nr_0 \to$
$\qquad \circ(nextoutput = inf \wedge nr = nr_0 \oplus 1)$
– $\beta_0 \wedge P \to \circ P$
for every P-formula P not
containing *nextoutput* and *nr*.
– $\beta_0 \wedge mn \neq nr \wedge P \to \circ P$
for every P-formula P.

The partial correctness of the protocol can be formulated by the following assertions:

$$\vdash_{\Sigma_{TP\Psi}} \quad start_{\Psi} \to inf = u_0 \mathbf{atnext}(\beta_0 \wedge mn = nr) \tag{1}$$

$$\vdash_{\Sigma_{TP\Psi}} \quad \beta_0 \wedge mn = nr \wedge inf = u_i \to inf = u_{i+1} \mathbf{atnext}(\beta_0 \wedge mn = nr) \tag{2}$$

The paper gives a detailed and new proof for these assertions and the possible generalization of the applied temporal logical methods for more complex cases are discussed.