Verbose proof for `C2`.

`C2`:

$$\{1\} \quad (\forall\ (r :\ \{s :\ \text{nat} \mid\ s \leq m\}) :\ \text{C2_prop}(r))$$

Installing automatic rewrites: send_ax
distr
remove_lemma
nok_lemma1

`C2`:

$$[1] \quad (\forall\ (r :\ \{s :\ \text{nat} \mid\ s \leq m\}) :\ \text{C2_prop}(r))$$

Inducting on r
,
we get 3 subgoals:

`C2.1`:

$$\{1\} \quad r' \leq m$$
$$\{2\} \quad \text{C2_prop}(r')$$

Simplifying, rewriting, and recording with decision procedures,
This completes the proof of `C2.1`.

`C2.2`:

$$\{1\} \quad 0 \leq m \supset \text{C2_prop}(0)$$

Simplifying, rewriting, and recording with decision procedures,

`C2.2`:

$$[1] \quad 0 \leq m \supset \text{C2_prop}(0)$$

Expanding the definition of C2_prop
,

`C2.2`:

$$\begin{array}{ll}\{1\} & (\forall\ (p :\ \{s :\ \text{nat} \mid\ s\ <\ n\}),\\ & \quad (G :\ \{s :\ \text{nat} \mid\ s\ <\ n\}), (t :\ T), (\text{caucus} :\ [\{s :\ \text{nat} \mid\ s\ <\ n\}\ \rightarrow\ \text{bool}]) :\\ & \quad\ \text{ok}(p) \wedge\\ & \quad\quad \text{ok}(G) \wedge\\ & \quad\quad\ p \in \text{caucus} \wedge\\ & \quad\quad\quad G \in \text{caucus} \wedge\\ & \quad\quad\quad\ |\text{caucus}|\ > 2 \times |\text{nok}(\text{caucus})| \supset\\ & \quad\ \text{OMBG}(G, 0, t, \text{caucus})(p) = t)\end{array}$$

Skolemizing and flattening,

C2.2:

{-1}	ok(p')
{-2}	ok(G')
{-3}	$p' \in$ caucus$'$
{-4}	$G' \in$ caucus$'$
{-5}	$\lvert$caucus$'\rvert > 2 \times \lvert$nok(caucus$'$)$\rvert$
{1}	OMBG$(G', 0, t', \text{caucus}')(p') = t'$

Expanding the definition of OMBG

,

C2.2:

{-1}	ok(p')
{-2}	ok(G')
{-3}	$p' \in$ caucus$'$
{-4}	$G' \in$ caucus$'$
{-5}	$\lvert$caucus$'\rvert > 2 \times \lvert$nok(caucus$'$)$\rvert$
{1}	IF $G' \in$ caucus$' \wedge p' \in$ caucus$'$ THEN send(t', G', p') ELSE arb ENDIF = t'

Applying propositional simplification and decision procedures,

This completes the proof of C2.2.

C2.3:

{1}	$(\forall\ (j : \{i : \text{integer} \mid i \geq 0\}) :$ $j \leq m \supset$ C2_prop$(j) \supset$ $j + 1 \leq m \supset$ C2_prop$(j + 1))$

Skolemizing and flattening,

C2.3:

{-1}	$j' \leq m \supset$ C2_prop(j')
{-2}	$j' + 1 \leq m$
{1}	C2_prop$(j' + 1)$

Expanding the definition of C2_prop

,

C2.3:

$$
\begin{array}{ll}
\{\text{-}1\} & j' \leq m \supset \text{C2_prop}(j') \\
\{\text{-}2\} & j' + 1 \leq m \\
\hline
\{1\} & (\forall\, (p : \{s : \text{nat} \mid s < n\}), \\
 & \quad (G : \{s : \text{nat} \mid s < n\}), (t : T), (\text{caucus} : [\{s : \text{nat} \mid s < n\} \rightarrow \text{bool}]) : \\
 & \quad\; \text{ok}(p) \wedge \\
 & \quad\quad \text{ok}(G) \wedge \\
 & \quad\quad\; p \in \text{caucus} \wedge \\
 & \quad\quad\quad G \in \text{caucus} \wedge \\
 & \quad\quad\quad\; |\text{caucus}| > 1 + 2 \times |\text{nok}(\text{caucus})| + j' \supset \\
 & \quad\quad\; \text{OMBG}(G, 1 + j', t, \text{caucus})(p) = t)
\end{array}
$$

Skolemizing and flattening,

C2.3:

$$
\begin{array}{ll}
\{\text{-}1\} & j' \leq m \supset \text{C2_prop}(j') \\
\{\text{-}2\} & j' + 1 \leq m \\
\{\text{-}3\} & \text{ok}(p') \\
\{\text{-}4\} & \text{ok}(G') \\
\{\text{-}5\} & p' \in \text{caucus}' \\
\{\text{-}6\} & G' \in \text{caucus}' \\
\{\text{-}7\} & |\text{caucus}'| > 1 + 2 \times |\text{nok}(\text{caucus}')| + j' \\
\hline
\{1\} & \text{OMBG}(G', 1 + j', t', \text{caucus}')(p') = t'
\end{array}
$$

Expanding the definition of OMBG

,

C2.3:

$$
\begin{array}{ll}
\{\text{-}1\} & j' \leq m \supset \text{C2_prop}(j') \\
\{\text{-}2\} & j' + 1 \leq m \\
\{\text{-}3\} & \text{ok}(p') \\
\{\text{-}4\} & \text{ok}(G') \\
\{\text{-}5\} & p' \in \text{caucus}' \\
\{\text{-}6\} & G' \in \text{caucus}' \\
\{\text{-}7\} & |\text{caucus}'| > 1 + 2 \times |\text{nok}(\text{caucus}')| + j' \\
\hline
\{1\} & \text{IF } G' \in \text{caucus}' \wedge p' \in \text{caucus}' \\
 & \quad \text{THEN IF } p' = G' \\
 & \quad\;\; \text{THEN } \text{send}(t', G', G') \\
 & \quad\; \text{ELSE} \\
 & \quad\;\; \text{maj}(\text{caucus}' \setminus \{G'\}, \\
 & \quad\quad (\lambda\, (q : \{s : \text{nat} \mid s < n\}) : \\
 & \quad\quad\;\; \text{OMBG}(q, j', \text{send}(t', G', q), \text{caucus}' \setminus \{G'\})(p'))) \\
 & \quad\; \text{ENDIF} \\
 & \quad \text{ELSE arb} \\
 & \quad \text{ENDIF} = \\
 & \quad t'
\end{array}
$$

Repeatedly simplifying with BDDs, decision procedures, rewriting, and if-lifting,

C2.3:

{-1}	C2_prop(j')
{-2}	$1 + j' \leq m$
{-3}	ok(p')
{-4}	ok(G')
{-5}	$p' \in \text{caucus}'$
{-6}	$G' \in \text{caucus}'$
{-7}	$\lvert\text{caucus}'\rvert > 1 + 2 \times \lvert\text{nok}(\text{caucus}')\rvert + j'$
{1}	$p' = G'$
{2}	$\text{maj}(\text{caucus}' \setminus \{G'\}, (\lambda\ (q : \{s : \text{nat} \mid s < n\}) : \text{OMBG}(q, j', \text{send}(t', G', q), \text{caucus}' \setminus \{G'\})(p'))) = t'$

Rewriting using maj_ax

,

C2.3:

{-1}	C2_prop(j')
{-2}	$1 + j' \leq m$
{-3}	ok(p')
{-4}	ok(G')
{-5}	$p' \in \text{caucus}'$
{-6}	$G' \in \text{caucus}'$
{-7}	$\lvert\text{caucus}'\rvert > 1 + 2 \times \lvert\text{nok}(\text{caucus}')\rvert + j'$
{1}	$(\forall\ (p : \{s : \text{nat} \mid s < n\}) :$ $\text{ok}(p) \wedge p \in \text{caucus}' \setminus \{G'\} \supset$ $\text{OMBG}(p, j', \text{send}(t', G', p), \text{caucus}' \setminus \{G'\})(p') = t')$
{2}	$p' = G'$
{3}	$\text{maj}(\text{caucus}' \setminus \{G'\}, (\lambda\ (q : \{s : \text{nat} \mid s < n\}) : \text{OMBG}(q, j', \text{send}(t', G', q), \text{caucus}' \setminus \{G'\})(p'))) = t'$

Hiding formulas: -7, 3,

C2.3:

{-1}	C2_prop(j')
{-2}	$1 + j' \leq m$
{-3}	ok(p')
{-4}	ok(G')
{-5}	$p' \in \text{caucus}'$
{-6}	$G' \in \text{caucus}'$
{1}	$(\forall\ (p : \{s : \text{nat} \mid s < n\}) :$ $\text{ok}(p) \wedge p \in \text{caucus}' \setminus \{G'\} \supset$ $\text{OMBG}(p, j', \text{send}(t', G', p), \text{caucus}' \setminus \{G'\})(p') = t')$
{2}	$p' = G'$

Skolemizing and flattening,

C2.3:

{-1}	$\mathrm{ok}(p'')$
{-2}	$p'' \in \mathrm{caucus}' \setminus \{G'\}$
{-3}	$\mathrm{C2_prop}(j')$
{-4}	$1 + j' \leq m$
{-5}	$\mathrm{ok}(p')$
{-6}	$\mathrm{ok}(G')$
{-7}	$p' \in \mathrm{caucus}'$
{-8}	$G' \in \mathrm{caucus}'$
{1}	$\mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(p') = t'$
{2}	$p' = G'$

Expanding the definition of C2_prop

,

C2.3:

{-1}	$\mathrm{ok}(p'')$
{-2}	$p'' \in \mathrm{caucus}' \setminus \{G'\}$
{-3}	$(\forall\ (p : \{s : \mathrm{nat} \mid s < n\}),$ $(G : \{s : \mathrm{nat} \mid s < n\}), (t : T), (\mathrm{caucus} : [\{s : \mathrm{nat} \mid s < n\} \rightarrow \mathrm{bool}]) :$ $\mathrm{ok}(p) \wedge$ $\mathrm{ok}(G) \wedge$ $p \in \mathrm{caucus} \wedge$ $G \in \mathrm{caucus} \wedge$ $\lvert\mathrm{caucus}\rvert > 2 \times \lvert\mathrm{nok}(\mathrm{caucus})\rvert + j' \supset$ $\mathrm{OMBG}(G, j', t, \mathrm{caucus})(p) = t)$
{-4}	$1 + j' \leq m$
{-5}	$\mathrm{ok}(p')$
{-6}	$\mathrm{ok}(G')$
{-7}	$p' \in \mathrm{caucus}'$
{-8}	$G' \in \mathrm{caucus}'$
{1}	$\mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(p') = t'$
{2}	$p' = G'$

Instantiating quantified variables,

C2.3:

$$
\begin{array}{ll}
\{\text{-}1\} & \mathrm{ok}(p'') \\
\{\text{-}2\} & p'' \in \mathrm{caucus}' \setminus \{G'\} \\
\{\text{-}3\} & \mathrm{ok}(p') \wedge \\
 & \quad \mathrm{ok}(p'') \wedge \\
 & \quad\quad p' \in \mathrm{caucus}' \setminus \{G'\} \wedge \\
 & \quad\quad\quad p'' \in \mathrm{caucus}' \setminus \{G'\} \wedge \\
 & \quad\quad\quad\quad |\mathrm{caucus}' \setminus \{G'\}| \; > 2 \times |\mathrm{nok}(\mathrm{caucus}' \setminus \{G'\})| \; + \; j' \supset \\
 & \quad\quad\quad \mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(p') = \mathrm{send}(t', G', p'') \\
\{\text{-}4\} & 1 \; + \; j' \leq m \\
\{\text{-}5\} & \mathrm{ok}(p') \\
\{\text{-}6\} & \mathrm{ok}(G') \\
\{\text{-}7\} & p' \in \mathrm{caucus}' \\
\{\text{-}8\} & G' \in \mathrm{caucus}' \\
\hline
\{1\} & \mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(p') = t' \\
\{2\} & p' = G'
\end{array}
$$

Applying propositional simplification and decision procedures,

we get 2 subgoals:

C2.3.1:

$$
\begin{array}{ll}
\{\text{-}1\} & \mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(p') = \mathrm{send}(t', G', p'') \\
\{\text{-}2\} & \mathrm{ok}(p'') \\
\{\text{-}3\} & p'' \in \mathrm{caucus}' \setminus \{G'\} \\
\{\text{-}4\} & 1 \; + \; j' \leq m \\
\{\text{-}5\} & \mathrm{ok}(p') \\
\{\text{-}6\} & \mathrm{ok}(G') \\
\{\text{-}7\} & p' \in \mathrm{caucus}' \\
\{\text{-}8\} & G' \in \mathrm{caucus}' \\
\hline
\{1\} & \mathrm{OMBG}(p'', j', t', \mathrm{caucus}' \setminus \{G'\})(p') = t' \\
\{2\} & p' = G'
\end{array}
$$

Simplifying, rewriting, and recording with decision procedures,

This completes the proof of C2.3.1.

C2.3.2:

$$
\begin{array}{ll}
\{\text{-}1\} & \mathrm{ok}(p'') \\
\{\text{-}2\} & p'' \in \mathrm{caucus}' \setminus \{G'\} \\
\{\text{-}3\} & 1 \; + \; j' \leq m \\
\{\text{-}4\} & \mathrm{ok}(p') \\
\{\text{-}5\} & \mathrm{ok}(G') \\
\{\text{-}6\} & p' \in \mathrm{caucus}' \\
\{\text{-}7\} & G' \in \mathrm{caucus}' \\
\hline
\{1\} & p' \in \mathrm{caucus}' \setminus \{G'\} \\
\{2\} & \mathrm{OMBG}(p'', j', t', \mathrm{caucus}' \setminus \{G'\})(p') = t' \\
\{3\} & p' = G'
\end{array}
$$

Trying repeated skolemization, instantiation, and if-lifting,

This completes the proof of C2.3.2.
Q.E.D.