# Malloc Specification

January 13, 2020

$$
\begin{aligned}
&\text{PC} \mapsto_r (\text{RW}, \text{Global}, b_m, e_m, a_m) && (1)\\
*\ &\mathop{\Large *}_{r \in \texttt{regs}} \exists w, r \mapsto_r w && (2)\\
*\ &\text{region } W * \text{full\_sts\_world } W && (3)\\
*\ &\triangleright (\text{PC} \mapsto_r \textit{continuation} && (4)\\
&\quad * \exists b'\ e', e' - b' = size - 1 \wedge r_1 \mapsto_r (\text{RWX}, \text{Global}, b', e', b') && (5)\\
&\quad * \mathop{\Large *}_{r \in \texttt{regs}/\{r_1\}} \exists w, r \mapsto_r w && (6)\\
&\quad * \text{region } (W[e', \cdots, b' := \texttt{permanent}]) && (7)\\
&\quad * \text{full\_sts\_world } (W[e', \cdots, b' := \texttt{permanent}]) && (8)\\
&\quad * \mathop{\Large *}_{a \in [b', e']} \text{rel } a \text{ RWX} && (9)\\
&\quad \mathrel{-\!\!*} \textbf{WP Seq (Instr Executable) } \{\Phi\}) && (10)\\
\vdash\ &\textbf{WP Seq (Instr Executable) } \{\Phi\} && (11)
\end{aligned}
$$

(1) the program counter after jumping the Malloc subroutine

(2) general purpose registers

(3) region and collection of state transition systems

(4) the program counter is set to the continuation once Malloc is done

(5) $b'$ and $e'$ denote the malloc'ed region, must be a fresh region. $r_1$ now contains a capability to that region

(6) general purpose registers

(7) the updated region with the new permanent addresses

(8) the updated STS collection

(9) each address in the malloc'ed range is in the region with permission RWX

(10) the continuation should have $\Phi$ as its postcondition

(11) then malloc followed by the continuation has $\Phi$ as its postcondition