A proof of Doug Lea's memory manager

John Wickerson

February 21, 2011

Chapter 1

Glossary of macros, typedefs and minor routines

`MALLOC_ALIGNMENT`	=	8
`MAX_SIZE_T`	=	$FFFF\ FFFF_h$
`SIZE_T_SIZE`	=	4
`SIZE_T_BITSIZE`	=	32
`SIZE_T_ZERO`	=	0
`SIZE_T_ONE`	=	1
`SIZE_T_TWO`	=	2
`SIZE_T_FOUR`	=	4
`TWO_SIZE_T_SIZES`	=	8
`FOUR_SIZE_T_SIZES`	=	16
`SIX_SIZE_T_SIZES`	=	24
`HALF_MAX_SIZE_T`	=	$7FFF\ FFFF_h$
`CHUNK_ALIGN_MASK`	=	111_b
`mchunk`	=	`struct malloc_chunk`
`mchunkptr`	=	`mchunk*`
`sbinptr`	=	`mchunk*`
`bindex_t`	=	`unsigned int`
`binmap_t`	=	`unsigned int`
`flag_t`	=	`unsigned int`
`MCHUNK_SIZE`	=	16
`CHUNK_OVERHEAD`	=	4
`MIN_CHUNK_SIZE`	=	16
`chunk2mem(p)`	=	$\mathtt{p} + 8$
`mem2chunk(mem)`	=	$\mathtt{mem} - 8$
`MAX_REQUEST`	=	$2^{32} - 63$
`MIN_REQUEST`	=	11
`pad_request(req)`	=	$\lceil \mathtt{req} + 4 \rceil_8$
`request2size(req)`	=	$\max\{16, \lceil \mathtt{req} + 4 \rceil_8\}$

$$\begin{array}{lll}
\texttt{PINUSE\_BIT} & = & 1_b \\
\texttt{CINUSE\_BIT} & = & 10_b \\
\texttt{FLAG4\_BIT} & = & 100_b \\
\texttt{INUSE\_BITS} & = & 11_b \\
\texttt{FLAG\_BITS} & = & 111_b \\
\texttt{cinuse(p)} & = & [\mathtt{p}_{[1]}] == 1 \\
\texttt{pinuse(p)} & = & [\mathtt{p}_{[0]}] == 1 \\
\texttt{is\_inuse(p)} & = & \texttt{is\_mmapped(p)} \vee \texttt{cinuse(p)} \\
\texttt{is\_mmapped(p)} & = & [\mathtt{p}_{[1,0]}] == 00 \\
\texttt{chunksize(p)} & = & [(\mathtt{p}+1)_{[31..3]}000]
\end{array}$$

$$\left\{\mathtt{p}_{[0]} \mapsto \_\right\}\ \texttt{clear\_pinuse(p)}\ \left\{\mathtt{p}_{[0]} \mapsto 0\right\}$$

$$\begin{array}{lll}
\texttt{chunk\_plus\_offset(p,s)} & = & p+s \\
\texttt{chunk\_minus\_offset(p,s)} & = & p-s \\
\texttt{next\_chunk(p)} & = & \mathit{next}(\mathtt{p}) \\
\texttt{prev\_chunk(p)} & = & \mathit{prev}(\mathtt{p}) \\
\texttt{next\_pinuse(p)} & = & \mathit{flags}(\mathit{next}(\mathtt{p})) = \_\blacktriangle \\
\texttt{get\_foot(p,s)} & = & \mathit{prev\_foot}(\mathtt{p}+\mathtt{s})
\end{array}$$

$$\left\{\mathit{prev\_foot}(\mathtt{p}+\mathtt{s}) = \_\right\}\ \texttt{set\_foot(p,s)}\ \left\{\mathit{prev\_foot}(\mathtt{p}+\mathtt{s}) = \mathtt{s}\right\}$$

$$\left\{\begin{array}{l} \mathit{size}(\mathtt{p}) = \_ \wedge \mathit{flags}(\mathtt{p}) = \_\_ \\ \wedge\, \mathit{prev\_foot}(\mathtt{p}+\mathtt{s}) = \_ \end{array}\right\}\ \texttt{set\_size\_and\_pinuse\_of\_free\_chunk(p,s)}\ \left\{\begin{array}{l} \mathit{size}(\mathtt{p}) = \mathtt{s} \wedge \mathit{flags}(\mathtt{p}) = {}^{\triangledown}\blacktriangle \\ \wedge\, \mathit{prev\_foot}(\mathit{next}(\mathtt{p})) = \mathtt{s} \end{array}\right\}$$

$$\left\{\begin{array}{l} \mathit{size}(\mathtt{p}) = \_ \wedge \mathit{flags}(\mathtt{p}) = \_\_ \\ \wedge\, \mathit{prev\_foot}(\mathtt{p}+\mathtt{s}) = \_ \\ \wedge\, \mathit{flags}(\mathtt{p}+\mathtt{s}) = \_\_ \end{array}\right\}\ \texttt{set\_free\_with\_pinuse(p,s,n)}\ \left\{\begin{array}{l} \mathit{size}(\mathtt{p}) = \mathtt{s} \wedge \mathit{flags}(\mathtt{p}) = {}^{\triangledown}\blacktriangle \\ \wedge\, \mathit{prev\_foot}(\mathit{next}(\mathtt{p})) = \mathtt{s} \\ \wedge\, \mathit{flags}(\mathit{next}(\mathtt{p})) = \_\triangle \end{array}\right\}$$

$$\begin{array}{lll}
\texttt{tchunk} & = & \texttt{malloc\_tree\_chunk} \\
\texttt{tchunkptr} & = & \texttt{tchunk*} \\
\texttt{tbinptr} & = & \texttt{tchunk*} \\
\texttt{leftmost\_child(t)} & = & \begin{cases} \mathit{child}_0(*\mathtt{t}) & \text{if } \mathit{child}_0(*\mathtt{t}) \neq 0 \\ \mathit{child}_1(*\mathtt{t}) & \text{otherwise} \end{cases} \\
\texttt{NSMALLBINS} & = & 32 \\
\texttt{NTREEBINS} & = & 32 \\
\texttt{SMALLBIN\_SHIFT} & = & 3 \\
\texttt{SMALLBIN\_WIDTH} & = & 8 \\
\texttt{TREEBIN\_SHIFT} & = & 8 \\
\texttt{MIN\_LARGE\_SIZE} & = & 256 \\
\texttt{MAX\_SMALL\_SIZE} & = & 255 \\
\texttt{MAX\_SMALL\_REQUEST} & = & 244 \\
\texttt{mstate} & = & \texttt{struct malloc\_state} \\
\texttt{mparams} & = & \texttt{struct malloc\_params} \\
\texttt{is\_small(s)} & = & \mathtt{s} < 256 \\
\texttt{small\_index(s)} & = & \lfloor \mathtt{s}/8 \rfloor \\
\texttt{small\_index2size(i)} & = & 8 \times \mathtt{i} \\
\texttt{MIN\_SMALL\_INDEX} & = & 2
\end{array}$$

$$\left\{\texttt{smallbins}[2\texttt{i}+2] \mapsto C_1 * \texttt{smallbins}[2\texttt{i}+3] \mapsto C_2\right\}\ \texttt{x := smallbin\_at(M,i)}\ \left\{\texttt{x.fd} \mapsto C_1 * \texttt{x.bk} \mapsto C_2\right\}$$

$$\texttt{treebin\_at(M,i)} = \texttt{treebins}[\texttt{i}]$$

$$\left\{\texttt{I} = \_\right\}\ \texttt{compute\_tree\_index(S,I)}\ \left\{\texttt{I} = \begin{cases} 0 & \text{if } \texttt{S} < 256 \\ 31 & \text{if } \texttt{S} > 2^{24} \\ 2(\log_2 \llbracket \texttt{S} \rrbracket - 8) & \text{if } 0 \leq \{\!\{\texttt{S}\}\!\} < \frac{1}{2}\llbracket \texttt{S} \rrbracket \\ 2(\log_2 \llbracket \texttt{S} \rrbracket - 8) + 1 & \text{if } \frac{1}{2}\llbracket \texttt{S} \rrbracket \leq \{\!\{\texttt{S}\}\!\} < \llbracket \texttt{S} \rrbracket \end{cases}\right\}$$

$$\texttt{bin\_for\_tree\_index(i)} = \begin{cases} 31 & \text{if } \texttt{i} = 31 \\ \lfloor \texttt{i}/2 \rfloor + 6 & \text{otherwise} \end{cases}$$

$$\texttt{leftshift\_for\_tree\_index(i)} = \begin{cases} 0 & \text{if } \texttt{i} = 31 \\ 25 - \lfloor \texttt{i}/2 \rfloor & \text{otherwise} \end{cases}$$

$$\texttt{minsize\_for\_tree\_index(i)} = \begin{cases} 2 \ll (\lfloor \texttt{i}/2 \rfloor + 7) & \text{if } \texttt{i} \text{ even} \\ 3 \ll (\lfloor \texttt{i}/2 \rfloor + 7) & \text{if } \texttt{i} \text{ odd} \end{cases}$$

$$\texttt{idx2bit(i)} = 1 \ll \texttt{i}$$

$$\left\{\texttt{smallmap}[\texttt{i}] = \_\right\}\ \texttt{mark\_smallmap(M,i)}\ \left\{\texttt{smallmap}[\texttt{i}] = 1\right\}$$

$$\left\{\texttt{smallmap}[\texttt{i}] = \_\right\}\ \texttt{clear\_smallmap(M,i)}\ \left\{\texttt{smallmap}[\texttt{i}] = 0\right\}$$

$$\texttt{smallmap\_is\_marked(M,i)} = \texttt{smallmap}[\texttt{i}] = 1$$

$$\left\{\texttt{treemap}[\texttt{i}] = \_\right\}\ \texttt{mark\_treemap(M,i)}\ \left\{\texttt{treemap}[\texttt{i}] = 1\right\}$$

$$\left\{\texttt{treemap}[\texttt{i}] = \_\right\}\ \texttt{clear\_treemap(M,i)}\ \left\{\texttt{treemap}[\texttt{i}] = 0\right\}$$

$$\texttt{treemap\_is\_marked(M,i)} = \texttt{treemap}[\texttt{i}] = 1$$

$$\texttt{least\_bit(x)} = \begin{cases} \mathbf{0}\,\overset{i}{1}\,\mathbf{0} & \text{if } \texttt{x}_i = 1 \wedge \forall j < i.\, \texttt{x}_j = 0\} \\ \mathbf{0} & \text{if } \texttt{x}{=}0 \end{cases}$$

$$\texttt{left\_bits(x)} = \begin{cases} \mathbf{1}\,\overset{i}{0}\,\mathbf{0} & \text{if } \texttt{x}_i = 1 \wedge \forall j < i.\, \texttt{x}_j = 0\} \\ \mathbf{0} & \text{if } \texttt{x} = 0 \end{cases}$$

$$\texttt{same\_or\_left\_bits(x)} = \begin{cases} \mathbf{1}\,\overset{i}{1}\,\mathbf{0} & \text{if } \texttt{x}_i = 1 \wedge \forall j < i.\, \texttt{x}_j = 0\} \\ \mathbf{0} & \text{if } \texttt{x} = 0 \end{cases}$$

$$\left\{\texttt{I} = \_\right\}\ \texttt{compute\_bit2idx(X,I)}\ \left\{\texttt{X} \neq \texttt{0} \Rightarrow \texttt{I} = \log_2 \texttt{X}\right\}$$

$$\left\{p\right\}\ \texttt{mark\_inuse\_foot(M,p,s)}\ \left\{p\right\}$$

$$\left\{\begin{array}{l} \mathit{size}(\texttt{p}) = \_ \wedge \mathit{flags}(\texttt{p}) = \_P \\ \wedge\, \mathit{flags}(\texttt{p}+\texttt{s}) = C\_ \end{array}\right\}\ \texttt{set\_inuse(M,p,s)}\ \left\{\begin{array}{l} \mathit{size}(\texttt{p}) = \texttt{s} \wedge \mathit{flags}(\texttt{p}) = \blacktriangledown P \\ \wedge\, \mathit{flags}(\mathit{next}(\texttt{p})) = C\blacktriangle \end{array}\right\}$$

$$\left\{\begin{array}{l} \mathit{size}(\texttt{p}) = \_ \wedge \mathit{flags}(\texttt{p}) = \_\_ \\ \wedge\, \mathit{flags}(\texttt{p}+\texttt{s}) = C\_ \end{array}\right\}\ \texttt{set\_inuse\_and\_pinuse(M,p,s)}\ \left\{\begin{array}{l} \mathit{size}(\texttt{p}) = \texttt{s} \wedge \mathit{flags}(\texttt{p}) = \blacktriangledown\blacktriangle \\ \wedge\, \mathit{flags}(\mathit{next}(\texttt{p})) = C\blacktriangle \end{array}\right\}$$

$$\left\{\begin{array}{l} \mathit{size}(\texttt{p}) = \_ \\ \wedge\, \mathit{flags}(\texttt{p}) = \_\_ \end{array}\right\}\ \texttt{set\_inuse\_and\_pinuse\_of\_inuse\_chunk(M,p,s)}\ \left\{\begin{array}{l} \mathit{size}(\texttt{p}) = \texttt{s} \\ \wedge\, \mathit{flags}(\texttt{p}) = \blacktriangledown\blacktriangle \end{array}\right\}$$

Chapter 2

State

Shorthand:

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

Predicates:

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

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:

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \_ \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} \_ \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} \_ \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{pinuse}} \_\right\}$$

```
set_inuse_and_pinuse(M,p,s)
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{pinuse}} 1\right\}$$

Verification:

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \_ \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} \_ \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} \_ \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{pinuse}} \_\right\}$$

```
p->head = (s|PINUSE_BIT|CINUSE_BIT);
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{pinuse}} \_\right\}$$

```
((mchunkptr)(((char*)p) + s))->head |= PINUSE_BIT;
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 1 \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{pinuse}} 1\right\}$$

3.2 `set_size_and_pinuse_of_free_chunk`

Specification:

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \_ \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} \_ \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} \_ \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{prevfoot}} \_\right\}$$

```
set_size_and_pinuse_of_free_chunk(p,s)
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{prevfoot}} \mathtt{s}\right\}$$

Verification:

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \_ \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} \_ \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} \_ \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{prevfoot}} \_\right\}$$

```
p->head = (s|PINUSE_BIT);
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{prevfoot}} \_\right\}$$

```
set_foot(p,s);
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \ast \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \ast \mathtt{p} \xmapsto{\mathsf{cinuse}} 0 \ast \mathtt{p}+\mathtt{s} \xmapsto{\mathsf{prevfoot}} \mathtt{s}\right\}$$

3.3 `set_size_and_pinuse_of_inuse_chunk`

Specification:

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \_ \;*\; \mathtt{p} \xmapsto{\mathsf{pinuse}} \_ \;*\; \mathtt{p} \xmapsto{\mathsf{cinuse}} \_\right\}$$

```
set_size_and_pinuse_of_inuse_chunk(M,p,s)
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \;*\; \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \;*\; \mathtt{p} \xmapsto{\mathsf{cinuse}} 1\right\}$$

Verification:

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \_ \;*\; \mathtt{p} \xmapsto{\mathsf{pinuse}} \_ \;*\; \mathtt{p} \xmapsto{\mathsf{cinuse}} \_\right\}$$

```
p->head = (s|PINUSE_BIT|CINUSE_BIT);
```

$$\left\{\mathtt{p} \xmapsto{\mathsf{size}} \mathtt{s} \;*\; \mathtt{p} \xmapsto{\mathsf{pinuse}} 1 \;*\; \mathtt{p} \xmapsto{\mathsf{cinuse}} 1\right\}$$

3.4 insert_small_chunk

Specification:

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

```
insert_small_chunk(M,P,S) //mods={}
```

$$\left\{\mathit{smallbin}_{\lfloor \mathtt{S}/8 \rfloor}(U \uplus \{\mathtt{P} + 2\mathtt{w} \mapsto \mathtt{S} - 1\mathtt{w}\})\right\}$$

Verification:

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

```
bindex_t I = small_index(S);
```

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

```
mchunkptr B = smallbin_at(M, I);
```

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

```
mchunkptr F = B;
```

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

```
//assert(S >= MIN_CHUNK_SIZE);
if (!smallmap_is_marked(M, I))
```

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

```
  mark_smallmap(M, I);
```

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

```
else //if (RTCHECK(ok_address(M, B->fd)))
```

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

```
  F = B->fd;
```

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

```
// else {
```

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

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

```
B->fd = P;
F->bk = P;
P->fd = F;
P->bk = B;
```

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

$$\left\{\begin{array}{l}\exists i.\, \mathsf{S} = 8i \;*\; \mathsf{B} = \mathtt{smallbin} + 2i \;*\; 0 \leq i < 32 \;*\; \mathsf{B} \xmapsto{\mathsf{fd}} \mathsf{P} \;*\; \mathsf{P} \xmapsto{\mathsf{bk}} \mathsf{B} \\ *\; (\mathit{bnode}\,|i|)^*(\mathsf{P}, \mathsf{B}, U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\}) \;*\; \mathtt{smallmap}_{[i]} = 1\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists i.\, \mathsf{S} = 8i \;*\; 0 \leq i < 32 \\ *\; \mathit{bin}(|i|, \mathtt{smallbin} + 2i, U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\}) \\ *\; \mathtt{smallmap}_{[i]} = (U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\} \neq \{\})\end{array}\right\}$$

$$\left\{\mathit{smallbin}_{\lfloor \mathsf{S}/8 \rfloor}(U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\})\right\}$$

3.5 unlink_small_chunk

Specification:

$$\left\{\mathit{smallbin}_{\lfloor \mathsf{S}/8 \rfloor}(U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\})\right\}$$

```
unlink_small_chunk(M,P,S) //mods={}
```

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

Verification:

$$\left\{\mathit{smallbin}_{\lfloor \mathsf{S}/8 \rfloor}(U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\})\right\}$$

$$\left\{\begin{array}{l}\exists i, x.\, \mathsf{S} = 8i \;*\; 0 \leq i < 32 \;*\; x = \mathtt{smallbin} + 2i\mathsf{w} \\ *\; \mathit{bin}(|i|, x, U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\}) \\ *\; \mathtt{smallmap}_{[i]} = (U \uplus \{\mathsf{P} + 2\mathsf{w} \mapsto \mathsf{S} - 1\mathsf{w}\} \neq \{\})\end{array}\right\}$$

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

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

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

```
mchunkptr F = P->fd;
mchunkptr B = P->bk;
bindex_t I = small_index(S);
```

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

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

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

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

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

```
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;
```

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

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

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

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

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

3.6 unlink_first_small_chunk

Specification:

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

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

$$\left\{\tfrac{1}{2}(\mathtt{P} \xmapsto{\mathsf{size}} 8\mathtt{I}) \ast \mathtt{P} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{P} \xmapsto{\mathsf{bk}} \_ \ast \mathit{smallbin}_{\mathtt{I}}(U)\right\}$$

Verification:

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

```
mchunkptr F = P->fd;
//assert(P != B);
//assert(P != F);
//assert(chunksize(P) == small_index2size(I));
```

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

```
if (B == F)
  clear_smallmap(M, I);
```

$$\left\{\begin{array}{l}\mathtt{B} = \mathtt{smallbin} + 2\mathtt{Iw} \ast 0 \le \mathtt{I} < 32\\ \ast\ \mathtt{B} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{B} \xmapsto{\mathsf{bk}} \_ \ast U = \{\}\\ \ast\ \mathtt{smallmap}_{[\mathtt{I}]} = (U \neq \{\}) \ast \tfrac{1}{2}(\mathtt{P} \xmapsto{\mathsf{size}} 8\mathtt{I}) \ast \mathtt{P} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{P} \xmapsto{\mathsf{bk}} \_\end{array}\right\}$$

```
else //if (RTCHECK(ok_address(M, F))) {
```

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

```
  B->fd = F;
  F->bk = B;
```

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

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

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

$$\left\{\tfrac{1}{2}(\mathtt{P} \xmapsto{\mathsf{size}} 8\mathtt{I}) \ast \mathtt{P} \xmapsto{\mathsf{fd}} \_ \ast \mathtt{P} \xmapsto{\mathsf{bk}} \_ \ast \mathit{smallbin}_{\mathtt{I}}(U)\right\}$$

Chapter 4

dlmalloc

Specification:

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

```
dlmalloc(bytes)
```

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

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) {
```

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

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;
```

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

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

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

‘Remainderless’ fit to a smallbin

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

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

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

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

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

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

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

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

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

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

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

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

```
// use Lemma 1
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

‘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);
```

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

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

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

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

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

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

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

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

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

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

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

```
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\mathsf{w} \mapsto_{\mathsf{u}} 8\mathtt{i}-1\mathsf{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 \mathbin{\uplus\!\!-} \{q+2\mathsf{w} \mapsto m\}) \\
\ast\ (m+1)\mathsf{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\mathsf{w} \ \ast\ \mathop{\ast}_{i=m+2}^{(\mathtt{p}-q)/\mathsf{w}+1}. q + i\mathsf{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\mathsf{w} \mapsto \_ \\
\ast\ \mathtt{least\_addr} = 5\mathsf{w} \ \ast\ n\mathsf{w} = \lceil \mathtt{bytes} \rceil_{\mathsf{w}} \ \ast\ \mathtt{nb} = \max\{16, \lceil \mathtt{bytes}+4 \rceil_8\} \ \ast\ 8\mathtt{i} \geq (n+1)\mathsf{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);
```

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

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

```
      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)
```

$$\left\{\mathtt{bytes} \geq 2^{32} - 63\right\}$$

```
  nb = MAX_SIZE_T; /* Too big to allocate. Force failure (in sys alloc) */
```

$$\left\{\mathtt{nb} = 2^{32} - 1\right\}$$

```
else {
  $\left\{P_{large}\right\}$ where $P_{large} = 244 < \mathtt{bytes} < 2^{32} - 63$
  nb = pad_request(bytes);
  $\left\{P_{large} \wedge P_{nb}\right\}$
  if (gm->treemap != 0 && (mem = tmalloc_large(gm, nb)) != 0) {
    $\left\{P_{large} \wedge P_{nb} \wedge \mathtt{mem} = p + 2 \wedge \mathit{flags}(p) = ▼▲ \wedge \mathit{size}(p) \geq \mathtt{nb}\right\}$
    check_malloced_chunk(gm, mem, nb);
    goto postaction;
  }
}
```

Using the designated victim

```
$\left\{P_{nb}\right\}$
if (nb <= gm->dvsize) {
  $\left\{P_{nb} \wedge \mathtt{nb} \leq \mathtt{dvsize}\right\}$
  size_t rsize = gm->dvsize - nb;
  $\left\{P_{nb} \wedge \mathtt{nb} \leq \mathtt{dvsize} \wedge \mathtt{rsize} = \mathtt{dvsize} - \mathtt{nb}\right\}$
  mchunkptr p = gm->dv;
  $\left\{P_{nb} \wedge \mathtt{nb} \leq \mathit{size}(\mathtt{p}) \wedge \mathtt{rsize} = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathit{flags}(\mathtt{p}) = ▽▲\right\}$
  if (rsize >= MIN_CHUNK_SIZE) { /* split dv */
    $\left\{P_{nb} \wedge \mathtt{rsize} = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathtt{rsize} \geq 16 \wedge \mathit{flags}(\mathtt{p}) = ▽▲\right\}$
    mchunkptr r = gm->dv = chunk_plus_offset(p, nb);
    $\left\{P_{nb} \wedge \mathtt{rsize} = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathtt{rsize} \geq 16 \wedge \mathtt{r} = \mathtt{p} + \mathtt{nb} \wedge \mathit{flags}(\mathtt{p}) = ▽▲\right\}$
    gm->dvsize = rsize;
    set_size_and_pinuse_of_free_chunk(r, rsize);
    $\left\{P_{nb} \wedge \mathtt{rsize} = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathtt{rsize} \geq 16 \wedge \mathtt{r} = \mathtt{p} + \mathtt{nb} \wedge \mathit{flags}(\mathtt{p}) = ▽▲\right.$
     $\left.\wedge \mathit{flags}(\mathtt{r}) = ▽▲ \wedge \mathit{size}(\mathtt{r}) = \mathtt{rsize}\right\}$
    set_size_and_pinuse_of_inuse_chunk(gm, p, nb);
    $\left\{P_{nb} \wedge \mathtt{rsize} \geq 16 \wedge \mathtt{r} = \mathtt{p} + \mathtt{nb} \wedge \mathit{flags}(\mathtt{p}) = ▼▲ \wedge \mathit{size}(p) = \mathtt{nb}\right.$
     $\left.\wedge \mathit{flags}(\mathtt{r}) = ▽▲ \wedge \mathit{size}(\mathtt{r}) = \mathtt{rsize}\right\}$
  }
  else { /* exhaust dv */
    $\left\{P_{nb} \wedge (\mathit{size}(\mathtt{p}) = \mathtt{nb} \vee \mathit{size}(\mathtt{p}) = \mathtt{nb} + 8) \wedge \mathit{flags}(\mathtt{p}) = ▽▲\right\}$
    size_t dvs = gm->dvsize;
    gm->dvsize = 0;
    gm->dv = 0;
    set_inuse_and_pinuse(gm, p, dvs);
    $\left\{P_{nb} \wedge (\mathit{size}(\mathtt{p}) = \mathtt{nb} \vee \mathit{size}(\mathtt{p}) = \mathtt{nb} + 8) \wedge \mathit{flags}(\mathtt{p}) = ▼▲\right\}$
  }
  $\left\{P_{nb} \wedge (\mathit{size}(\mathtt{p}) = \mathtt{nb} \vee \mathit{size}(\mathtt{p}) = \mathtt{nb} + 8) \wedge \mathit{flags}(\mathtt{p}) = ▼▲\right\}$
  mem = chunk2mem(p);
  check_malloced_chunk(gm, mem, nb);
  $\left\{P_{nb} \wedge (\mathit{size}(\mathtt{p}) = \mathtt{nb} \vee \mathit{size}(\mathtt{p}) = \mathtt{nb} + 8) \wedge \mathit{flags}(\mathtt{p}) = ▼▲ \wedge \mathtt{mem} = \mathtt{p} + 2\right\}$
```

```
      goto postaction;
    }
```

Using the top chunk

```
    else if (nb < gm->topsize) { /* Split top */
      $\left\{P_{nb} \wedge \mathtt{nb} < \mathit{size}(\mathtt{top})\right\}$
      size_t rsize = gm->topsize -= nb;
      $\left\{P_{nb} \wedge \mathtt{rsize} = \mathit{size}(\mathtt{top}) - \mathtt{nb} \wedge \mathtt{rsize} > 0\right\}$
      mchunkptr p = gm->top;
      $\left\{P_{nb} \wedge \mathtt{rsize} = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathtt{rsize} > 0\right\}$
      mchunkptr r = gm->top = chunk_plus_offset(p, nb);
      $\left\{P_{nb} \wedge \mathtt{rsize} = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathtt{rsize} > 0 \wedge \mathtt{r} = \mathtt{p} + \mathtt{nb}\right\}$
      r->head = rsize | PINUSE_BIT;
      $\left\{P_{nb} \wedge \mathit{size}(\mathtt{r}) = \mathit{size}(\mathtt{p}) - \mathtt{nb} \wedge \mathit{size}(\mathtt{r}) > 0 \wedge \mathit{flags}(\mathtt{r}) = \triangledown\blacktriangle \wedge \mathtt{r} = \mathtt{p} + \mathtt{nb}\right\}$
      set_size_and_pinuse_of_inuse_chunk(gm, p, nb);
      $\left\{P_{nb} \wedge \mathit{size}(\mathtt{p}) = \mathtt{nb} \wedge \mathit{flags}(\mathtt{p}) = \blacktriangledown\blacktriangle \wedge \mathit{size}(\mathtt{r}) > 0 \wedge \mathit{flags}(\mathtt{r}) = \triangledown\blacktriangle \wedge \mathtt{r} = \mathtt{p} + \mathtt{nb}\right\}$
      mem = chunk2mem(p);
      $\left\{P_{nb} \wedge \mathit{size}(\mathtt{p}) = \mathtt{nb} \wedge \mathit{flags}(\mathtt{p}) = \blacktriangledown\blacktriangle \wedge \mathtt{mem} = \mathtt{p} + 2\right\}$
      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;
}
```