A proof of Doug Lea's memory manager

John Wickerson

April 29, 2011

Chapter 1

Glossary of macros, typedefs and minor routines

$$
\begin{array}{ll}
\texttt{MALLOC\_ALIGNMENT} & = 8 \\
\texttt{MAX\_SIZE\_T} & = \mathit{FFFF\ FFFF}_h \\
\texttt{SIZE\_T\_SIZE} & = 4 \\
\texttt{SIZE\_T\_BITSIZE} & = 32 \\
\texttt{SIZE\_T\_ZERO} & = 0 \\
\texttt{SIZE\_T\_ONE} & = 1 \\
\texttt{SIZE\_T\_TWO} & = 2 \\
\texttt{SIZE\_T\_FOUR} & = 4 \\
\texttt{TWO\_SIZE\_T\_SIZES} & = 8 \\
\texttt{FOUR\_SIZE\_T\_SIZES} & = 16 \\
\texttt{SIX\_SIZE\_T\_SIZES} & = 24 \\
\texttt{HALF\_MAX\_SIZE\_T} & = \mathit{7FFF\ FFFF}_h \\
\texttt{CHUNK\_ALIGN\_MASK} & = 111_b \\
\texttt{mchunk} & = \texttt{struct malloc\_chunk} \\
\texttt{mchunkptr} & = \texttt{mchunk*} \\
\texttt{shinptr} & = \texttt{mchunk*} \\
\texttt{bindex\_t} & = \texttt{unsigned int} \\
\texttt{binmap\_t} & = \texttt{unsigned int} \\
\texttt{flag\_t} & = \texttt{unsigned int} \\
\texttt{MCHUNK\_SIZE} & = 16 \\
\texttt{CHUNK\_OVERHEAD} & = 4 \\
\texttt{MIN\_CHUNK\_SIZE} & = 16 \\
\texttt{chunk2mem(p)} & = p + 8 \\
\texttt{mem2chunk(mem)} & = \texttt{mem} - 8 \\
\texttt{MAX\_REQUEST} & = 2^{32} - 63 \\
\texttt{MIN\_REQUEST} & = 11 \\
\texttt{pad\_request(req)} & = \lceil \texttt{req} + 4 \rceil_8 \\
\texttt{request2size(req)} & = \max\{16, \lceil \texttt{req} + 4 \rceil_8\} \\
\texttt{PINUSE\_BIT} & = 1_b \\
\texttt{CINUSE\_BIT} & = 10_b \\
\texttt{FLAG\_BIT} & = 100_b \\
\texttt{INUSE\_BITS} & = 11_b \\
\texttt{FLAG\_BITS} & = 111_b \\
\texttt{cinuse(p)} & = [p_{[1]} == 1 \\
\texttt{pinuse(p)} & = [p_{[0]} == 1 \\
\texttt{is\_inuse(p)} & = \texttt{is\_mmapped(p)} \vee \texttt{cinuse(p)} \\
\texttt{is\_mmapped(p)} & = [p_{[1:0]} == 00 \\
\texttt{chunksize(p)} & = [(p+1)]_{[31:3]}000[\\
\left\{p_{01} \mapsto \_\right\} \texttt{clear\_pinuse(p)} & \left\{p_{01} \mapsto 0\right\} \\
\texttt{chunk\_plus\_offset(p,s)} & = p + s \\
\texttt{chunk\_minus\_offset(p,s)} & = p - s \\
\texttt{next\_chunk(p)} & = \texttt{ncat(p)} \\
\texttt{prev\_chunk(p)} & = \texttt{prev(p)} \\
\texttt{next\_pinuse(p)} & = \mathit{flags}(\mathit{ncat}(p)) = \blacktriangle \\
\texttt{get\_foot(p,s)} & = \mathit{prev\_foot}(p+s) \\
\left\{\mathit{prev\_foot}(p+s) = \_\right\} \texttt{set\_foot(p,s)} & \left\{\mathit{prev\_foot}(p+s) = s\right\} \\
\left\{\begin{array}{l}\mathit{size}(p) = \_ \wedge \mathit{flags}(p) = \_\_\_\_ \\ \wedge\ \mathit{prev\_foot}(p+s) = \_\end{array}\right\} \texttt{set\_size\_and\_pinuse\_of\_free\_chunk(p,s)} & \left\{\begin{array}{l}\mathit{size}(p) = s \wedge \mathit{flags}(p) = \blacktriangledown\blacktriangle \\ \wedge\ \mathit{prev\_foot}(\mathit{next}(p)) = s\end{array}\right\} \\
\left\{\begin{array}{l}\mathit{size}(p) = \_ \wedge \mathit{flags}(p) = \_\_\_\_ \\ \wedge\ \mathit{prev\_foot}(p+s) = \_ \\ \wedge\ \mathit{flags}(p+s) = \_\_\_\end{array}\right\} \texttt{set\_free\_with\_pinuse(p,s,n)} & \left\{\begin{array}{l}\mathit{size}(p) = s \wedge \mathit{flags}(p) = \blacktriangledown\blacktriangle \\ \wedge\ \mathit{prev\_foot}(\mathit{next}(p)) = s \\ \wedge\ \mathit{flags}(\mathit{next}(p)) = \triangle\end{array}\right\} \\
\texttt{tchunk} & = \texttt{malloc\_tree\_chunk} \\
\texttt{tchunkptr} & = \texttt{tchunk*} \\
\texttt{tbinptr} & = \texttt{tchunk*} \\
\texttt{leftmost\_child(t)} & = \begin{cases} \mathit{child}_0(\texttt{rt}) & \text{if } \mathit{child}_0(\texttt{rt}) \neq 0 \\ \mathit{child}_1(\texttt{rt}) & \text{otherwise} \end{cases} \\
\texttt{NSMALLBINS} & = 32 \\
\texttt{NTREEBINS} & = 32 \\
\texttt{SMALLBIN\_SHIFT} & = 3 \\
\texttt{SMALLBIN\_WIDTH} & = 8 \\
\texttt{TREEBIN\_SHIFT} & = 8 \\
\texttt{MIN\_LARGE\_SIZE} & = 256 \\
\texttt{MAX\_SMALL\_SIZE} & = 255 \\
\texttt{MAX\_SMALL\_REQUEST} & = 244 \\
\texttt{mstate} & = \texttt{struct malloc\_state} \\
\texttt{mparams} & = \texttt{struct malloc\_params} \\
\texttt{is\_small(s)} & = s < 256 \\
\texttt{small\_index(s)} & = [s/8] \\
\texttt{small\_index2size(i)} & = 8 \times i \\
\texttt{MIN\_SMALL\_INDEX} & = 2 \\
\left\{\mathit{smallbins}[2i+2] \mapsto C_1 * \mathit{smallbins}[2i+3] \mapsto C_2\right\} \texttt{x := smallbin\_at(M,i)} & \left\{\texttt{x}.\texttt{fd} \mapsto C_1 * \texttt{x}.\texttt{bk} \mapsto C_2\right\} \\
\texttt{treebin\_at(M,i)} & = \texttt{treebins[i]} \\
\left\{\texttt{I} = \_\right\} \texttt{compute\_tree\_index(S,I)} & \left\{\texttt{I} = \begin{cases} 0 & \text{if } \mathbb{S} < 256 \\ 31 & \text{if } \mathbb{S} \geq 2^{24} \\ 2(\log_2[\![\mathbb{S}]\!] - 8) & \text{if } 0 \leq [\![\mathbb{S}]\!] < \lfloor [\![\mathbb{S}]\!] \\ 2(\log_2[\![\mathbb{S}]\!] - 8) + 1 & \text{if } \lfloor [\![\mathbb{S}]\!] \leq [\![\mathbb{S}]\!] < [\![\mathbb{S}]\!] \end{cases}\right\} \\
\texttt{bin\_for\_tree\_index(i)} & = \begin{cases} 31 & \text{if } \mathtt{i} = 31 \\ [1/2] + 6 & \text{otherwise} \end{cases} \\
\texttt{leftshift\_for\_tree\_index(i)} & = \begin{cases} 0 & \text{if } \mathtt{i} = 31 \\ 25 - [1/2] & \text{otherwise} \end{cases} \\
\texttt{minsize\_for\_tree\_index(i)} & = \begin{cases} 2 \ll ([1/2] + 7) & \text{if i even} \\ 3 \ll ([1/2] + 7) & \text{if i odd} \end{cases} \\
\texttt{idx2bit(i)} & = 1 \ll \mathtt{i} \\
\left\{\mathit{smallmap}[\mathtt{i}] = \_\right\} \texttt{mark\_smallmap(M,i)} & \left\{\mathit{smallmap}[\mathtt{i}] = 1\right\} \\
\left\{\mathit{smallmap}[\mathtt{i}] = \_\right\} \texttt{clear\_smallmap(M,i)} & \left\{\mathit{smallmap}[\mathtt{i}] = 0\right\} \\
\texttt{smallmap\_is\_marked(M,i)} & = \mathit{smallmap}[\mathtt{i}] = 1 \\
\left\{\mathit{treemap}[\mathtt{i}] = \_\right\} \texttt{mark\_treemap(M,i)} & \left\{\mathit{treemap}[\mathtt{i}] = 1\right\} \\
\left\{\mathit{treemap}[\mathtt{i}] = \_\right\} \texttt{clear\_treemap(M,i)} & \left\{\mathit{treemap}[\mathtt{i}] = 0\right\} \\
\texttt{treemap\_is\_marked(M,i)} & = \mathit{treemap}[\mathtt{i}] = 1 \\
\texttt{least\_bit(x)} & = \begin{cases} \mathbf{0}\ \mathbf{1}\ \mathbf{0} & \text{if } \mathtt{x}_i = 1 \wedge \forall j < i.\, \mathtt{x}_j = 0 \} \\ \mathbf{0} & \text{if } \mathtt{x} = 0 \end{cases} \\
\texttt{left\_bits(x)} & = \begin{cases} \mathtt{1}\ \mathtt{0}\ \mathbf{0} & \text{if } \mathtt{x}_i = 1 \wedge \forall j < i.\, \mathtt{x}_j = 0 \} \\ \mathbf{0} & \text{if } \mathtt{x} = 0 \end{cases} \\
\texttt{same\_or\_left\_bits(x)} & = \begin{cases} \mathtt{1}\ \mathtt{1}\ \mathbf{0} & \text{if } \mathtt{x}_i = 1 \wedge \forall j < i.\, \mathtt{x}_j = 0 \} \\ \mathbf{0} & \text{if } \mathtt{x} = 0 \end{cases} \\
\left\{\mathtt{I} = \_\right\} \texttt{compute\_bit2idx(X,I)} & \left\{\mathtt{x} \neq 0 \Rightarrow \mathtt{I} = \log_2 \mathtt{X}\right\} \\
\left\{p\right\} \texttt{mark\_inuse\_foot(M,p,s)} & \left\{p\right\} \\
\left\{\begin{array}{l}\mathit{size}(p) = \_ \wedge \mathit{flags}(p) = \_P \\ \wedge\ \mathit{flags}(p+s) = C_*\end{array}\right\} \texttt{set\_inuse(M,p,s)} & \left\{\begin{array}{l}\mathit{size}(p) = s \wedge \mathit{flags}(p) = \blacktriangledown P \\ \wedge\ \mathit{flags}(\mathit{next}(p)) = C\blacktriangle\end{array}\right\} \\
\left\{\begin{array}{l}\mathit{size}(p) = \_ \wedge \mathit{flags}(p) = \_\_\_\_ \\ \wedge\ \mathit{flags}(p+s) = C_*\end{array}\right\} \texttt{set\_inuse\_and\_pinuse(M,p,s)} & \left\{\begin{array}{l}\mathit{size}(p) = s \wedge \mathit{flags}(p) = \blacktriangledown\blacktriangle \\ \wedge\ \mathit{flags}(\mathit{next}(p)) = C\blacktriangle\end{array}\right\} \\
\left\{\begin{array}{l}\mathit{size}(p) = \_ \\ \wedge\ \mathit{flags}(p) = \_\_\_\end{array}\right\} \texttt{set\_inuse\_and\_pinuse\_of\_inuse\_chunk(M,p,s)} & \left\{\begin{array}{l}\mathit{size}(p) = s \\ \wedge\ \mathit{flags}(p) = \blacktriangledown\blacktriangle\end{array}\right\}
\end{array}
$$

Chapter 2

State

Shorthand:

$$
\begin{aligned}
|i| &\stackrel{\text{def}}{=} \{8i\} \\
\|i\| &\stackrel{\text{def}}{=} \texttt{compute\_tree\_index}^{-1}(i) \\
\mathsf{w} &\stackrel{\text{def}}{=} 4 \\
x \uplus y &\stackrel{\text{def}}{=} \begin{cases} x \cup y & \text{if } x \cap y = \{\} \\ \text{undefined} & \text{otherwise} \end{cases} \\
x \uplus\!\!- y &\stackrel{\text{def}}{=} \begin{cases} x - y & \text{if } y \subseteq x \\ \text{undefined} & \text{otherwise} \end{cases}
\end{aligned}
$$

Predicates:

$$
\begin{aligned}
x \xmapsto{\mathsf{prevfoot}} s &\stackrel{\text{def}}{=} x \mapsto s \\
x \xmapsto{\mathsf{size}} s &\stackrel{\text{def}}{=} \exists n.\, (x + 1\mathsf{w}) \mapsto_{[31..3]} n \ * \ 8n = s \\
x \xmapsto{\mathsf{pinuse}} b &\stackrel{\text{def}}{=} (x + 1\mathsf{w}) \mapsto_{[0]} b \\
x \xmapsto{\mathsf{cinuse}} b &\stackrel{\text{def}}{=} (x + 1\mathsf{w}) \mapsto_{[1]} b \\
x \xmapsto{\mathsf{fd}} y &\stackrel{\text{def}}{=} x + 2\mathsf{w} \mapsto y \\
x \xmapsto{\mathsf{bk}} y &\stackrel{\text{def}}{=} x + 3\mathsf{w} \mapsto y \\
\mathit{ublock}(x, y, B) &\stackrel{\text{def}}{=} \mathsf{let}\ s = y - x\ \mathsf{in}\ \exists n.\, B = \{x + 2\mathsf{w} \mapsto_{\mathsf{u}} n\mathsf{w}\} \ * \ (n+1)\mathsf{w} = s \\
&\quad * \ \tfrac{1}{2}(x \xmapsto{\mathsf{size}} s) \ * \ y \xmapsto{\mathsf{pinuse}} 0 \ * \ x \xmapsto{\mathsf{cinuse}} 0 \\
&\quad * \ s \geq 4\mathsf{w} \ * \ \mathop{\Large *}_{i=4}^{s/\mathsf{w}}.\, x + i\mathsf{w} \mapsto \_ \ * \ y \xmapsto{\mathsf{prevfoot}} s \\
\mathit{ablock}(x, y, B) &\stackrel{\text{def}}{=} \mathsf{let}\ s = y - x\ \mathsf{in}\ \exists n.\, B = \{x + 2\mathsf{w} \mapsto_{\mathsf{a}} n\mathsf{w}\} \ * \ (n+1)\mathsf{w} \leq s \\
&\quad * \ \tfrac{1}{2}(x \xmapsto{\mathsf{size}} s) \ * \ y \xmapsto{\mathsf{pinuse}} 1 \ * \ x \xmapsto{\mathsf{cinuse}} 1 \\
&\quad * \ s \geq 4\mathsf{w} \ * \ \mathop{\Large *}_{i=n+2}^{s/\mathsf{w}+1}.\, x + i\mathsf{w} \mapsto \_ \\
\mathit{block} &\stackrel{\text{def}}{=} \mathit{ublock} \vee \mathit{ablock} \\
\mathit{bin}(S, x, U) &\stackrel{\text{def}}{=} (U = \{\} \ * \ x \xmapsto{\mathsf{fd}} \_ \ * \ x \xmapsto{\mathsf{bk}} \_) \\
&\quad \vee (\exists y.\, x \xmapsto{\mathsf{fd}} y \ * \ y \xmapsto{\mathsf{bk}} x \ * \ (\mathit{bnode}\ S)^*(y, x, U)) \\
\mathit{bnode}\ S\,(x, y, U) &\stackrel{\text{def}}{=} \exists s.\, x \xmapsto{\mathsf{fd}} y \ * \ y \xmapsto{\mathsf{bk}} x \ * \ U = \{x + 2\mathsf{w} \mapsto s - 1\mathsf{w}\} \ * \ \tfrac{1}{2}(x \xmapsto{\mathsf{size}} s) \ * \ s \in S \\
\mathit{sorted}(L, \sqsubseteq) &\stackrel{\text{def}}{=} \forall i, j.\, i \leq j \Rightarrow L(i) \sqsubseteq L(j) \\
\mathit{coallesced}(B) &\stackrel{\text{def}}{=} \exists L.\, \mathrm{ran}\, L = B \ * \ \mathit{sorted}(L, \leq_1) \ * \ \nexists i.\, (L(i))_3 = (L(i+1))_3 = \mathsf{u} \\
\mathit{arena}(B) &\stackrel{\text{def}}{=} \mathit{coallesced}(B) \ * \ \texttt{start} \xmapsto{\mathsf{pinuse}} 1 \ * \ \texttt{start} \xmapsto{\mathsf{prevfoot}} \_ \\
&\quad * \ \mathit{block}^*(\texttt{start}, \texttt{top}, B) \ * \ \mathit{ublock}(\texttt{top}, \texttt{top} + \texttt{topsize}, \_) \\
\mathit{smallbin}_i(U) &\stackrel{\text{def}}{=} i \in [0, 32) \ * \ \mathit{bin}(|i|, \texttt{smallbin} + 2i\mathsf{w}, U) \ * \ \texttt{smallmap}_{[i]} = (U \neq \{\}) \\
\mathit{treebin}_i(U) &\stackrel{\text{def}}{=} i \in [0, 32) \ * \ \mathit{bin}(\|i\|, \texttt{treebins} + i\mathsf{w}, U) \ * \ \texttt{treemap}_{[i]} = (U \neq \{\}) \\
\mathit{state}(A) &\stackrel{\text{def}}{=} \exists \{U_i \mid i \in [0, 64)\}.\, \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}.\, U_i)_{\mathsf{u}}) \ * \ \texttt{least\_addr} = 5\mathsf{w} \\
&\qquad\qquad * \ \mathop{\Large *}_{i=0}^{32}.\, \mathit{smallbin}_i(U_i) \ * \ \mathop{\Large *}_{i=0}^{32}.\, \mathit{treebin}_i(U_{i+32}) \\
\mathit{invariant} &\stackrel{\text{def}}{=} \boxed{\exists A.\, \mathit{state}(A)} \\
\mathit{token}(x, n) &\stackrel{\text{def}}{=} \boxed{\exists A.\, \mathit{state}(A \uplus \{x \mapsto n\})} \ * \ \tfrac{1}{2}(x - 2\mathsf{w} \xmapsto{\mathsf{size}} \_)
\end{aligned}
$$

Lemma 1. *The assertion*

$$\mathit{block}(x, y, B_1) \ * \ \mathit{ablock}(y, z, B_2) \ * \ \mathit{coallesced}(B_1 \uplus B_2 \uplus B_3)$$

implies

$$\mathit{ublock}(x, y, B_1) \ * \ \mathit{ablock}(y, z, B_2) \ * \ \mathit{coallesced}(B_1 \uplus B_2 \uplus B_3).$$

Chapter 3

Auxilliary operations

3.1 set_inuse_and_pinuse

Specification:

$\left\{p.^{\mathtt{size}}{}_{\_} * p.^{\mathtt{pinuse}}{}_{\_} * p.^{\mathtt{cinuse}}{}_{\_} * p + s.^{\mathtt{pinuse}}{}_{\_}\right\}$
set_inuse_and_pinuse(M,p,s)
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}1 * p + s.^{\mathtt{pinuse}}{}1\right\}$

Verification:

$\left\{p.^{\mathtt{size}}{}_{\_} * p.^{\mathtt{pinuse}}{}_{\_} * p.^{\mathtt{cinuse}}{}_{\_} * p + s.^{\mathtt{pinuse}}{}_{\_}\right\}$
p->head = (s|PINUSE_BIT|CINUSE_BIT);
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}1 * p + s.^{\mathtt{pinuse}}{}_{\_}\right\}$
((bchunkptr)(((char*)p) + s))->head |= PINUSE_BIT;
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}1 * p + s.^{\mathtt{pinuse}}{}1\right\}$

3.2 set_size_and_pinuse_of_free_chunk

Specification:

$\left\{p.^{\mathtt{size}}{}_{\_} * p.^{\mathtt{pinuse}}{}_{\_} * p.^{\mathtt{cinuse}}{}_{\_} * p + s.^{\mathtt{pinuse}}{}_{\_}\right\}$
set_size_and_pinuse_of_free_chunk(p,s)
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}0 * p + s.^{\mathtt{pinuse}}{}s\right\}$

Verification:

$\left\{p.^{\mathtt{size}}{}_{\_} * p.^{\mathtt{pinuse}}{}_{\_} * p.^{\mathtt{cinuse}}{}_{\_} * p + s.^{\mathtt{pinuse}}{}_{\_}\right\}$
p->head = (s|PINUSE_BIT);
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}0 * p + s.^{\mathtt{pinuse}}{}_{\_}\right\}$
set_foot(p,s);
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}0 * p + s.^{\mathtt{pinuse}}{}s\right\}$

3.3 set_size_and_pinuse_of_inuse_chunk

Specification:

$\left\{p.^{\mathtt{size}}{}_{\_} * p.^{\mathtt{pinuse}}{}_{\_} * p.^{\mathtt{cinuse}}{}_{\_}\right\}$
set_size_and_pinuse_of_inuse_chunk(M,p,s)
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}1\right\}$

Verification:

$\left\{p.^{\mathtt{size}}{}_{\_} * p.^{\mathtt{pinuse}}{}_{\_} * p.^{\mathtt{cinuse}}{}_{\_}\right\}$
p->head = (s|PINUSE_BIT|CINUSE_BIT);
$\left\{p.^{\mathtt{size}}{}s * p.^{\mathtt{pinuse}}{}1 * p.^{\mathtt{cinuse}}{}1\right\}$

3.4 insert_small_chunk

Specification:

$\left\{\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathit{smallbin}_{|\mathbb{S}/8|}(U)\right\}$
insert_small_chunk(M,P,S) /*node*/
$\left\{\mathit{smallbin}_{|\mathbb{S}/8|}(U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})\right\}$

Verification:

$\left\{\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathit{smallbin}_{|\mathbb{S}/8|}(U)\right\}$
bindex_t I = small_index(S);
$\left\{\begin{array}{l}\exists B.\ \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * B = \mathit{smallbin} + 2I w * 0 \le \mathbb{I} < 32 \\ * \mathit{bin}(\mathbb{I}, B, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = (U \neq \{\})\end{array}\right\}$
mchunkptr B = smallbin_at(M, I);
$\left\{\begin{array}{l}\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathbb{B} = \mathit{smallbin} + 2I w * 0 \le \mathbb{I} < 32 \\ * \mathit{bin}(\mathbb{I}, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = (U \neq \{\})\end{array}\right\}$
mchunkptr F = B;
$\left\{\begin{array}{l}\exists F'.\ \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} \\ * \mathbb{B} = \mathit{smallbin} + 2I w * F = \mathbb{B} * 0 \le \mathbb{I} < 32 \\ * \left([\mathbb{B}.^{\mathtt{fd}}{}_{\_} * \mathbb{B}.^{\mathtt{bk}}{}_{\_} * U = \{\}\right) \\ \vee \left(\mathbb{B}.^{\mathtt{fd}}{} F' * F'.^{\mathtt{bk}}{}\mathbb{B} * (\mathit{bnode}\ \mathbb{I})^*(F', \mathbb{B}, U)\right) \\ * \mathit{smallmap}_{|\mathbb{S}/8|} = (U \neq \{\})\end{array}\right\}$
//assert(B >= MIN_CHUNK_SIZE);
if (!smallmap_is_marked(M, I))
$\left\{\begin{array}{l}\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathbb{B} = \mathit{smallbin} + 2I w * F = \mathbb{B} * 0 \le \mathbb{I} < 32 \\ * \mathbb{B}.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * (\mathit{bnode}\ \mathbb{I})^*(\mathbb{P}, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = 0 * U = \{\}\end{array}\right\}$
mark_smallmap(M, I);
$\left\{\begin{array}{l}\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathbb{B} = \mathit{smallbin} + 2I w * 0 \le \mathbb{I} < 32 \\ * \mathbb{B}.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * (\mathit{bnode}\ \mathbb{I})^*(\mathbb{P}, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = 1\end{array}\right\}$
else /*if (RTCHECK(OK_address(M, B->fd)))
$\left\{\begin{array}{l}\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathbb{B} = \mathit{smallbin} + 2I w * 0 \le \mathbb{I} < 32 \\ * \mathbb{B}.^{\mathtt{fd}}{} F * F'.^{\mathtt{bk}}{}\mathbb{B} * (\mathit{bnode}\ \mathbb{I})^*(F, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = 1 \\ F = \mathbb{B}{-}2d;\end{array}\right\}$
$\left\{\begin{array}{l}\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}\mathbb{I} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathbb{B} = \mathit{smallbin} + 2I w * 0 \le \mathbb{I} < 32 \\ * \mathbb{B}.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * (\mathit{bnode}\ \mathbb{I})^*(\mathbb{P}, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = 1\end{array}\right\}$
// else {
// CORRUPTION_ERROR_ACTION(M);
// }
$\left\{\begin{array}{l}\exists i.\ \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}i * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathbb{B} = \mathit{smallbin} + 2i * 0 \le i < 32 \\ * \mathbb{B}.^{\mathtt{fd}}{}_{\_} * F.^{\mathtt{bk}}{}_{\_} * (\mathit{bnode}\ i)^*(F, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = 1\end{array}\right\}$
B->fd = P;
F->bk = P;
P->fd = F;
P->bk = B;
$\left\{\begin{array}{l}\exists i.\ \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * \mathbb{S} = \mathbb{S}i * \mathbb{B} = \mathit{smallbin} + 2i * 0 \le i < 32 \\ * \mathbb{B}.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}\mathbb{B} \\ * (\mathit{bnode}\ i)^*(\mathbb{P}, \mathbb{B}, U) * \mathit{smallmap}_{|\mathbb{S}/8|} = 1\end{array}\right\}$
$\left\{\begin{array}{l}\exists i.\ \mathbb{S} = \mathbb{S}i * \mathbb{B} = \mathit{smallbin} + 2i * 0 \le i < 32 * \mathbb{B}.^{\mathtt{fd}}{} \mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{} \mathbb{B} \\ * (\mathit{bnode}\ i)^*(\mathbb{P}, \mathbb{B}, U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\}) * \mathit{smallmap}_{|\mathbb{S}/8|} = 1\end{array}\right\}$
$\left\{\begin{array}{l}\exists i.\ \mathbb{S} = \mathbb{S}i * 0 \le i < 32 \\ * \mathit{bin}(i, \mathit{smallbin} + 2i, U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\}) \\ * \mathit{smallmap}_{|\mathbb{S}/8|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$
$\left\{\mathit{smallbin}_{|\mathbb{S}/8|}(U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})\right\}$

3.5 unlink_small_chunk

Specification:

$\left\{\mathit{smallbin}_{|\mathbb{S}/8|}(U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})\right\}$
unlink_small_chunk(M,P,S) /*node*/
$\left\{\left[p.^{\mathtt{size}}{}\mathbb{S}\right) * p.^{\mathtt{fd}}{}_{\_} * p.^{\mathtt{bk}}{}_{\_} * \mathit{smallbin}_{|\mathbb{S}/8|}(U)\right\}$

$\mathit{smallbin}_{|\mathbb{S}/8|}(U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})$

Defn of *smallbin*.

∃*p*

∃*i*

$\mathbb{S} = \mathbb{S}i * 0 \le i < 32$
$* \ x = \mathit{smallbin} + 2iw$

$\mathit{bin}(i, x, U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})$

$\mathit{smallmap}_{|i|} = 1$

Defn of *bin*.

∃*y*

$x.^{\mathtt{fd}}{}y$ | $y.^{\mathtt{bk}}{}x$ | $(\mathit{bnode}\ i)^*(y, x, U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})$

Split *bnode* list into three.

$\exists U_1\ U_2$

$U = U_1 \uplus U_2$ | $(\mathit{bnode}\ i)^*(y, \mathbb{P}, U_2)$ | $\exists F\ \mathbb{P}.^{\mathtt{bk}}{}F$ $* \ F.^{\mathtt{fd}}{}\mathbb{P}$ $* \ \left[p.^{\mathtt{size}}{}\mathbb{S}\right)$ $* \ (\mathit{bnode}\ i)^*(F, x, U_2)$

Enroll RTC one step.

$(y = \mathbb{P} * U_1 = \{\}) \vee (\exists B.$
$(\mathit{bnode}\ i)^*(y, B, U_1 \uplus \{B + 2w{\mapsto}\_\})$
$* \ B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B)$

schunkptr F = P->fd;

$\mathbb{P}.^{\mathtt{bk}}{}y$ | $\mathbb{P}.^{\mathtt{fd}}{}y$ | $\left[p.^{\mathtt{size}}{}\mathbb{S}\right)$ | $(\mathit{bnode}\ i)^*(\mathbb{P}, x, U_2)$

Extend scope of ∃*B*. Choose $B = x$ in first disjunct.

$\exists B.$
$(y = \mathbb{P} * U_1 = \{\} * B = x) \vee$
$(\mathit{bnode}\ i)^*(y, B, U_1 \uplus \{B + 2w{\mapsto}\_\})$
$* \ B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B)$

Twist.

$(y = \mathbb{P} * U_1 = \{\} * B = x) \vee$
$(\mathit{bnode}\ i)^*(y, B, U_1 \uplus \{B + 2w{\mapsto}\_\})$
$* \ B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B)$

$U = U_1 \uplus U_2$

Distribute $x.^{\mathtt{fd}}{}y$ * $y.^{\mathtt{bk}}{}x$ into disjunction.

$(B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B * y = \mathbb{P} * U_1 = \{\} * B = x) \vee$
$(\mathit{bnode}\ i)^*(y, B, U_1 \uplus \{B + 2w{\mapsto}\_\})$
$* \ B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B * x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x)$

Distribute $B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B$ out of disjunction. Forget $y = \mathbb{P}$ from first disjunct.

$(U_1 = \{\} * B = x) \vee$
$((\mathit{bnode}\ i)^*(y, B, U_1 \uplus \{B + 2w{\mapsto}\_\})$
$* \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x)$

$B.^{\mathtt{fd}}{}\mathbb{P}$ | $\mathbb{P}.^{\mathtt{bk}}{}B$

schunkptr B = P->bk;

$(U_1 = \{\} * \mathbb{B} = x) \vee$
$((\mathit{bnode}\ i)^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\})$
$* \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x)$

$\mathbb{B}.^{\mathtt{fd}}{}\mathbb{P}$ | $\mathbb{P}.^{\mathtt{bk}}{}\mathbb{B}$

$(U_1 = \{\} * \mathbb{B} = x) \vee \exists y.$
$((\mathit{bnode}\ i)^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\})$
$* \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x)$

binder_t I = small_index(S);

$\mathbb{S} = \mathbb{S}\mathbb{I} * 0 \le \mathbb{I} < 32$
$* \ x = \mathit{smallbin} + 2Iw$

$(U_1 = \{\} * \mathbb{B} = x) \vee \exists y.$
$((\mathit{bnode}\ \mathbb{I})^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\})$
$* \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x)$

$\mathbb{B}.^{\mathtt{fd}}{}y$ | $y.^{\mathtt{bk}}{}\mathbb{B}$ | $U = U_1 \uplus U_2$ | $x.^{\mathtt{bk}}{}y$ | $y.^{\mathtt{fd}}{}x$ | $\left[p.^{\mathtt{size}}{}\mathbb{S}\right)$ | $(\mathit{bnode}\ \mathbb{I})^*(\mathbb{P}, x, U_2)$ | $\mathit{smallmap}_{|\mathbb{I}|} = 1$

Twist. Forget values of $y.^{\mathtt{bk}}{}$ and $\mathbb{P}.^{\mathtt{fd}}{}$.

if (P==B) {

$y.^{\mathtt{bk}}{}\mathbb{P}$ | $\mathbb{P}.^{\mathtt{fd}}{}y$ | $(\mathit{bnode}\ \mathbb{I})^*(\mathbb{P}, x, U_2)$ | $U = U_1 \uplus U_2$ | $\mathit{smallmap}_{|\mathbb{I}|} = 1$ | $\mathbb{P}.^{\mathtt{bk}}{}x$ | $x.^{\mathtt{fd}}{}\mathbb{P}$ | $\left[p.^{\mathtt{size}}{}\mathbb{S}\right)$

$\mathbb{B} = F$

Ribbons 1 and 4 contradict second disjunction of ribbon 2. Hence $U_1 = \{\}$ and $U_2 = \{\}$.

$x.^{\mathtt{bk}}{}y$ | $y.^{\mathtt{fd}}{}x$ | $U = \{\}$

clear_smallmap(M,I)

$U = \{\}$ | $\mathit{smallmap}_{|\mathbb{I}|} = (U \neq \{\})$

Defn of *bin*.

$\mathit{bin}(\mathbb{I}, x, U)$

} else {

$\mathbb{B} \neq F$

From ribbons 1, 2 and 5, declare U_1 and U_2 can't both be empty. Extend scope of $\exists y$ in ribbon 2, choosing $y = \mathbb{P}$ in first disjunct.

$\exists y.\ (y = \mathbb{P} * U_1 = \{\} * \mathbb{B} = x) \vee$
$((\mathit{bnode}\ \mathbb{I})^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\})$
$* \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x)$

$\mathbb{B}.^{\mathtt{fd}}{}y$ | $x.^{\mathtt{bk}}{}y$ | $(\mathit{bnode}\ \mathbb{I})^*(\mathbb{P}, x, U_2)$ | $U = U_1 \uplus U_2$ | $\mathit{smallmap}_{|\mathbb{I}|} = (U \neq \{\})$

B->fd == F F->bk == B

$y.^{\mathtt{bk}}{}\mathbb{B}$ | $\mathbb{B}.^{\mathtt{fd}}{}y$

Distribute $\mathbb{B}.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}\mathbb{B}$ into disjunction.

∃*y*

$(y = F * U_1 = \{\} * \mathbb{B} = x * \mathbb{B}.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}\mathbb{B}) \vee$
$(\mathit{bnode}\ \mathbb{I})^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\})$
$* \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x * \mathbb{B}.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}\mathbb{B})$

Distribute $x.^{\mathtt{fd}}{}y$ * $y.^{\mathtt{bk}}{}x$ out of disjunction.

$x.^{\mathtt{fd}}{}y$ | $y.^{\mathtt{bk}}{}x$

$(y = F * U_1 = \{\}) \vee$
$((\mathit{bnode}\ \mathbb{I})^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\})$
$* \ \mathbb{B}.^{\mathtt{fd}}{}F * F.^{\mathtt{bk}}{}\mathbb{B})$

RotR RTC.

$(\mathit{bnode}\ \mathbb{I})^*(y, F, U_1)$

Merge two *bnode* lists.

$(\mathit{bnode}\ \mathbb{I})^*(y, x, U)$

Defn of *bin*.

$\mathit{bin}(\mathbb{I}, x, U)$

}

Defn of *smallbin*.

$\mathit{smallbin}_{|\mathbb{S}/8|}(U)$

Verification:

$\left\{\mathit{smallbin}_{|\mathbb{S}/8|}(U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\})\right\}$
$\left\{\begin{array}{l}\exists i, x.\ \mathbb{S} = \mathbb{S}i * 0 \le i < 32 * x = \mathit{smallbin} + 2iw \\ * \ \mathit{bin}(i, x, U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\}) \\ * \ \mathit{smallmap}_{|i|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$
$\left\{\begin{array}{l}\exists i, x, y.\ \mathbb{S} = \mathbb{S}i * 0 \le i < 32 * x = \mathit{smallbin} + 2iw \\ * \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x * (\mathit{bnode}\ i)^*(y, x, U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\}) \\ * \ \mathit{smallmap}_{|i|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$
$\left\{\begin{array}{l}\exists i, x, y, F, U_1, U_2.\ \mathbb{S} = \mathbb{S}i * 0 \le i < 32 * x = \mathit{smallbin} + 2iw \\ * \ x.^{\mathtt{fd}}{}y * y.^{\mathtt{bk}}{}x * U = U_1 \uplus U_2 \\ * \ (\mathit{bnode}\ i)^*(y, \mathbb{P}, U_1) * \mathbb{P}.^{\mathtt{bk}}{}F * F.^{\mathtt{fd}}{}\mathbb{P} * \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * (\mathit{bnode}\ i)^*(F, x, U_2) \\ * \ \mathit{smallmap}_{|i|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$
$\left\{\begin{array}{l}\exists i, x, y, F, B, U_1, U_2.\ \mathbb{S} = \mathbb{S}i * 0 \le i < 32 * x = \mathit{smallbin} + 2iw \\ * \ U = U_1 \uplus U_2 \\ * \ ((y = \mathbb{P} * B = x * U_1 = \{\}) \\ \vee \ (y.^{\mathtt{bk}}{}y * y.^{\mathtt{fd}}{}x * (\mathit{bnode}\ i)^*(y, B, U_1 \uplus \{B + 2w{\mapsto}\_\}))) \\ * \ B.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}B * y.^{\mathtt{fd}}{}F * \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * F.^{\mathtt{bk}}{}\mathbb{P} * (\mathit{bnode}\ i)^*(F, x, U_2) \\ * \ \mathit{smallmap}_{|i|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$
mchunkptr F = P->fd;
mchunkptr B = P->bk;
$\left\{\begin{array}{l}\exists x, y, U_1, U_2.\ \mathbb{S} = \mathbb{S}\mathbb{I} * 0 \le \mathbb{I} < 32 * x = \mathit{smallbin} + 2Iw \\ * \ U = U_1 \uplus U_2 \\ * \ ((y = \mathbb{P} * F = x * U_1 = \{\}) \\ \vee \ (y.^{\mathtt{bk}}{}y * y.^{\mathtt{fd}}{}x * (\mathit{bnode}\ \mathbb{I})^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\}))) \\ * \ \mathbb{B}.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}\mathbb{B} * \mathbb{P}.^{\mathtt{fd}}{}F * \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * F.^{\mathtt{bk}}{}\mathbb{P} * (\mathit{bnode}\ \mathbb{I})^*(F, x, U_2) \\ * \ \mathit{smallmap}_{|\mathbb{I}|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$
bindex_t I = small_index(S);
$\left\{\begin{array}{l}\exists x, y, U_1, U_2.\ \mathbb{S} = \mathbb{S}\mathbb{I} * 0 \le \mathbb{I} < 32 * x = \mathit{smallbin} + 2Iw \\ * \ U = U_1 \uplus U_2 \\ * \ ((y = \mathbb{P} * x = x * U_1 = \{\}) \\ \vee \ (y.^{\mathtt{bk}}{}y * y.^{\mathtt{fd}}{}x * (\mathit{bnode}\ \mathbb{I})^*(y, \mathbb{B}, U_1 \uplus \{\mathbb{B} + 2w{\mapsto}\_\}))) \\ * \ \mathbb{B}.^{\mathtt{fd}}{}\mathbb{P} * \mathbb{P}.^{\mathtt{bk}}{}\mathbb{B} * \mathbb{P}.^{\mathtt{fd}}{}F * \left[p.^{\mathtt{size}}{}\mathbb{S}\right) * F.^{\mathtt{bk}}{}\mathbb{P} * (\mathit{bnode}\ \mathbb{I})^*(F, x, U_2) \\ * \ \mathit{smallmap}_{|\mathbb{I}|} = (U \uplus \{\mathbb{P} + 2w{\mapsto}\mathbb{S} - 1w\} \neq \{\})\end{array}\right\}$

```
//assert(P != B);
//assert(P != F);
//assert(chunksize(P) == small_index2size(I));
if (F == B)
```

$$\left\{\begin{array}{l}\exists x.\, \mathtt{S} = 8\mathtt{I} \,*\, 0 \le \mathtt{I} < 32 \,*\, x = \mathtt{smallbin} + 2\mathtt{I}\mathtt{w} \\ *\; U = \{\} \,*\, \mathtt{F} = \mathtt{B} = x \\ *\; \mathtt{B} \overset{\mathsf{fd}}{\longmapsto} \mathtt{P} \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \mathtt{B} \,*\, \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \mathtt{F} \,*\, \mathtt{F} \overset{\mathsf{bk}}{\longmapsto} \mathtt{P} \,*\, \tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} \mathtt{S}) \\ *\; \mathtt{smallmap}_{[\mathtt{I}]} = (U \uplus \{\mathtt{P} + 2\mathtt{w} \mapsto \mathtt{S} - 1\mathtt{w}\} \neq \{\})\end{array}\right\}$$

```
  clear_smallmap(M, I);
```

$$\left\{\begin{array}{l}\exists x.\, \mathtt{S} = 8\mathtt{I} \,*\, 0 \le \mathtt{I} < 32 \,*\, x = \mathtt{smallbin} + 2\mathtt{I}\mathtt{w} \\ *\; U = \{\} \,*\, x \overset{\mathsf{fd}}{\longmapsto} \_ \,*\, x \overset{\mathsf{bk}}{\longmapsto} \_ \,*\, \mathtt{smallmap}_{[\mathtt{I}]} = (U \neq \{\}) \\ *\; \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \_ \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \_ \,*\, \tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} \mathtt{S})\end{array}\right\}$$

```
else //if (RTCHECK((F == smallbin_at(M,I) || ok_address(M, F)) &&
     // (B == smallbin_at(M,I) || ok_address(M, B)))) {
  F->bk = B;
  B->fd = F;
```

$$\left\{\begin{array}{l}\exists x, U_1, U_2.\, \mathtt{S} = 8\mathtt{I} \,*\, 0 \le \mathtt{I} < 32 \,*\, x = \mathtt{smallbin} + 2\mathtt{I}\mathtt{w} \\ *\; U = U_1 \uplus U_2 \,*\, U \neq \{\} \\ *\; (\mathtt{B} = x \,*\, U_1 = \{\}) \\ \vee\, (\exists y.\, x \overset{\mathsf{fd}}{\longmapsto} y \,*\, y \overset{\mathsf{bk}}{\longmapsto} x \,*\, (\mathit{bnode}\,|\mathtt{I}|)^*(y, \mathtt{B}, U_1 \uplus\!- \{\mathtt{B} + 2\mathtt{w} \mapsto \_\})) \\ *\; \mathtt{B} \overset{\mathsf{fd}}{\longmapsto} \mathtt{F} \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \mathtt{B} \,*\, \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \mathtt{F} \,*\, \tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} \mathtt{S}) \,*\, \mathtt{F} \overset{\mathsf{bk}}{\longmapsto} \mathtt{B} \,*\, (\mathit{bnode}\,|\mathtt{I}|)^*(\mathtt{F}, x, U_2) \\ *\; \mathtt{smallmap}_{[\mathtt{I}]} = (U \uplus \{\mathtt{P} + 2\mathtt{w} \mapsto \mathtt{S} - 1\mathtt{w}\} \neq \{\})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists x, y, U_1, U_2.\, \mathtt{S} = 8\mathtt{I} \,*\, 0 \le \mathtt{I} < 32 \,*\, x = \mathtt{smallbin} + 2\mathtt{I}\mathtt{w} \\ *\; U = U_1 \uplus U_2 \,*\, U \neq \{\} \,*\, x \overset{\mathsf{fd}}{\longmapsto} y \,*\, y \overset{\mathsf{bk}}{\longmapsto} x \\ *\; (\mathit{bnode}\,|\mathtt{I}|)^*(y, \mathtt{F}, U_1) \\ *\; \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \_ \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \_ \,*\, \tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} \mathtt{S}) \,*\, (\mathit{bnode}\,|\mathtt{I}|)^*(\mathtt{F}, x, U_2) \\ *\; \mathtt{smallmap}_{[\mathtt{I}]} = (U \uplus \{\mathtt{P} + 2\mathtt{w} \mapsto \mathtt{S} - 1\mathtt{w}\} \neq \{\})\end{array}\right\}$$

```
}
// else {
// CORRUPTION_ERROR_ACTION(M);
// }
```

$$\left\{\begin{array}{l}\mathtt{S} = 8\mathtt{I} \,*\, 0 \le \mathtt{I} < 32 \\ *\; \mathit{bin}(|\mathtt{I}|, \mathtt{smallbin} + 2\mathtt{I}\mathtt{w}, U) \,*\, \mathtt{smallmap}_{[\mathtt{I}]} = (U \neq \{\}) \\ *\; \tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} \mathtt{S}) \,*\, \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \_ \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \_\end{array}\right\}$$

$$\left\{\tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} \mathtt{S}) \,*\, \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \_ \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \_ \,*\, \mathit{smallbin}_{\lfloor \mathtt{S}/8 \rfloor}(U)\right\}$$

3.6 unlink_first_small_chunk

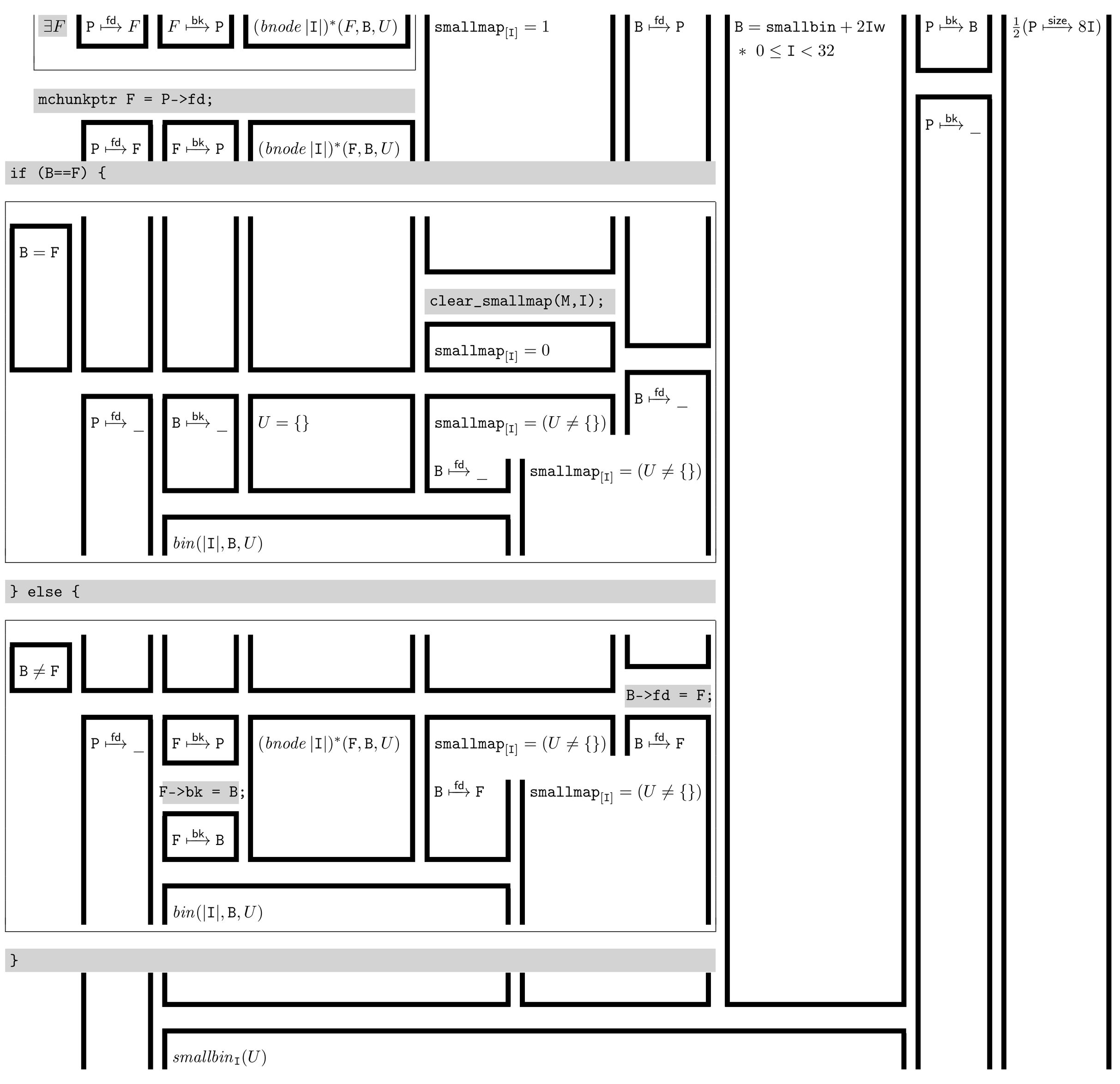
Specification:

$$\left\{\begin{array}{l}\exists F.\, \mathtt{B} = \mathtt{smallbin} + 2\mathtt{I}\mathtt{w} \,*\, 0 \le \mathtt{I} < 32 \\ *\; \mathtt{B} \overset{\mathsf{fd}}{\longmapsto} \mathtt{P} \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \mathtt{B} \,*\, \tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} 8\mathtt{I}) \,*\, \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} F \,*\, F \overset{\mathsf{bk}}{\longmapsto} \mathtt{P} \\ *\; (\mathit{bnode}\,|\mathtt{I}|)^*(F, \mathtt{B}, U) \,*\, \mathtt{smallmap}_{[\mathtt{I}]} = 1\end{array}\right\}$$

```
unlink_first_small_chunk(M, B, P, I) //mods={}
```

$$\left\{\tfrac{1}{2}(\mathtt{P} \overset{\mathsf{size}}{\longmapsto} 8\mathtt{I}) \,*\, \mathtt{P} \overset{\mathsf{fd}}{\longmapsto} \_ \,*\, \mathtt{P} \overset{\mathsf{bk}}{\longmapsto} \_ \,*\, \mathit{smallbin}_{\mathtt{I}}(U)\right\}$$

Verification:



Chapter 4

dlmalloc

Specification:

$$\left\{\mathit{state}(A)\right\}$$

```
dlmalloc(bytes)
```

$$\left\{\begin{array}{l}\exists n.\ n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathit{state}(A \uplus \{\mathtt{ret} \mapsto n\mathtt{w}\})\\ \ast \mathop{\ast}_{i=0}^{n}. \mathtt{ret} + i\mathtt{w} \mapsto \_ \ast \tfrac{1}{2}(\mathtt{ret} - 2\mathtt{w} \xmapsto{\mathsf{size}} \_)\end{array}\right\}$$

Verification:

$$\left\{\mathit{state}(A)\right\}$$

```
void* dlmalloc(size_t bytes) {
#if USE_LOCKS
  ensure_initialization(); /* initialize in sys_alloc if not using locks */
#endif
  if (!PREACTION(gm)) {
    void* mem;
    size_t nb;
    if (bytes <= MAX_SMALL_REQUEST) {
```

$$\left\{\mathit{state}(A) \ast \mathtt{bytes} \leq 244\right\}$$

Allocating small chunks

```
      bindex_t idx;
      binmap_t smallbits;
      nb = (bytes < MIN_REQUEST)? MIN_CHUNK_SIZE : pad_request(bytes);
      idx = small_index(nb);
      smallbits = gm->smallmap >> idx;
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{idx} < 32 \ast \mathtt{smallbits} = \lfloor\mathtt{smallmap}/2^{\mathtt{idx}}\rfloor\\ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
      if ((smallbits & 0x3U) != 0) { /* Remainderless fit to a smallbin. */
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{idx} < 32 \ast \mathtt{smallbits} = \lfloor\mathtt{smallmap}/2^{\mathtt{idx}}\rfloor\\ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\\ \ast \mathtt{smallbits}_{[1,0]} \neq 00\end{array}\right\}$$

‘Remainderless’ fit to a smallbin

```
        mchunkptr b, p;
        idx += ~smallbits & 1; /* Uses next bin if idx empty */
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32 \ast \mathtt{smallmap}_{[\mathtt{idx}]} = 1\\ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        b = smallbin_at(gm, idx);
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32 \ast \mathtt{smallmap}_{[\mathtt{idx}]} = 1\\ \ast \mathtt{b} = \mathtt{smallbins} + 8\mathtt{idx} \ast \mathit{bin}(|\mathtt{idx}|, \mathtt{b}, U_{\mathtt{idx}}) \ast U_{\mathtt{idx}} \neq \{\}\\ \ast \mathop{\ast}_{i\in[0..32)-\mathtt{idx}}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        // rename U_idx to U_idx++[p+2w->8idx-1w]
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, p, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{p + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \mathtt{smallmap}_{[\mathtt{idx}]} = 1 \ast \mathtt{b} = \mathtt{smallbins} + 8\mathtt{idx}\\ \ast \mathtt{b} \xmapsto{\mathsf{fd}} p \ast p \xmapsto{\mathsf{bk}} \mathtt{b} \ast (\mathit{bnode}\,|\mathtt{idx}|)^*(p, \mathtt{b}, U_{\mathtt{idx}} \uplus \{p + 2\mathtt{w} \mapsto 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathop{\ast}_{i\in[0..32)-\mathtt{idx}}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        p = b->fd;
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n, F.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \mathtt{smallmap}_{[\mathtt{idx}]} = 1 \ast \mathtt{b} = \mathtt{smallbins} + 8\mathtt{idx}\\ \ast \mathtt{b} \xmapsto{\mathsf{fd}} \mathtt{p} \ast \mathtt{p} \xmapsto{\mathsf{bk}} \mathtt{b} \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} F \ast F \xmapsto{\mathsf{bk}} \mathtt{p} \ast (\mathit{bnode}\,|\mathtt{idx}|)^*(F, \mathtt{b}, U_{\mathtt{idx}})\\ \ast \mathop{\ast}_{i\in[0..32)-\mathtt{idx}}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        //assert(chunksize(p) == small_index2size(idx));
        unlink_first_small_chunk(gm, b, p, idx);
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast \mathit{block}^*(\mathtt{start}, \mathtt{p}, B_1) \ast \mathit{ublock}(\mathtt{p}, \mathtt{p} + 8\mathtt{idx}, \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast \mathit{block}^*(\mathtt{start}, \mathtt{p}, B_1) \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2)\\ \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        // use Lemma 1
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\}) \ast \mathit{ablock}(q, \mathtt{p}, q + 2\mathtt{w} \mapsto m\mathtt{w})))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q) \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1\\ \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q)\\ \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        set_inuse_and_pinuse(gm, p, small_index2size(idx));
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q)\\ \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q)\\ \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast \mathit{block}^*(\mathtt{start}, \mathtt{p}, B_1) \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2)\\ \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{prevfoot}} 8\mathtt{idx} \ast \mathop{\ast}_{i=4}^{2\mathtt{idx}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w} \ast 2 \leq \mathtt{idx} < 32\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast \mathit{block}^*(\mathtt{start}, \mathtt{p}, B_1) \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2)\\ \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1\\ \ast \mathop{\ast}_{i=2}^{n+2}. \mathtt{p} + i\mathtt{w} \mapsto \_ \ast \mathop{\ast}_{i=n+2}^{2\mathtt{idx}+1}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{idx} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast \mathit{block}^*(\mathtt{start}, \mathtt{p}, B_1) \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{idx}, \mathtt{top}, B_2)\\ \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \mathit{ablock}(\mathtt{p}, \mathtt{p} + 8\mathtt{idx}, \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{a}} n\mathtt{w}\}) \ast \mathop{\ast}_{i=2}^{n+2}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{idx}) \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{a}} n\mathtt{w}\})\\ \ast \mathop{\ast}_{i=2}^{n+2}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} \_) \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists n.\ n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathit{state}(A \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto n\mathtt{w}\})\\ \ast \mathop{\ast}_{i=0}^{n}. \mathtt{p} + 2\mathtt{w} + i\mathtt{w} \mapsto \_ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} \_)\end{array}\right\}$$

```
        mem = chunk2mem(p);
        //check_malloced_chunk(gm, mem, nb);
```

$$\left\{\begin{array}{l}\exists n.\ n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathit{state}(A \uplus \{\mathtt{mem} \mapsto n\mathtt{w}\})\\ \ast \mathop{\ast}_{i=0}^{n}. \mathtt{mem} + i\mathtt{w} \mapsto \_ \ast \tfrac{1}{2}(\mathtt{mem} - 2\mathtt{w} \xmapsto{\mathsf{size}} \_)\end{array}\right\}$$

```
        goto postaction;
      }
      else if (nb > gm->dvsize) {
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{idx} < 32 \ast \mathtt{smallbits} = \lfloor\mathtt{smallmap}/2^{\mathtt{idx}}\rfloor\\ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
        if (smallbits != 0) { /* Use chunk in next nonempty smallbin */
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{idx} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{idx} < 32 \ast \mathtt{smallbits} = \lfloor\mathtt{smallmap}/2^{\mathtt{idx}}\rfloor \ast \mathtt{smallmap} \geq 2^{\mathtt{idx}}\\ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

‘Remainderful’ fit to a smallbin

```
          mchunkptr b, p, r;
          size_t rsize;
          bindex_t i;
          binmap_t leftbits = (smallbits << idx) & left_bits(idx2bit(idx));
          binmap_t leastbit = least_bit(leftbits);
          compute_bit2idx(leastbit, i);
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \mathtt{smallmap}_{[\mathtt{i}]} = 1\\ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
          b = smallbin_at(gm, i);
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}) \ast \mathtt{least\_addr} = 5\mathtt{w}\\ \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \mathtt{smallmap}_{[\mathtt{i}]} = 1\\ \ast \mathtt{b} = \mathtt{smallbins} + 8\mathtt{i} \ast \mathit{bin}(|\mathtt{i}|, \mathtt{b}, U_{\mathtt{i}}) \ast U_{\mathtt{i}} \neq \{\}\\ \ast \mathop{\ast}_{i\in[0..32)-\mathtt{i}}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
          // rename U_idx to U_idx++[p+2w->8i-1w]
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, p, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{p + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \mathtt{smallmap}_{[\mathtt{i}]} = 1 \ast \mathtt{b} = \mathtt{smallbins} + 8\mathtt{i}\\ \ast \mathtt{b} \xmapsto{\mathsf{fd}} p \ast p \xmapsto{\mathsf{bk}} \mathtt{b} \ast (\mathit{bnode}\,|\mathtt{i}|)^*(p, \mathtt{b}, U_{\mathtt{i}} \uplus \{p + 2\mathtt{w} \mapsto 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathop{\ast}_{i\in[0..32)-\mathtt{i}}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
          p = b->fd;
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n, F.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \mathtt{smallmap}_{[\mathtt{i}]} = 1 \ast \mathtt{b} = \mathtt{smallbins} + 8\mathtt{i}\\ \ast \mathtt{b} \xmapsto{\mathsf{fd}} \mathtt{p} \ast \mathtt{p} \xmapsto{\mathsf{bk}} \mathtt{b} \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{i}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} F \ast F \xmapsto{\mathsf{bk}} \mathtt{p} \ast (\mathit{bnode}\,|\mathtt{i}|)^*(F, \mathtt{b}, U_{\mathtt{i}})\\ \ast \mathop{\ast}_{i\in[0..32)-\mathtt{i}}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
          //assert(chunksize(p) == small_index2size(i));
          unlink_first_small_chunk(gm, b, p, i);
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, n.\ \mathit{arena}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{i}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
          //... as before ...
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q)\\ \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{i}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{i}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0\\ \ast \mathtt{p} + 8\mathtt{i} \xmapsto{\mathsf{prevfoot}} 8\mathtt{i} \ast \mathop{\ast}_{i=4}^{2\mathtt{i}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{i}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\end{array}\right\}$$

```
          rsize = small_index2size(i) - nb;
          /* Fit here cannot be remainderless if 4byte sizes */
          if (SIZE_T_SIZE != 4 && rsize < MIN_CHUNK_SIZE)
```

$$\left\{\mathsf{false}\right\}$$

```
            set_inuse_and_pinuse(gm, p, small_index2size(i));
          else {
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q)\\ \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{i}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{i}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0\\ \ast \mathtt{p} + 8\mathtt{i} \xmapsto{\mathsf{prevfoot}} 8\mathtt{i} \ast \mathop{\ast}_{i=4}^{2\mathtt{i}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} 8\mathtt{i}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\\ \ast \mathtt{rsize} = 8\mathtt{i} - \mathtt{nb}\end{array}\right\}$$

```
            set_size_and_pinuse_of_inuse_chunk(gm, p, nb);
            r = chunk_plus_offset(p, nb);
```

$$\left\{\begin{array}{l}\exists\{U_i \mid i \in [0,63)\}, B_1, B_2, n.\ \mathit{coallesced}(A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}} \uplus \{\mathtt{p} + 2\mathtt{w} \mapsto_{\mathsf{u}} 8\mathtt{i} - 1\mathtt{w}\})\\ \ast \mathtt{start} \xmapsto{\mathsf{prevfoot}} \_ \ast \mathit{ublock}(\mathtt{top}, \mathtt{top} + \mathtt{topsize}, \_)\\ \ast ((\mathtt{start} = \mathtt{p} \ast B_1 = \{\})\\ \vee (\exists q, m.\ \mathtt{start} \xmapsto{\mathsf{pinuse}} 1 \ast \mathit{block}^*(\mathtt{start}, q, B_1 \uplus\!\!- \{q + 2\mathtt{w} \mapsto m\})\\ \ast (m+1)\mathtt{w} \leq \mathtt{p} - q \ast \tfrac{1}{2}(q \xmapsto{\mathsf{size}} \mathtt{p} - q)\\ \ast q \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p} - q \geq 4\mathtt{w} \ast \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathtt{w}+1}. q + i\mathtt{w} \mapsto \_))\\ \ast \mathit{block}^*(\mathtt{p} + 8\mathtt{i}, \mathtt{top}, B_2) \ast B_1 \uplus B_2 = A_{\mathsf{a}} \uplus (\biguplus_{i=0}^{64}. U_i)_{\mathsf{u}}\\ \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{nb}) \ast \mathtt{p} + 8\mathtt{idx} \xmapsto{\mathsf{pinuse}} 0 \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1\\ \ast \mathtt{p} + 8\mathtt{i} \xmapsto{\mathsf{prevfoot}} 8\mathtt{i} \ast \mathop{\ast}_{i=4}^{2\mathtt{i}}. \mathtt{p} + i\mathtt{w} \mapsto \_\\ \ast \mathtt{least\_addr} = 5\mathtt{w} \ast n\mathtt{w} = \lceil\mathtt{bytes}\rceil_{\mathtt{w}} \ast \mathtt{nb} = \max\{16, \lceil\mathtt{bytes}+4\rceil_8\} \ast 8\mathtt{i} \geq (n+1)\mathtt{w}\\ \ast 2 \leq \mathtt{i} < 32 \ast \tfrac{1}{2}(\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{nb}) \ast \mathtt{p} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{p} \xmapsto{\mathsf{bk}} \_ \ast \mathop{\ast}_{i=0}^{32}. \mathit{smallbin}_i(U_i) \ast \mathop{\ast}_{i=0}^{32}. \mathit{treebin}_i(U_{i+32})\\ \ast \mathtt{rsize} = 8\mathtt{i} - \mathtt{nb} \ast \mathtt{r} = \mathtt{p} + \mathtt{nb}\end{array}\right\}$$

$$\left\{\begin{array}{l}P_{small} \wedge P_{nb} \wedge \mathit{flags}(\mathtt{p}) = \blacktriangledown\blacktriangle \wedge \mathit{size}(p) = \mathtt{nb} \wedge \mathtt{rsize} = \mathit{size}(p) - \mathtt{nb}\\ \wedge\, \mathtt{r} = \mathtt{p} + \mathtt{nb}\end{array}\right\}$$

```
            set_size_and_pinuse_of_free_chunk(r, rsize);
```

$$\left\{\begin{array}{l}P_{small} \wedge P_{nb} \wedge \mathit{flags}(\mathtt{p}) = \blacktriangledown\blacktriangle \wedge \mathit{size}(p) = \mathtt{nb} \wedge \mathtt{rsize} = \mathit{size}(p) - \mathtt{nb}\\ \wedge\, \mathtt{r} = \mathtt{p} + \mathtt{nb} \wedge \mathit{flags}(\mathtt{r}) = \triangledown\blacktriangle \wedge \mathit{size}(\mathtt{r}) = \mathtt{rsize}\end{array}\right\}$$

```
            replace_dv(gm, r, rsize);
```

$$\left\{\begin{array}{l}P_{small} \wedge P_{nb} \wedge \mathit{flags}(\mathtt{p}) = \blacktriangledown\blacktriangle \wedge \mathit{size}(p) = \mathtt{nb} \wedge \mathtt{rsize} = \mathit{size}(p) - \mathtt{nb}\\ \wedge\, \mathtt{r} = \mathtt{p} + \mathtt{nb} \wedge \mathit{flags}(\mathtt{r}) = \triangledown\blacktriangle \wedge \mathit{size}(\mathtt{r}) = \mathtt{rsize}\\ \wedge\, \mathtt{dv} = \mathtt{r} \wedge \mathtt{dvsize} = \mathtt{rsize}\end{array}\right\}$$

```
          }
          mem = chunk2mem(p);
          check_malloced_chunk(gm, mem, nb);
```

$$\left\{\begin{array}{l}P_{small} \wedge P_{nb} \wedge \mathit{flags}(\mathtt{p}) = \blacktriangledown\blacktriangle \wedge \mathit{size}(p) = \mathtt{nb} \wedge \mathtt{rsize} = \mathit{size}(p) - \mathtt{nb}\\ \wedge\, \mathtt{r} = \mathtt{p} + \mathtt{nb} \wedge \mathit{flags}(\mathtt{r}) = \triangledown\blacktriangle \wedge \mathit{size}(\mathtt{r}) = \mathtt{rsize} \wedge \mathtt{mem} = \mathtt{p} + 2\end{array}\right\}$$

```
          goto postaction;
        }
```

Using a treebin instead

```
        else if (gm->treemap != 0 && (mem = tmalloc_small(gm, nb)) != 0) {
```

$$\left\{\begin{array}{l}P_{small} \wedge P_{nb} \wedge \mathtt{idx} = \lfloor\mathtt{nb}/8\rfloor \wedge \forall i \in [\mathtt{idx}, 32).\ \mathit{smallbin}(i) = \emptyset\\ \wedge\, \mathtt{mem} = p + 2 \wedge \mathit{flags}(p) = \blacktriangledown\blacktriangle \wedge \mathit{size}(p) \geq \mathtt{nb}\end{array}\right\}$$

```
          check_malloced_chunk(gm, mem, nb);
          goto postaction;
```

```
    }
  }
```

Allocating large chunks

```
  else if (bytes >= MAX_REQUEST)
    {bytes ≥ 2^32 − 63}
    nb = MAX_SIZE_T; /* Too big to allocate. Force failure (in sys alloc) */
    {nb = 2^32 − 1}
  else {
    {P_large} where P_large = 264 < bytes < 2^32 − 63
    nb = pad_request(bytes);
    {P_large ∧ P_nb}
    if (gm->treemap != 0 && (mem = tmalloc_large(gm, nb)) != 0) {
      {P_large ∧ P_nb ∧ mem = p + 2 ∧ flags(p) = ▼▲ ∧ size(p) ≥ nb}
      check_malloced_chunk(gm, mem, nb);
      goto postaction;
    }
  }
```

Using the designated victim

```
  {P_nb}
  if (nb <= gm->dvsize) {
    {P_nb ∧ nb ≤ dvsize}
    size_t rsize = gm->dvsize - nb;
    {P_nb ∧ nb ≤ dvsize ∧ rsize = dvsize − nb}
    mchunkptr p = gm->dv;
    {P_nb ∧ nb ≤ size(p) ∧ rsize = size(p) − nb ∧ flags(p) = ▽▲}
    if (rsize >= MIN_CHUNK_SIZE) { /* split dv */
      {P_nb ∧ rsize = size(p) − nb ∧ rsize ≥ 16 ∧ flags(p) = ▽▲}
      mchunkptr r = gm->dv = chunk_plus_offset(p, nb);
      {P_nb ∧ rsize = size(p) − nb ∧ rsize ≥ 16 ∧ r = p + nb ∧ flags(p) = ▽▲}
      gm->dvsize = rsize;
      set_size_and_pinuse_of_free_chunk(r, rsize);
      {P_nb ∧ rsize = size(p) − nb ∧ rsize ≥ 16 ∧ r = p + nb ∧ flags(p) = ▽▲
       ∧ flags(r) = ▽▲ ∧ size(r) = rsize}
      set_size_and_pinuse_of_inuse_chunk(gm, p, nb);
      {P_nb ∧ rsize ≥ 16 ∧ r = p + nb ∧ flags(p) = ▼▲ ∧ size(p) = nb
       ∧ flags(r) = ▽▲ ∧ size(r) = rsize}
    }
    else { /* exhaust dv */
      {P_nb ∧ (size(p) = nb ∨ size(p) = nb + 8) ∧ flags(p) = ▽▲}
      size_t dvs = gm->dvsize;
      gm->dvsize = 0;
      gm->dv = 0;
      set_inuse_and_pinuse(gm, p, dvs);
      {P_nb ∧ (size(p) = nb ∨ size(p) = nb + 8) ∧ flags(p) = ▼▲}
    }
    {P_nb ∧ (size(p) = nb ∨ size(p) = nb + 8) ∧ flags(p) = ▼▲}
    mem = chunk2mem(p);
    check_malloced_chunk(gm, mem, nb);
    {P_nb ∧ (size(p) = nb ∨ size(p) = nb + 8) ∧ flags(p) = ▼▲ ∧ mem = p + 2}
    goto postaction;
  }
```

Using the top chunk

```
  else if (nb < gm->topsize) { /* Split top */
    {P_nb ∧ nb < size(top)}
    size_t rsize = gm->topsize -= nb;
    {P_nb ∧ rsize = size(top) − nb ∧ rsize > 0}
    mchunkptr p = gm->top;
    {P_nb ∧ rsize = size(p) − nb ∧ rsize > 0}
    mchunkptr r = gm->top = chunk_plus_offset(p, nb);
    {P_nb ∧ rsize = size(p) − nb ∧ rsize > 0 ∧ r = p + nb}
    r->head = rsize | PINUSE_BIT;
    {P_nb ∧ size(r) = size(p) − nb ∧ size(r) > 0 ∧ flags(r) = ▽▲ ∧ r = p + nb}
    set_size_and_pinuse_of_inuse_chunk(gm, p, nb);
    {P_nb ∧ size(r) = nb ∧ flags(p) = ▼▲ ∧ size(r) > 0 ∧ flags(r) = ▽▲ ∧ r = p + nb}
    mem = chunk2mem(p);
    {P_nb ∧ size(p) = nb ∧ flags(p) = ▼▲ ∧ mem = p + 2}
    check_top_chunk(gm, gm->top);
    check_malloced_chunk(gm, mem, nb);
    goto postaction;
  }
```

Obtaining memory from the system

```
  mem = sys_alloc(gm, nb);
 postaction:
  POSTACTION(gm);
  return mem;
 }
 return 0;
}
```