Verbose proof for `C1`.

`C1:`

$$\begin{array}{|ll}
 & \\ \hline
\{1\} & (\forall\ (r:\ \{s:\ \mathrm{nat}\ |\ \ s \le m\}):\ \mathrm{C1_prop}(r))
\end{array}$$

Installing automatic rewrites: send_ax
distr

`C1:`

$$\begin{array}{|ll}
 & \\ \hline
[1] & (\forall\ (r:\ \{s:\ \mathrm{nat}\ |\ \ s \le m\}):\ \mathrm{C1_prop}(r))
\end{array}$$

Inducting on r

,

we get 3 subgoals:

`C1.1:`

$$\begin{array}{|ll}
 & \\ \hline
\{1\} & r' \le m \\
\{2\} & \mathrm{C1_prop}(r')
\end{array}$$

Simplifying, rewriting, and recording with decision procedures,

This completes the proof of `C1.1`.

`C1.2:`

$$\begin{array}{|ll}
 & \\ \hline
\{1\} & 0 \le m \supset \mathrm{C1_prop}(0)
\end{array}$$

Applying disjunctive simplification to flatten sequent,

`C1.2:`

$$\begin{array}{|ll}
\{\text{-}1\} & 0 \le m \\ \hline
\{1\} & \mathrm{C1_prop}(0)
\end{array}$$

Expanding the definition of C1_prop

,

`C1.2:`

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

Skolemizing and flattening,

`C1.2:`

$$
\begin{array}{|ll}
\{\text{-}1\} & 0 \leq m \\
\{\text{-}2\} & \mathrm{ok}(p') \\
\{\text{-}3\} & \mathrm{ok}(q') \\
\{\text{-}4\} & p' \in \mathrm{caucus}' \\
\{\text{-}5\} & q' \in \mathrm{caucus}' \\
\{\text{-}6\} & G' \in \mathrm{caucus}' \\
\{\text{-}7\} & |\mathrm{caucus}'| \ > \ 0 \\
\{\text{-}8\} & 0 \geq |\mathrm{nok}(\mathrm{caucus}')| \\
\hline
\{1\} & \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(p') = \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(q')
\end{array}
$$

Simplifying, rewriting, and recording with decision procedures,

`C1.2:`

$$
\begin{array}{|ll}
\{\text{-}1\} & 0 \leq m \\
\{\text{-}2\} & \mathrm{ok}(p') \\
\{\text{-}3\} & \mathrm{ok}(q') \\
\{\text{-}4\} & p' \in \mathrm{caucus}' \\
\{\text{-}5\} & q' \in \mathrm{caucus}' \\
\{\text{-}6\} & G' \in \mathrm{caucus}' \\
\{\text{-}7\} & |\mathrm{caucus}'| \ > \ 0 \\
\{\text{-}8\} & 0 \geq |\mathrm{nok}(\mathrm{caucus}')| \\
\hline
\{1\} & \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(p') = \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(q')
\end{array}
$$

Case splitting on $\mathrm{ok}(G')$

,

we get 2 subgoals:

`C1.2.1:`

$$
\begin{array}{|ll}
\{\text{-}1\} & \mathrm{ok}(G') \\
\{\text{-}2\} & 0 \leq m \\
\{\text{-}3\} & \mathrm{ok}(p') \\
\{\text{-}4\} & \mathrm{ok}(q') \\
\{\text{-}5\} & p' \in \mathrm{caucus}' \\
\{\text{-}6\} & q' \in \mathrm{caucus}' \\
\{\text{-}7\} & G' \in \mathrm{caucus}' \\
\{\text{-}8\} & |\mathrm{caucus}'| \ > \ 0 \\
\{\text{-}9\} & 0 \geq |\mathrm{nok}(\mathrm{caucus}')| \\
\hline
\{1\} & \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(p') = \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(q')
\end{array}
$$

Expanding the definition of OMBG

,

`C1.2.1:`

[-1]	$\mathrm{ok}(G')$
[-2]	$0 \leq m$
[-3]	$\mathrm{ok}(p')$
[-4]	$\mathrm{ok}(q')$
[-5]	$p' \in \mathrm{caucus}'$
[-6]	$q' \in \mathrm{caucus}'$
[-7]	$G' \in \mathrm{caucus}'$
[-8]	$\lvert\mathrm{caucus}'\rvert \;>\; 0$
[-9]	$0 \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
{1}	$\mathrm{send}(t', G', p') = \mathrm{send}(t', G', q')$

Simplifying, rewriting, and recording with decision procedures,

This completes the proof of `C1.2.1`.

`C1.2.2:`

{-1}	$0 \leq m$
{-2}	$\mathrm{ok}(p')$
{-3}	$\mathrm{ok}(q')$
{-4}	$p' \in \mathrm{caucus}'$
{-5}	$q' \in \mathrm{caucus}'$
{-6}	$G' \in \mathrm{caucus}'$
{-7}	$\lvert\mathrm{caucus}'\rvert \;>\; 0$
{-8}	$0 \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
{1}	$\mathrm{ok}(G')$
{2}	$\mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(p') = \mathrm{OMBG}(G', 0, t', \mathrm{caucus}')(q')$

Hiding formulas: 2,

`C1.2.2:`

[-1]	$0 \leq m$
[-2]	$\mathrm{ok}(p')$
[-3]	$\mathrm{ok}(q')$
[-4]	$p' \in \mathrm{caucus}'$
[-5]	$q' \in \mathrm{caucus}'$
[-6]	$G' \in \mathrm{caucus}'$
[-7]	$\lvert\mathrm{caucus}'\rvert \;>\; 0$
[-8]	$0 \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
[1]	$\mathrm{ok}(G')$

Adding type constraints for $\lvert\mathrm{nok}(\mathrm{caucus}')\rvert$

,

C1.2.2:

{-1}	$\|\text{nok}(\text{caucus}')\| \geq 0$
[-2]	$0 \leq m$
[-3]	$\text{ok}(p')$
[-4]	$\text{ok}(q')$
[-5]	$p' \in \text{caucus}'$
[-6]	$q' \in \text{caucus}'$
[-7]	$G' \in \text{caucus}'$
[-8]	$\|\text{caucus}'\| > 0$
[-9]	$0 \geq \|\text{nok}(\text{caucus}')\|$
[1]	$\text{ok}(G')$

Using lemma fincard_non_empty

,

C1.2.2:

{-1}	$(\exists\ (z: \{s: \text{nat} \mid s < n\}): \text{nok}(\text{caucus}')(z)) \Leftrightarrow \|\text{nok}(\text{caucus}')\| \neq 0$
{-2}	$\|\text{nok}(\text{caucus}')\| \geq 0$
[-3]	$0 \leq m$
[-4]	$\text{ok}(p')$
[-5]	$\text{ok}(q')$
[-6]	$p' \in \text{caucus}'$
[-7]	$q' \in \text{caucus}'$
[-8]	$G' \in \text{caucus}'$
[-9]	$\|\text{caucus}'\| > 0$
[-10]	$0 \geq \|\text{nok}(\text{caucus}')\|$
[1]	$\text{ok}(G')$

Applying propositional simplification and decision procedures,

C1.2.2:

{-1}	$\|\text{nok}(\text{caucus}')\| = 0$
{-2}	$\|\text{nok}(\text{caucus}')\| \geq 0$
[-3]	$0 \leq m$
[-4]	$\text{ok}(p')$
[-5]	$\text{ok}(q')$
[-6]	$p' \in \text{caucus}'$
[-7]	$q' \in \text{caucus}'$
[-8]	$G' \in \text{caucus}'$
[-9]	$\|\text{caucus}'\| > 0$
[-10]	$0 \geq \|\text{nok}(\text{caucus}')\|$
{1}	$(\exists\ (z: \{s: \text{nat} \mid s < n\}): \text{nok}(\text{caucus}')(z))$
[2]	$\text{ok}(G')$

Instantiating the top quantifier in 1 with the terms: G!1

,

`C1.2.2:`

{-1}	$\lvert \mathrm{nok}(\mathrm{caucus}') \rvert = 0$
{-2}	$\lvert \mathrm{nok}(\mathrm{caucus}') \rvert \geq 0$
[-3]	$0 \leq m$
[-4]	$\mathrm{ok}(p')$
[-5]	$\mathrm{ok}(q')$
[-6]	$p' \in \mathrm{caucus}'$
[-7]	$q' \in \mathrm{caucus}'$
[-8]	$G' \in \mathrm{caucus}'$
[-9]	$\lvert \mathrm{caucus}' \rvert > 0$
[-10]	$0 \geq \lvert \mathrm{nok}(\mathrm{caucus}') \rvert$
{1}	$\mathrm{nok}(\mathrm{caucus}')(G')$
[2]	$\mathrm{ok}(G')$

Expanding the definition of nok

,

`C1.2.2:`

{-1}	$\lvert \{z : \mathrm{proc} \mid z \in \mathrm{caucus}' \wedge \neg \mathrm{ok}(z)\} \rvert = 0$
{-2}	$\lvert \{z : \mathrm{proc} \mid z \in \mathrm{caucus}' \wedge \neg \mathrm{ok}(z)\} \rvert \geq 0$
[-3]	$0 \leq m$
[-4]	$\mathrm{ok}(p')$
[-5]	$\mathrm{ok}(q')$
[-6]	$p' \in \mathrm{caucus}'$
[-7]	$q' \in \mathrm{caucus}'$
[-8]	$G' \in \mathrm{caucus}'$
[-9]	$\lvert \mathrm{caucus}' \rvert > 0$
{-10}	$0 \geq \lvert \{z : \mathrm{proc} \mid z \in \mathrm{caucus}' \wedge \neg \mathrm{ok}(z)\} \rvert$
{1}	TRUE
[2]	$\mathrm{ok}(G')$

which is trivially true.

This completes the proof of `C1.2.2`.

`C1.3:`

{1}	$(\forall\ (j : \{i : \mathrm{integer} \mid i \geq 0\}) : j \leq m \supset \mathrm{C1\_prop}(j) \supset j + 1 \leq m \supset \mathrm{C1\_prop}(j + 1))$

Skolemizing and flattening,

`C1.3:`

{-1}	$j' \leq m \supset \mathrm{C1\_prop}(j')$
{-2}	$j' + 1 \leq m$
{1}	$\mathrm{C1\_prop}(j' + 1)$

Expanding the definition of C1_prop

,

`C1.3:`

$$
\begin{array}{|ll}
\{\text{-}1\} & j' \le m \supset \text{C1\_prop}(j') \\
\{\text{-}2\} & j' + 1 \le m \\
\hline
\{1\} & (\forall\ (p:\ \{s:\ \text{nat} \mid s < n\}), \\
& \quad (q:\ \{s:\ \text{nat} \mid s < n\}), \\
& \quad (G:\ \{s:\ \text{nat} \mid s < n\}), (\text{caucus}:\ [\{s:\ \text{nat} \mid s < n\} \to \text{bool}]), (t:\ T): \\
& \quad\ \text{ok}(p) \wedge \\
& \qquad \text{ok}(q) \wedge \\
& \qquad\ p \in \text{caucus} \wedge \\
& \qquad\quad q \in \text{caucus} \wedge \\
& \qquad\qquad G \in \text{caucus} \wedge \\
& \qquad\qquad\ |\text{caucus}| > 3 + 3 \times j' \wedge \\
& \qquad\qquad\quad 1 + j' \ge |\text{nok}(\text{caucus})| \supset \\
& \quad\ \text{OMBG}(G, 1 + j', t, \text{caucus})(p) = \\
& \qquad \text{OMBG}(G, 1 + j', t, \text{caucus})(q))
\end{array}
$$

Skolemizing and flattening,

`C1.3:`

$$
\begin{array}{|ll}
\{\text{-}1\} & j' \le m \supset \text{C1\_prop}(j') \\
\{\text{-}2\} & j' + 1 \le m \\
\{\text{-}3\} & \text{ok}(p') \\
\{\text{-}4\} & \text{ok}(q') \\
\{\text{-}5\} & p' \in \text{caucus}' \\
\{\text{-}6\} & q' \in \text{caucus}' \\
\{\text{-}7\} & G' \in \text{caucus}' \\
\{\text{-}8\} & |\text{caucus}'| > 3 + 3 \times j' \\
\{\text{-}9\} & 1 + j' \ge |\text{nok}(\text{caucus}')| \\
\hline
\{1\} & \text{OMBG}(G', 1 + j', t', \text{caucus}')(p') = \\
& \quad \text{OMBG}(G', 1 + j', t', \text{caucus}')(q')
\end{array}
$$

Simplifying, rewriting, and recording with decision procedures,

`C1.3:`

$$
\begin{array}{|ll}
\{\text{-}1\} & \text{C1\_prop}(j') \\
\{\text{-}2\} & 1 + j' \le m \\
\{\text{-}3\} & \text{ok}(p') \\
\{\text{-}4\} & \text{ok}(q') \\
\{\text{-}5\} & p' \in \text{caucus}' \\
\{\text{-}6\} & q' \in \text{caucus}' \\
\{\text{-}7\} & G' \in \text{caucus}' \\
\{\text{-}8\} & |\text{caucus}'| > 3 + 3 \times j' \\
\{\text{-}9\} & 1 + j' \ge |\text{nok}(\text{caucus}')| \\
\hline
\{1\} & \text{OMBG}(G', 1 + j', t', \text{caucus}')(p') = \\
& \quad \text{OMBG}(G', 1 + j', t', \text{caucus}')(q')
\end{array}
$$

Case splitting on $\text{ok}(G')$

,

we get 2 subgoals:

`C1.3.1:`

{-1}	$\text{ok}(G')$
{-2}	$\text{C1\_prop}(j')$
{-3}	$1 + j' \leq m$
{-4}	$\text{ok}(p')$
{-5}	$\text{ok}(q')$
{-6}	$p' \in \text{caucus}'$
{-7}	$q' \in \text{caucus}'$
{-8}	$G' \in \text{caucus}'$
{-9}	$\lvert\text{caucus}'\rvert > 3 + 3 \times j'$
{-10}	$1 + j' \geq \lvert\text{nok}(\text{caucus}')\rvert$
{1}	$\text{OMBG}(G', 1 + j', t', \text{caucus}')(p') =$ $\text{OMBG}(G', 1 + j', t', \text{caucus}')(q')$

Applying C2
where

`C1.3.1:`

{-1}	$(\forall\ (r :\ \{s :\ \text{nat} \mid\ s \leq m\}) :\ \text{C2\_prop}(r))$
[-2]	$\text{ok}(G')$
[-3]	$\text{C1\_prop}(j')$
[-4]	$1 + j' \leq m$
[-5]	$\text{ok}(p')$
[-6]	$\text{ok}(q')$
[-7]	$p' \in \text{caucus}'$
[-8]	$q' \in \text{caucus}'$
[-9]	$G' \in \text{caucus}'$
[-10]	$\lvert\text{caucus}'\rvert > 3 + 3 \times j'$
[-11]	$1 + j' \geq \lvert\text{nok}(\text{caucus}')\rvert$
[1]	$\text{OMBG}(G', 1 + j', t', \text{caucus}')(p') =$ $\text{OMBG}(G', 1 + j', t', \text{caucus}')(q')$

Expanding the definition of C2_prop

,

`C1.3.1:`

$$
\begin{array}{|ll}
\{-1\} & (\forall\ (r:\ \{s:\ \text{nat}\ |\ \ s \leq m\}):\\
& \quad (\forall\ (p:\ \{s:\ \text{nat}\ |\ \ s\ <\ n\}),\\
& \quad\ (G:\ \{s:\ \text{nat}\ |\ \ s\ <\ n\}), (t:\ T), (\text{caucus}:\ [\{s:\ \text{nat}\ |\ \ s\ <\ n\}\ \rightarrow\ \text{bool}]):\\
& \qquad \text{ok}(p)\wedge\\
& \qquad\quad \text{ok}(G)\wedge\\
& \qquad\qquad p \in \text{caucus}\wedge\\
& \qquad\qquad\ G \in \text{caucus}\wedge\\
& \qquad\qquad\quad |\text{caucus}|\ >\ r\ + 2 \times |\text{nok}(\text{caucus})| \supset\\
& \qquad\ \ \text{OMBG}(G, r, t, \text{caucus})(p) = t))\\
[-2] & \text{ok}(G')\\
[-3] & \text{C1\_prop}(j')\\
[-4] & 1\ +\ j' \leq m\\
[-5] & \text{ok}(p')\\
[-6] & \text{ok}(q')\\
[-7] & p' \in \text{caucus}'\\
[-8] & q' \in \text{caucus}'\\
[-9] & G' \in \text{caucus}'\\
[-10] & |\text{caucus}'|\ >\ 3\ +\ 3 \times j'\\
[-11] & 1\ +\ j' \geq |\text{nok}(\text{caucus}')|\\
\hline
[1] & \text{OMBG}(G', 1\ +\ j', t', \text{caucus}')(p') =\\
& \ \ \text{OMBG}(G', 1\ +\ j', t', \text{caucus}')(q')
\end{array}
$$

Installing automatic rewrites: -1

`C1.3.1:`

$$
\begin{array}{|ll}
\{-1\} & (\forall\ (r:\ \{s:\ \text{nat}\ |\ \ s \leq m\}):\\
& \quad (\forall\ (p:\ \{s:\ \text{nat}\ |\ \ s\ <\ n\}),\\
& \quad\ (G:\ \{s:\ \text{nat}\ |\ \ s\ <\ n\}), (t:\ T), (\text{caucus}:\ [\{s:\ \text{nat}\ |\ \ s\ <\ n\}\ \rightarrow\ \text{bool}]):\\
& \qquad \text{ok}(p)\wedge\\
& \qquad\quad \text{ok}(G)\wedge\\
& \qquad\qquad p \in \text{caucus}\wedge\\
& \qquad\qquad\ G \in \text{caucus}\wedge\\
& \qquad\qquad\quad |\text{caucus}|\ >\ r\ + 2 \times |\text{nok}(\text{caucus})| \supset\\
& \qquad\ \ \text{OMBG}(G, r, t, \text{caucus})(p) = t))\\
[-2] & \text{ok}(G')\\
[-3] & \text{C1\_prop}(j')\\
[-4] & 1\ +\ j' \leq m\\
[-5] & \text{ok}(p')\\
[-6] & \text{ok}(q')\\
[-7] & p' \in \text{caucus}'\\
[-8] & q' \in \text{caucus}'\\
[-9] & G' \in \text{caucus}'\\
[-10] & |\text{caucus}'|\ >\ 3\ +\ 3 \times j'\\
[-11] & 1\ +\ j' \geq |\text{nok}(\text{caucus}')|\\
\hline
[1] & \text{OMBG}(G', 1\ +\ j', t', \text{caucus}')(p') =\\
& \ \ \text{OMBG}(G', 1\ +\ j', t', \text{caucus}')(q')
\end{array}
$$

Simplifying, rewriting, and recording with decision procedures,

This completes the proof of `C1.3.1`.

C1.3.2:

{-1}	$\mathrm{C1\_prop}(j')$
{-2}	$1 + j' \le m$
{-3}	$\mathrm{ok}(p')$
{-4}	$\mathrm{ok}(q')$
{-5}	$p' \in \mathrm{caucus}'$
{-6}	$q' \in \mathrm{caucus}'$
{-7}	$G' \in \mathrm{caucus}'$
{-8}	$\lvert\mathrm{caucus}'\rvert > 3 + 3 \times j'$
{-9}	$1 + j' \ge \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
{1}	$\mathrm{ok}(G')$
{2}	$\mathrm{OMBG}(G', 1 + j', t', \mathrm{caucus}')(p') =$ $\mathrm{OMBG}(G', 1 + j', t', \mathrm{caucus}')(q')$

Expanding the definition of OMBG

,

C1.3.2:

[-1]	$\mathrm{C1\_prop}(j')$
[-2]	$1 + j' \le m$
[-3]	$\mathrm{ok}(p')$
[-4]	$\mathrm{ok}(q')$
[-5]	$p' \in \mathrm{caucus}'$
[-6]	$q' \in \mathrm{caucus}'$
[-7]	$G' \in \mathrm{caucus}'$
[-8]	$\lvert\mathrm{caucus}'\rvert > 3 + 3 \times j'$
[-9]	$1 + j' \ge \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
[1]	$\mathrm{ok}(G')$
{2}	$\textsc{if}\ p' = G'\ \textsc{then}\ \mathrm{send}(t', G', G')$ $\textsc{else}$ $\mathrm{maj}(\mathrm{caucus}' \setminus \{G'\}, (\lambda\ (q:\ \{s:\ \mathrm{nat} \mid s < n\}): \mathrm{OMBG}(q, j', \mathrm{send}(t', G', q), \mathrm{caucus}' \setminus \{G'\})(p')))$ $\textsc{endif} =$ $\textsc{if} q' = G'\ \textsc{then}\ \mathrm{send}(t', G', G')$ $\textsc{else}$ $\mathrm{maj}(\mathrm{caucus}' \setminus \{G'\}, (\lambda\ (q:\ \{s:\ \mathrm{nat} \mid s < n\}): \mathrm{OMBG}(q, j', \mathrm{send}(t', G', q), \mathrm{caucus}' \setminus \{G'\})(q')))$ $\textsc{endif}$

Applying propositional simplification and decision procedures,

`C1.3.2:`

[-1]	$\mathrm{C1\_prop}(j')$
[-2]	$1 + j' \leq m$
[-3]	$\mathrm{ok}(p')$
[-4]	$\mathrm{ok}(q')$
[-5]	$p' \in \mathrm{caucus}'$
[-6]	$q' \in \mathrm{caucus}'$
[-7]	$G' \in \mathrm{caucus}'$
[-8]	$\lvert\mathrm{caucus}'\rvert > 3 + 3 \times j'$
[-9]	$1 + j' \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
[1]	$\mathrm{ok}(G')$
{2}	$\mathrm{maj}(\mathrm{caucus}' \setminus \{G'\}, (\lambda\ (q:\ \{s:\ \mathrm{nat} \mid s < n\}) : \mathrm{OMBG}(q, j', \mathrm{send}(t', G', q), \mathrm{caucus}' \setminus \{G'\})(p'))) =$ $\mathrm{maj}(\mathrm{caucus}' \setminus \{G'\}, (\lambda\ (q:\ \{s:\ \mathrm{nat} \mid s < n\}) : \mathrm{OMBG}(q, j', \mathrm{send}(t', G', q), \mathrm{caucus}' \setminus \{G'\})(q')))$

Rewriting using maj_ext

,

`C1.3.2:`

[-1]	$\mathrm{C1\_prop}(j')$
[-2]	$1 + j' \leq m$
[-3]	$\mathrm{ok}(p')$
[-4]	$\mathrm{ok}(q')$
[-5]	$p' \in \mathrm{caucus}'$
[-6]	$q' \in \mathrm{caucus}'$
[-7]	$G' \in \mathrm{caucus}'$
[-8]	$\lvert\mathrm{caucus}'\rvert > 3 + 3 \times j'$
[-9]	$1 + j' \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
{1}	$(\forall\ (p:\ \{s:\ \mathrm{nat} \mid s < n\}) :$ $p \in \mathrm{caucus}' \setminus \{G'\} \supset$ $\mathrm{OMBG}(p, j', \mathrm{send}(t', G', p), \mathrm{caucus}' \setminus \{G'\})(p') =$ $\mathrm{OMBG}(p, j', \mathrm{send}(t', G', p), \mathrm{caucus}' \setminus \{G'\})(q'))$
[2]	$\mathrm{ok}(G')$
{3}	$\mathrm{maj}(\mathrm{caucus}' \setminus \{G'\}, (\lambda\ (q:\ \{s:\ \mathrm{nat} \mid s < n\}) : \mathrm{OMBG}(q, j', \mathrm{send}(t', G', q), \mathrm{caucus}' \setminus \{G'\})(p'))) =$ $\mathrm{maj}(\mathrm{caucus}' \setminus \{G'\}, (\lambda\ (q:\ \{s:\ \mathrm{nat} \mid s < n\}) : \mathrm{OMBG}(q, j', \mathrm{send}(t', G', q), \mathrm{caucus}' \setminus \{G'\})(q')))$

Hiding formulas: 3,

`C1.3.2:`

[-1]	$\mathrm{C1\_prop}(j')$
[-2]	$1 \; + \; j' \leq m$
[-3]	$\mathrm{ok}(p')$
[-4]	$\mathrm{ok}(q')$
[-5]	$p' \in \mathrm{caucus}'$
[-6]	$q' \in \mathrm{caucus}'$
[-7]	$G' \in \mathrm{caucus}'$
[-8]	$\lvert\mathrm{caucus}'\rvert \; > \; 3 \; + \; 3 \times j'$
[-9]	$1 \; + \; j' \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
{1}	$(\forall\ (p:\ \{s:\ \mathrm{nat} \mid \ s \ < \ n\}):$ $p \in \mathrm{caucus}' \setminus \{G'\} \supset$ $\mathrm{OMBG}(p, j', \mathrm{send}(t', G', p), \mathrm{caucus}' \setminus \{G'\})(p') =$ $\mathrm{OMBG}(p, j', \mathrm{send}(t', G', p), \mathrm{caucus}' \setminus \{G'\})(q'))$
[2]	$\mathrm{ok}(G')$

Skolemizing and flattening,

`C1.3.2:`

{-1}	$p'' \in \mathrm{caucus}' \setminus \{G'\}$
[-2]	$\mathrm{C1\_prop}(j')$
[-3]	$1 \; + \; j' \leq m$
[-4]	$\mathrm{ok}(p')$
[-5]	$\mathrm{ok}(q')$
[-6]	$p' \in \mathrm{caucus}'$
[-7]	$q' \in \mathrm{caucus}'$
[-8]	$G' \in \mathrm{caucus}'$
[-9]	$\lvert\mathrm{caucus}'\rvert \; > \; 3 \; + \; 3 \times j'$
[-10]	$1 \; + \; j' \geq \lvert\mathrm{nok}(\mathrm{caucus}')\rvert$
{1}	$\mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(p') =$ $\mathrm{OMBG}(p'', j', \mathrm{send}(t', G', p''), \mathrm{caucus}' \setminus \{G'\})(q')$
[2]	$\mathrm{ok}(G')$

Expanding the definition of C1_prop

,

`C1.3.2:`

$$
\begin{array}{l|l}
\{\text{-}1\} & p'' \in \text{caucus}' \setminus \{G'\} \\
\{\text{-}2\} & (\forall\ (p:\ \{s:\ \text{nat} \mid\ s\ <\ n\}), \\
 & \quad (q:\ \{s:\ \text{nat} \mid\ s\ <\ n\}), \\
 & \quad (G:\ \{s:\ \text{nat} \mid\ s\ <\ n\}), (\text{caucus}:\ [\{s:\ \text{nat} \mid\ s\ <\ n\}\ \rightarrow\ \text{bool}]), (t:\ T): \\
 & \quad\quad \text{ok}(p) \wedge \\
 & \quad\quad\quad \text{ok}(q) \wedge \\
 & \quad\quad\quad\quad p \in \text{caucus} \wedge \\
 & \quad\quad\quad\quad\quad q \in \text{caucus} \wedge \\
 & \quad\quad\quad\quad\quad\quad G \in \text{caucus} \wedge \\
 & \quad\quad\quad\quad\quad\quad\quad |\text{caucus}|\ >\ 3 \times j' \wedge \\
 & \quad\quad\quad\quad\quad\quad\quad\quad j' \geq |\text{nok}(\text{caucus})| \supset \\
 & \quad\quad\quad \text{OMBG}(G, j', t, \text{caucus})(p) = \text{OMBG}(G, j', t, \text{caucus})(q)) \\
[\text{-}3] & 1\ +\ j' \leq m \\
[\text{-}4] & \text{ok}(p') \\
[\text{-}5] & \text{ok}(q') \\
[\text{-}6] & p' \in \text{caucus}' \\
[\text{-}7] & q' \in \text{caucus}' \\
[\text{-}8] & G' \in \text{caucus}' \\
[\text{-}9] & |\text{caucus}'|\ >\ 3\ +\ 3 \times j' \\
[\text{-}10] & 1\ +\ j' \geq |\text{nok}(\text{caucus}')| \\
\hline
\{1\} & \text{OMBG}(p'', j', \text{send}(t', G', p''), \text{caucus}' \setminus \{G'\})(p') = \\
 & \quad \text{OMBG}(p'', j', \text{send}(t', G', p''), \text{caucus}' \setminus \{G'\})(q') \\
[2] & \text{ok}(G')
\end{array}
$$

Instantiating quantified variables,

`C1.3.2:`

$$
\begin{array}{l|l}
\{\text{-}1\} & p'' \in \text{caucus}' \setminus \{G'\} \\
\{\text{-}2\} & \text{ok}(p') \wedge \\
 & \quad \text{ok}(q') \wedge \\
 & \quad\quad p' \in \text{caucus}' \setminus \{G'\} \wedge \\
 & \quad\quad\quad q' \in \text{caucus}' \setminus \{G'\} \wedge \\
 & \quad\quad\quad\quad p'' \in \text{caucus}' \setminus \{G'\} \wedge \\
 & \quad\quad\quad\quad\quad |\text{caucus}' \setminus \{G'\}|\ >\ 3 \times j' \wedge \\
 & \quad\quad\quad\quad\quad\quad j' \geq |\text{nok}(\text{caucus}' \setminus \{G'\})| \supset \\
 & \quad \text{OMBG}(p'', j', \text{send}(t', G', p''), \text{caucus}' \setminus \{G'\})(p') = \\
 & \quad\quad \text{OMBG}(p'', j', \text{send}(t', G', p''), \text{caucus}' \setminus \{G'\})(q') \\
[\text{-}3] & 1\ +\ j' \leq m \\
[\text{-}4] & \text{ok}(p') \\
[\text{-}5] & \text{ok}(q') \\
[\text{-}6] & p' \in \text{caucus}' \\
[\text{-}7] & q' \in \text{caucus}' \\
[\text{-}8] & G' \in \text{caucus}' \\
[\text{-}9] & |\text{caucus}'|\ >\ 3\ +\ 3 \times j' \\
[\text{-}10] & 1\ +\ j' \geq |\text{nok}(\text{caucus}')| \\
\hline
\{1\} & \text{OMBG}(p'', j', \text{send}(t', G', p''), \text{caucus}' \setminus \{G'\})(p') = \\
 & \quad \text{OMBG}(p'', j', \text{send}(t', G', p''), \text{caucus}' \setminus \{G'\})(q') \\
[2] & \text{ok}(G')
\end{array}
$$

Trying repeated skolemization, instantiation, and if-lifting,

This completes the proof of `C1.3.2`.

Q.E.D.