byzantine$[m, n:$ nat$, T:$ NONEMPTY_TYPE$]:$ THEORY

BEGIN

ASSUMING

mn_prop : ASSUMPTION $3 \times m < n$

ENDASSUMING

npos : LEMMA $n > 0$

proc : TYPE $=$ below$[n]$

rounds : TYPE $=$ upto$[m]$

vector : TYPE $=$ [proc $\rightarrow T$]

procset : TYPE $=$ setof[proc]

ok : procset

id : (bijective?[proc, proc]) $=$ ($\lambda$ ($p$ : proc) : $p$)

IMPORTING cardinality@finite_cardinality[proc, $n$, id], cardinality@card_set[proc, $n$, id]

$G, p, q, z$ : VAR proc

$r$ : VAR rounds

caucus : VAR procset

$v$ : VAR vector

$t$ : VAR $T$

nok(caucus) : procset $= \{z :$ proc $\mid z \in$ caucus $\wedge \neg$ok$(z)\}$

allprocs : procset $=$ fullset[proc]

allset_card : LEMMA $|$allprocs$| = n$

max_faults : AXIOM $|$nok(allprocs)$| \leq m$

remove_lemma : LEMMA $p \in$ caucus $\supset |$caucus $\setminus \{p\}| = |$caucus$| - 1$

nok_lemma1 : LEMMA ok$(p) \supset |$nok(caucus $\setminus \{p\}$)$| = |$nok(caucus)$|$

nok_lemma3 : LEMMA
$\neg$ok$(p) \wedge p \in$ caucus $\supset |$nok(caucus $\setminus \{p\}$)$| = |$nok(caucus)$| - 1$

maj(caucus, $v$) : $T$

maj_ax : AXIOM

$|\mathrm{caucus}| > 2 \times |\mathrm{nok}(\mathrm{caucus})| \wedge$
$(\forall\ p: \ \mathrm{ok}(p) \wedge p \in \mathrm{caucus} \supset v(p) = t) \supset$
$\mathrm{maj}(\mathrm{caucus}, v) = t$

maj_ext : AXIOM
$\forall\ (v_1, v_2: \ \mathrm{vector}):$
$(\forall\ p: \ p \in \mathrm{caucus} \supset v_1(p) = v_2(p)) \supset \mathrm{maj}(\mathrm{caucus}, v_1) = \mathrm{maj}(\mathrm{caucus}, v_2)$

send : $[T, \ \mathrm{proc}, \ \mathrm{proc} \ \rightarrow \ T]$

send_ax : AXIOM $\mathrm{ok}(p) \wedge \mathrm{ok}(q) \supset \mathrm{send}(t, p, q) = t$

$\mathrm{distr}(t, p): \ \mathrm{vector} \ = \ (\lambda\ (z: \ \mathrm{proc}): \ \mathrm{send}(t, p, z))$

arb : $T$

$\mathrm{OMBG}(G, r, t, \ \mathrm{caucus})(p):$
RECURSIVE $T$ = IF $r = 0$
THEN IF $G \in \mathrm{caucus} \wedge p \in \mathrm{caucus}$
THEN $\mathrm{send}(t, G, p)$
ELSE arb
ENDIF
ELSE IF $G \in \mathrm{caucus} \wedge p \in \mathrm{caucus}$ THEN IF $p = G$ THEN $\mathrm{send}(t, G, G)$
ELSE $\mathrm{maj}(\mathrm{caucus} \setminus \{G\}, (\lambda\ q: \ \mathrm{OMBG}(q, r - 1, \ \mathrm{send}(t, G, q), \mathrm{caucus} \setminus \{G\})(p)))$
ENDIF
ELSE arb
ENDIF
ENDIF
MEASURE $r$

$\mathrm{C2\_prop}(r): \ \mathrm{bool} \ =$
$(\forall\ p, G, t, \ \mathrm{caucus}:$
$\mathrm{ok}(p) \wedge$
$\mathrm{ok}(G) \wedge$
$p \in \mathrm{caucus} \wedge$
$G \in \mathrm{caucus} \wedge$
$|\mathrm{caucus}| > 2 \times |\mathrm{nok}(\mathrm{caucus})| + r \supset$
$\mathrm{OMBG}(G, r, t, \ \mathrm{caucus})(p) = t)$

$C_2$ : LEMMA $\mathrm{C2\_prop}(r)$

C2_final : THEOREM $\mathrm{ok}(p) \wedge \mathrm{ok}(G) \supset \mathrm{OMBG}(G, m, t, \ \mathrm{allprocs})(p) = t$

$\mathrm{C1\_prop}(r): \ \mathrm{bool} \ =$
$(\forall\ p, q, G, \ \mathrm{caucus}, t:$
$\mathrm{ok}(p) \wedge$
$\mathrm{ok}(q) \wedge$
$p \in \mathrm{caucus} \wedge$
$q \in \mathrm{caucus} \wedge$
$G \in \mathrm{caucus} \wedge$
$|\mathrm{caucus}| > 3 \times r \wedge$
$r \geq |\mathrm{nok}(\mathrm{caucus})| \supset$
$\mathrm{OMBG}(G, r, t, \ \mathrm{caucus})(p) = \mathrm{OMBG}(G, r, t, \ \mathrm{caucus})(q))$

$C_1$ : LEMMA C1_prop($r$)

C1_final : THEOREM
$\mathrm{ok}(p) \land \mathrm{ok}(q) \supset \forall\ (G:\ \mathrm{proc}):\ \mathrm{OMBG}(G, m, t,\ \mathrm{allprocs})(p) = \mathrm{OMBG}(G, m, t,\ \mathrm{allprocs})(q)$

END byzantine