Verifying Memory Managers

John Wickerson

1 Preliminaries

1.1 Spatial closure operators

Suppose R and S are of type $loc \to loc \to assertion$. Define:

$$\begin{array}{rcl} R;S & \stackrel{\text{def}}{=} & \lambda x\, z.\, \exists y.\, R\, x\, y \;*\; S\, y\, z \\ R \vee S & \stackrel{\text{def}}{=} & \lambda x\, y.\, R\, x\, y \vee S\, x\, y \\ id & \stackrel{\text{def}}{=} & \lambda x\, y.\, x = y \wedge emp \\ R^* & \stackrel{\text{def}}{=} & \mu S.\, S = id \vee R;S \\ R^+ & \stackrel{\text{def}}{=} & R;R^* \end{array}$$

Then the ordinary *list* predicate can be defined like so:

$$list(x) \stackrel{\text{def}}{=} (\lambda x\, y.\, x \mapsto y)^*\, x\, 0$$

Furthermore, we can parameterise the definitions by an element m of a partial commutative monoid (PCM) $(M, \cdot, u)$. Define:

$$\begin{array}{rcl} R;S & \stackrel{\text{def}}{=} & \lambda x\, z\, m.\, \exists y\, m_1\, m_2.\, m = m_1 \cdot m_2 \;*\; R\, x\, y\, m_1 \;*\; S\, y\, z\, m_2 \\ R \vee S & \stackrel{\text{def}}{=} & \lambda x\, y\, m.\, R\, x\, y\, m \vee S\, x\, y\, m \\ id & \stackrel{\text{def}}{=} & \lambda x\, y\, m.\, x = y \wedge m = u \wedge emp \\ R^* & \stackrel{\text{def}}{=} & \mu S.\, S = id \vee R;S \\ R^+ & \stackrel{\text{def}}{=} & R;R^* \end{array}$$

Firstly, using the PCM of sets of naturals, $(\mathcal{P}\,\mathbb{N}, \uplus, \emptyset)$, we can define Bornat-style lists, which are parameterised by the set X of locations through which they pass, like so:

$$blist(x, X) \stackrel{\text{def}}{=} (\lambda x\, y\, X.\, x \mapsto y \wedge X = \{x\})^*\, x\, 0\, X$$

Secondly, using the unique 1-element PCM, $(\{u\}, \lambda\_\ \_.\, u, u)$, the extra parameters become redundant, and can be removed in such a way as to restore the original version above.

Thirdly, we can define an arena that comprises a chain of unallocated, allocated, and system blocks – more on this later.

1.2 Some proof rules

The hypothetical frame rule:

$$\frac{\overline{\Gamma \vdash \{P_i * R\}\, C_i\, \{Q_i * R\}}^{\,i} \qquad \Gamma, \overline{\{P_i\}\, f_i\, \{Q_i\}}^{\,i} \vdash \{P\}\, C\, \{Q\}}{\Gamma \vdash \{P * R\}\, \texttt{let}\ \overline{f_i = C_i}^{\,i}\ \texttt{in}\ C\, \{Q * R\}}\ \textsc{HypFrame}$$

Weakening the environment:

$$\frac{\Gamma' \vdash \{P\}\, C\, \{Q\} \qquad \Gamma \subseteq \Gamma'}{\Gamma \vdash \{P\}\, C\, \{Q\}}\ \Gamma\text{-}\textsc{Weaken}$$

Frame rule

$$\frac{\Gamma \vdash \{P\}\, C\, \{Q\} \qquad R \text{ stable under } \Gamma\, \mathsf{G}}{\Gamma \vdash \{P * R\}\, C\, \{Q * R\}}\ \textsc{Frame}$$

Region update

$$\frac{\Gamma \vdash \{P' * P\}\, C\, \{Q' * Q\} \qquad (P \rightsquigarrow Q) \text{ allowed by } \Gamma\, \mathsf{G} \qquad P, Q \text{ precise}}{\Gamma \vdash \{P' * \boxed{P * R}\}\, C\, \{Q' * \boxed{Q * R}\}}\ \textsc{RegUpdate}$$

Opening and closing a predicate definition

$$\frac{\Gamma(\alpha) = \lambda \overline{x}.\, P}{\Gamma \vdash \alpha(\overline{e}) \Rightarrow P[\overline{e}/\overline{x}]}\ \textsc{Open} \qquad \frac{\Gamma(\alpha) = \lambda \overline{x}.\, P}{\Gamma \vdash P[\overline{e}/\overline{x}] \Rightarrow \alpha(\overline{e})}\ \textsc{Close}$$

2 A variable-sized allocator

External spec

$$\vdash \left\{ emp \right\} \texttt{malloc(n)} \left\{ token\, \texttt{ret}\, \texttt{n} \ *\ \ast_{i=0}^{\texttt{n}-1}.\, (\texttt{ret} + i) \mapsto \_ \right\}$$
$$\vdash \left\{ \exists n.\, token\, \texttt{x}\, n \ *\ \ast_{i=0}^{n-1}.\, (\texttt{x} + i) \mapsto \_ \right\} \texttt{free(x)} \left\{ emp \right\}$$

2.1 Second implementation (Unix V7)

Note that the various 'pure' operators, such as '=' and '>' and 'def(−)', are all given an empty footprint. That is, read $x = 5$ as $x = 5 \wedge emp$.

Internal spec

$$\Gamma \vdash \left\{ anArena \right\} \texttt{malloc(n)} \left\{ \begin{array}{c} anArena \ *\ (token\, \texttt{ret}\, \texttt{n} \ *\ \ast_{i=0}^{\texttt{n}-1}.\, (\texttt{ret} + i) \mapsto \_ \\ \vee\ \texttt{ret} = 0) \end{array} \right\}$$
$$\Gamma \vdash \left\{ anArena \ *\ \exists n.\, token\, \texttt{x}\, n \ *\ \ast_{i=0}^{n-1}.\, (\texttt{x} + i) \mapsto \_ \right\} \texttt{free(x)} \left\{ anArena \right\}$$

where Γ defines:

$$
\begin{array}{rcl}
\mathit{ublock}\,x\,y\,B & \stackrel{\text{def}}{=} & B = \{(x+1) \mapsto_{\mathsf{u}} (y-x-1)\} \;*\; x < y \;*\; x \mapsto y \;*\; \ast_{i=x+1}^{y-1}.\, i \mapsto \_ \\
\mathit{ablock}\,x\,y\,B & \stackrel{\text{def}}{=} & B = \{(x+1) \mapsto_{\mathsf{a}} (y-x-1)\} \;*\; x < y \;*\; x_{|1} \stackrel{.5}{\mapsto} y \\
\mathit{sblock}\,x\,y\,B & \stackrel{\text{def}}{=} & B = \{(x+1) \mapsto_{\mathsf{s}} (y-x-1)\} \;*\; x < y \;*\; x_{|1} \mapsto y \\
\mathit{block} & \stackrel{\text{def}}{=} & \mathit{ublock} \vee \mathit{ablock} \vee \mathit{sblock} \\
\mathit{arena}\ A & \stackrel{\text{def}}{=} & \exists B : \mathcal{B}.\, \exists U, S : \mathbb{N} \rightharpoonup \mathbb{N}_0.\, \exists b. \\
 & & \mathit{block}^*\ \mathtt{s}\,\mathtt{t}\,B \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \;*\; \mathtt{t}_{|1} \mapsto \mathtt{s} \;*\; b > \mathtt{t} \;*\; \mathit{brk}\,b \\
\mathit{anArena} & \stackrel{\text{def}}{=} & \boxed{\exists A.\, \mathit{arena}\,A} \\
\mathit{token}\,x\,n & \stackrel{\text{def}}{=} & \boxed{\exists A.\, \mathit{arena}(A \uplus \{x \mapsto n\})} \;*\; (x-1)_{|1} \stackrel{.5}{\mapsto} (x+n) \\
\mathsf{G} & \stackrel{\text{def}}{=} & \bigcup_x \{\mathit{Malloc}, \mathit{Free}\,x\} \\
\mathit{Malloc} & \stackrel{\text{def}}{=} & \exists A, x, n.\, \mathit{arena}\,A \;\rightsquigarrow\; \mathit{arena}(A \uplus \{x \mapsto n\}) \\
\mathit{Free}\,x & \stackrel{\text{def}}{=} & \exists A, n.\, (x-1)_{|1} \stackrel{.5}{\mapsto} (x+n) \;\mid\; \mathit{arena}(A \uplus \{x \mapsto n\}) \;\rightsquigarrow\; \mathit{arena}\,A
\end{array}
$$

Note that we use the following separation algebra for the spatial closure operators:

$$\mathcal{B} \stackrel{\text{def}}{=} (\mathbb{N} \rightharpoonup \{\mathsf{u}, \mathsf{a}, \mathsf{s}\} \times \mathbb{N}_0, \uplus, \emptyset)$$

Note also that X_{a} tags each of X's values with a, and so on. So $\{2 \mapsto 4, 3 \mapsto 5\}_{\mathsf{a}}$ is $\{2 \mapsto_{\mathsf{a}} 4, 3 \mapsto_{\mathsf{a}} 5\}$.

Verification of malloc routine

```
#define testbusy(p) ((int)(p)&1)
#define setbusy(p) (struct store *)((int)(p)|1)
#define clearbusy(p) (struct store *)((int)(p)&~1)

struct store {struct store *ptr;};
static struct store *s; //arena start
static struct store *t; //arena top


char *malloc(unsigned int nbytes)
```

$\{\mathit{anArena}\}$

$\{\boxed{\exists A.\, \mathit{arena}\,A}\}$

```
// begin Existential
```

$\{\boxed{\mathit{arena}\,A}\}$

```
// begin Malloc action
{
```

$\left\{ arena\, A \right\}$

$$\left\{ \begin{array}{l} \exists B, U, S, b.\ block^*\, \mathtt{s}\, \mathtt{t}\, B \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \end{array} \right\}$$

```
register struct store *p, *q;
register nw;
static temp;
//omitted: code to initialise arena (JW: revisit this decision)
nw=(nbytes+WORD+WORD-1)/WORD; //where WORD=sizeof(struct store)
```

$$\left\{ \begin{array}{l} \exists B, U, S, b.\ block^*\, \mathtt{s}\, \mathtt{t}\, B \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

$$\left\{ \begin{array}{l} \exists B, U, S, b.\ block^*\, \mathtt{s}\, \mathtt{s}\, \emptyset \ *\ block^*\, \mathtt{s}\, \mathtt{t}\, B \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

$$\left\{ \begin{array}{l} \exists B, U, S, b, B_1, B_2. \\ block^*\, \mathtt{s}\, \mathtt{s}\, B_1 \ *\ block^*\, \mathtt{s}\, \mathtt{t}\, B_2 \ *\ B = B_1 \uplus B_2 \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

```
for(p=s; ; ) {
```

$$\left\{ \begin{array}{l} \exists B, U, S, b, B_1, B_2. \\ block^*\, \mathtt{s}\, \mathtt{p}\, B_1 \ *\ block^*\, \mathtt{p}\, \mathtt{t}\, B_2 \ *\ B = B_1 \uplus B_2 \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

```
  for(temp=0; ; ) {
```

$$\left\{ \begin{array}{l} \exists B, U, S, b, B_1, B_2. \\ block^*\, \mathtt{s}\, \mathtt{p}\, B_1 \ *\ block^*\, \mathtt{p}\, \mathtt{t}\, B_2 \ *\ B = B_1 \uplus B_2 \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

```
    if(!testbusy(p->ptr)) {
```

$$\left\{ \begin{array}{l} \exists B, U, S, b, B_1, B_2, q. \\ block^*\, \mathtt{s}\, \mathtt{p}\, B_1 \ *\ ublock\, \mathtt{p}\, q\, \{\mathtt{p} \mapsto_{\mathsf{u}} q - \mathtt{p}\} \ *\ block^*\, q\, \mathtt{t}\, B_2 \\ \ *\ B = B_1 \uplus \{\mathtt{p} \mapsto_{\mathsf{u}} q - \mathtt{p}\} \uplus B_2 \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

```
      while(!testbusy((q=p->ptr)->ptr)) {
```

$$\left\{ \begin{array}{l} \exists B, U, S, b, B_1, B_2, r. \\ block^*\, \mathtt{s}\, \mathtt{p}\, B_1 \ *\ ublock\, \mathtt{p}\, \mathtt{q}\, \{\mathtt{p} \mapsto_{\mathsf{u}} \mathtt{q} - \mathtt{p}\} \ *\ ublock\, \mathtt{q}\, r\, \{\mathtt{q} \mapsto_{\mathsf{u}} r - \mathtt{q}\} \ *\ block^*\, r\, \mathtt{t}\, B_2 \\ \ *\ B = B_1 \uplus \{\mathtt{p} \mapsto_{\mathsf{u}} \mathtt{q} - \mathtt{p}\} \uplus \{\mathtt{q} \mapsto_{\mathsf{u}} r - \mathtt{q}\} \uplus B_2 \ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ \ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \ *\ b > \mathtt{t} \ *\ brk\, b \ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \end{array} \right\}$$

```
        p->ptr = q->ptr; //coalesce consecutive free blocks
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2, r.\\ block^*\,\mathtt{s}\,\mathtt{p}\,B_1 \;*\; ublock\,\mathtt{p}\,r\,\{\mathtt{p}\mapsto_{\mathsf{u}} r-\mathtt{p}\} \;*\; block^*\,r\,\mathtt{t}\,B_2\\ *\;\; B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} r-\mathtt{p}\}\uplus B_2 \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}} \;*\; b>\mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil\end{array}\right\}$$

```
  }
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\\ block^*\,\mathtt{s}\,\mathtt{p}\,B_1 \;*\; ublock\,\mathtt{p}\,\mathtt{q}\,\{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\} \;*\; block^*\,\mathtt{q}\,\mathtt{t}\,B_2\\ *\;\; B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\}\uplus B_2 \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}} \;*\; b>\mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil\end{array}\right\}$$

```
  if(q>=p+nw && p+nw>=p) {
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\\ block^*\,\mathtt{s}\,\mathtt{p}\,B_1 \;*\; ublock\,\mathtt{p}\,\mathtt{q}\,\{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\} \;*\; block^*\,\mathtt{q}\,\mathtt{t}\,B_2\\ *\;\; B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\}\uplus B_2 \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}} \;*\; b>\mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil\\ *\;\; \mathtt{q}\geq \mathtt{p}+\mathtt{nw} \;*\; \mathtt{p}+\mathtt{nw}\geq \mathtt{p}\end{array}\right\}$$

```
    goto found;
```

$$\{\mathsf{false}\}$$

```
  }
}
//p's block is either allocated or too small
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\\ block^*\,\mathtt{s}\,\mathtt{p}\,B_1 \;*\; block^*\,\mathtt{p}\,\mathtt{t}\,B_2 \;*\; B = B_1\uplus B_2 \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}} \;*\; b>\mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil\end{array}\right\}$$

```
q = p;
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\\ block^*\,\mathtt{s}\,\mathtt{q}\,B_1 \;*\; block^*\,\mathtt{q}\,\mathtt{t}\,B_2 \;*\; B = B_1\uplus B_2 \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}} \;*\; b>\mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil \;*\; \mathtt{q}=\mathtt{p}\end{array}\right\}$$

```
p = clearbusy(p->ptr);
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\\ ((\exists B_1, B_2, \tau.\, block^*\,\mathtt{s}\,\mathtt{q}\,B_1 \;*\; block\,\mathtt{q}\,\mathtt{p}\,\{\mathtt{q}\mapsto_\tau \mathtt{p}-\mathtt{q}\}\\ *\;\; block^*\,\mathtt{p}\,\mathtt{t}\,B_2 \;*\; B = B_1\uplus\{\mathtt{q}\mapsto_\tau \mathtt{p}-\mathtt{q}\}\uplus B_2)\\ \vee\,(block^*\,\mathtt{s}\,\mathtt{q}\,B \;*\; \mathtt{q}=\mathtt{t} \;*\; \mathtt{p}=\mathtt{s})) \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}}\\ *\;\; b>\mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil\end{array}\right\}$$

```
if(p>q) {
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2, \tau.\\ block^*\,\mathtt{s}\,\mathtt{q}\,B_1 \;*\; block\,\mathtt{q}\,\mathtt{p}\,\{\mathtt{q}\mapsto_\tau \mathtt{p}-\mathtt{q}\} \;*\; block^*\,\mathtt{p}\,\mathtt{t}\,B_2\\ *\;\; B = B_1 \uplus \{\mathtt{q}\mapsto_\tau \mathtt{p}-\mathtt{q}\} \uplus B_2 \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \;*\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\end{array}\right\}$$

```
  } else if(q!=t || p!=s) {
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\; block^*\,\mathtt{s}\,\mathtt{q}\,B \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s}\\ *\;\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \;*\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\\ *\;\; \mathtt{q} = \mathtt{t} \;*\; \mathtt{p} = \mathtt{s} \;*\; (\mathtt{q} \neq \mathtt{t} \vee \mathtt{p} \neq \mathtt{s})\end{array}\right\}$$

$$\{\mathsf{false}\}$$

```
    return 0;
```

$$\{\mathsf{false}\}$$

```
  } else if(++temp>1) {
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\; block^*\,\mathtt{s}\,\mathtt{q}\,B \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\\ *\;\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \;*\; \mathtt{q} = \mathtt{t} \;*\; \mathtt{p} = \mathtt{s}\end{array}\right\}$$

```
    break;
```

$$\{\mathsf{false}\}$$

```
  }
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\; block^*\,\mathtt{s}\,\mathtt{p}\,B_1 \;*\; block^*\,\mathtt{p}\,\mathtt{t}\,B_2 \;*\; B = B_1 \uplus B_2\\ *\;\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \;*\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\end{array}\right\}$$

```
}
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\; block^*\,\mathtt{s}\,\mathtt{t}\,B \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\\ *\;\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \;*\; \mathtt{p} = \mathtt{s}\end{array}\right\}$$

```
temp = ((nw+BLOCK/WORD)/(BLOCK/WORD))*(BLOCK/WORD);
                                  //where BLOCK defaults to 1024
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\; block^*\,\mathtt{s}\,\mathtt{t}\,B \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\\ *\;\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \;*\; \mathtt{p} = \mathtt{s} \;*\; \mathtt{temp}{>}\mathtt{nw}\end{array}\right\}$$

```
q = (struct store *)sbrk(0);
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\; block^*\,\mathtt{s}\,\mathtt{t}\,B \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\\ *\;\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil \;*\; \mathtt{p} = \mathtt{s} \;*\; \mathtt{temp}{>}\mathtt{nw} \;*\; \mathtt{q} = b\end{array}\right\}$$

```
if(q + temp < q) {
```

$$\left\{\begin{array}{l}\exists B, U, S, b.\; block^*\,\mathtt{s}\,\mathtt{t}\,B \;*\; \mathtt{t}_{|1}\mapsto \mathtt{s} \;*\; B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\\ *\;\; b > \mathtt{t} \;*\; brk\,b \;*\; \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\end{array}\right\}$$

$$\{arena\,A \;*\; 0 = 0\}$$

```
  return 0;
```

$\{\mathsf{false}\}$

}

$\left\{\begin{array}{l}\exists B, U, S, b.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b > \mathtt{t}\ *\ brk\, b\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\ *\ \mathtt{q} = b\end{array}\right\}$

```
q = (struct store *)sbrk(temp * WORD);
```

$\left\{\begin{array}{l}(\exists B, U, S, b.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b > \mathtt{t}\ *\ brk\, b\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\ *\ \mathtt{q} = -1) \\ \vee\ (\exists B, U, S, b.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (b+i) \mapsto \_ \\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ b > \mathtt{t}\ *\ brk(b + \mathtt{temp}) \\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{temp}{>}\mathtt{nw}\ *\ \mathtt{q} = b)\end{array}\right\}$

```
if((INT)q == -1) {
```

$\left\{\begin{array}{l}\exists B, U, S, b.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ b > \mathtt{t} \\ *\ brk\, b\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\ *\ \mathtt{q} = -1\end{array}\right\}$

$\left\{\begin{array}{l}\exists B, U, S, b.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b > \mathtt{t}\ *\ brk\, b\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\end{array}\right\}$

$\{arena\, A\ *\ 0 = 0\}$

```
  return 0;
```

$\{\mathsf{false}\}$

}

$\left\{\begin{array}{l}\exists B, U, S.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (\mathtt{q}+i) \mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s} \\ *\ \mathtt{q} > \mathtt{t}\ *\ brk(\mathtt{q} + \mathtt{temp})\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\end{array}\right\}$

```
t->ptr = q;
```

$\left\{\begin{array}{l}\exists B, U, S.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (\mathtt{q}+i) \mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ \mathtt{t} \mapsto \mathtt{q} \\ *\ \mathtt{q} > \mathtt{t}\ *\ brk(\mathtt{q} + \mathtt{temp})\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\end{array}\right\}$

```
if(q!=t+1) {
```

$\left\{\begin{array}{l}\exists B, U, S.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (\mathtt{q}+i) \mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ \mathtt{t} \mapsto \mathtt{q} \\ *\ \mathtt{q} > \mathtt{t}+1\ *\ brk(\mathtt{q} + \mathtt{temp})\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\end{array}\right\}$

```
  t->ptr = setbusy(t->ptr);
```

$\left\{\begin{array}{l}\exists B, U, S.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (\mathtt{q}+i) \mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ \mathtt{t}_{|1} \mapsto \mathtt{q} \\ *\ \mathtt{q} > \mathtt{t}+1\ *\ brk(\mathtt{q} + \mathtt{temp})\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\end{array}\right\}$

```
  //allocate an sblock
```

$\left\{\begin{array}{l}\exists B, U, S.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (\mathtt{q}+i) \mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ sblock\, \mathtt{t}\, \mathtt{q}\, \{\mathtt{t} \mapsto_{\mathsf{s}} \mathtt{q} - \mathtt{t}\}\ *\ \mathtt{q} > \mathtt{t}+1\ *\ brk(\mathtt{q} + \mathtt{temp}) \\ *\ \mathtt{nw} = 1 + \lceil \frac{\mathtt{nbytes}}{\mathtt{WORD}} \rceil\ *\ \mathtt{p} = \mathtt{s}\ *\ \mathtt{temp}{>}\mathtt{nw}\end{array}\right\}$

```
}
```

```
  // t is either a ublock of size 0 or an sblock
```
$$\left\{\begin{array}{l}\exists B, U, S, \tau.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \ast_{i=0}^{\mathtt{temp}-1}.\ (\mathtt{q}+i)\mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ block\,\mathtt{t}\,\mathtt{q}\,\{\mathtt{t}\mapsto_\tau \mathtt{q}-\mathtt{t}\}\ *\ brk(\mathtt{q}+\mathtt{temp})\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}=\mathtt{s}\ *\ \mathtt{temp}>\mathtt{nw}\end{array}\right\}$$
```
  t = q->ptr = q+temp-1;
```
$$\left\{\begin{array}{l}\exists B, U, S, \tau, u.\ block^*\ \mathtt{s}\ u\ B\ *\ \mathtt{q}<\mathtt{t}\ *\ \mathtt{q}\mapsto \mathtt{t}\ *\ \ast_{i=1}^{\mathtt{t}-\mathtt{q}-1}.\ (\mathtt{q}+i)\mapsto \_\ *\ \mathtt{t}\mapsto \_ \\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ block\,u\,\mathtt{q}\,\{u\mapsto_\tau \mathtt{q}-u\}\ *\ brk(\mathtt{t}+1)\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}=\mathtt{s}\end{array}\right\}$$
```
  //make new unallocated block
```
$$\left\{\begin{array}{l}\exists B, U, S, \tau, u.\ block^*\ \mathtt{s}\ u\ B\ *\ block\,u\,\mathtt{q}\,\{u\mapsto_\tau \mathtt{q}-u\}\ *\ ublock\,\mathtt{q}\,\mathtt{t}\,\{\mathtt{q}\mapsto_{\mathsf{u}} \mathtt{t}-\mathtt{q}\} \\ *\ \mathtt{t}\mapsto \_\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ brk(\mathtt{t}+1)\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}=\mathtt{s}\end{array}\right\}$$
```
  t->ptr = setbusy(s);
```
$$\left\{\begin{array}{l}\exists B, U, S, \tau, u.\ block^*\ \mathtt{s}\ u\ B\ *\ block\,u\,\mathtt{q}\,\{u\mapsto_\tau \mathtt{q}-u\}\ *\ ublock\,\mathtt{q}\,\mathtt{t}\,\{\mathtt{q}\mapsto_{\mathsf{u}} \mathtt{t}-\mathtt{q}\} \\ *\ \mathtt{t}_{|1}\mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ brk(\mathtt{t}+1)\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}=\mathtt{s}\end{array}\right\}$$
```
  // restore loop invariant (JW: make sure they match)
```
$$\left\{\begin{array}{l}\exists B, U, S, b.\ block^*\ \mathtt{s}\ \mathtt{t}\ B\ *\ \mathtt{t}_{|1}\mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}=\mathtt{s}\end{array}\right\}$$
```
}
```
$$\{\mathsf{false}\}$$
```
found:
```
$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\ block^*\ \mathtt{s}\ \mathtt{p}\ B_1\ *\ ublock\,\mathtt{p}\,\mathtt{q}\,\{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\}\ *\ block^*\ \mathtt{q}\ \mathtt{t}\ B_2 \\ *\ B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\} \uplus B_2\ *\ \mathtt{t}_{|1}\mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{q}\geq \mathtt{p}+\mathtt{nw}\ *\ \mathtt{p}+\mathtt{nw}\geq \mathtt{p}\end{array}\right\}$$
```
if(q>p+nw) {
```
$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\ block^*\ \mathtt{s}\ \mathtt{p}\ B_1\ *\ ublock\,\mathtt{p}\,\mathtt{q}\,\{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\}\ *\ block^*\ \mathtt{q}\ \mathtt{t}\ B_2 \\ *\ B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{q}-\mathtt{p}\} \uplus B_2\ *\ \mathtt{t}_{|1}\mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{q}>\mathtt{p}+\mathtt{nw}\ *\ \mathtt{p}+\mathtt{nw}\geq \mathtt{p}\end{array}\right\}$$
```
  (p+nw)->ptr = p->ptr;
```
$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\ block^*\ \mathtt{s}\ \mathtt{p}\ B_1\ *\ \mathtt{p}\mapsto(\mathtt{p}+\mathtt{nw})\ *\ \ast_{i=1}^{\mathtt{nw}-1}.\ (\mathtt{p}+i)\mapsto \_ \\ *\ ublock(\mathtt{p}+\mathtt{nw})\,\mathtt{q}\,\{(\mathtt{p}+\mathtt{nw})\mapsto_{\mathsf{u}} (\mathtt{q}-\mathtt{p}-\mathtt{nw})\}\ *\ block^*\ \mathtt{q}\ \mathtt{t}\ B_2 \\ *\ B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{nw}\} \uplus \{(\mathtt{p}+\mathtt{nw})\mapsto_{\mathsf{u}} (\mathtt{q}-\mathtt{p}-\mathtt{nw})\} \uplus B_2\ *\ \mathtt{t}_{|1}\mapsto \mathtt{s} \\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}}\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}+\mathtt{nw}\geq \mathtt{p}\end{array}\right\}$$
```
}
```
$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\ block^*\ \mathtt{s}\ \mathtt{p}\ B_1\ *\ \mathtt{p}\mapsto(\mathtt{p}+\mathtt{nw})\ *\ \ast_{i=1}^{\mathtt{nw}-1}.\ (\mathtt{p}+i)\mapsto \_ \\ *\ block^*(\mathtt{p}+\mathtt{nw})\,\mathtt{t}\,B_2\ *\ B = B_1 \uplus \{\mathtt{p}\mapsto_{\mathsf{u}} \mathtt{nw}\} \uplus B_2\ *\ \mathtt{t}_{|1}\mapsto \mathtt{s}\ *\ B = U_{\mathsf{u}} \uplus A_{\mathsf{a}} \uplus S_{\mathsf{s}} \\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{nw} = 1+\left\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\right\rceil\ *\ \mathtt{p}+\mathtt{nw}\geq \mathtt{p}\end{array}\right\}$$
```
p->ptr = setbusy(p+nw);
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2.\ block^*\ \mathtt{s}\ \mathtt{p}\ B_1\ *\ ablock\,\mathtt{p}\,(\mathtt{p}+\mathtt{nw})\,\{\mathtt{p}\mapsto_{\mathsf{a}}\mathtt{nw}\}\\ *\ block^*(\mathtt{p}+\mathtt{nw})\,\mathtt{t}\,B_2\ *\ \ast_{i=1}^{\mathtt{nw}-1}.\,(\mathtt{p}+i)\mapsto\_\ *\ \mathtt{p}_{|1}\overset{.5}{\mapsto}(\mathtt{p}+\mathtt{nw})\\ *\ B=B_1\uplus\{\mathtt{p}\mapsto_{\mathsf{a}}\mathtt{nw}\}\uplus B_2\ *\ \mathtt{t}_{|1}\mapsto\mathtt{s}\ *\ B=U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus S_{\mathsf{s}}\\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{nw}=1+\lceil\frac{\mathtt{nbytes}}{\mathtt{WORD}}\rceil\ *\ \mathtt{p}+\mathtt{nw}\geq\mathtt{p}\end{array}\right\}$$

$$\left\{\begin{array}{l}arena(A\uplus\{(\mathtt{p}+1)\mapsto\lceil\mathtt{nbytes}/\mathtt{WORD}\rceil\})\\ *\ \ast_{i=0}^{\lceil\mathtt{nbytes}/\mathtt{WORD}\rceil-1}.\,(\mathtt{p}+1+i)\mapsto\_\ *\ \mathtt{p}_{|1}\overset{.5}{\mapsto}(\mathtt{p}+\mathtt{nw})\end{array}\right\}$$

```
  return((char *)(p+1));
```

$$\{\mathsf{false}\}$$

```
}
```

$$\{\mathsf{false}\}$$

Verification of free routine

```
free(register char *ap)
```

$$\{anArena\ *\ \exists n.\ token\ \mathtt{ap}\,n\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\}$$

$$\left\{\begin{array}{l}\boxed{\exists A.\ arena\,A}\ *\ \exists n.\ \boxed{\exists A.\ arena(A\uplus\{\mathtt{ap}\mapsto n\})}\ *\ (\mathtt{ap}-1)_{|1}\overset{.5}{\mapsto}(\mathtt{ap}+n)\\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\end{array}\right\}$$

$$\{\exists n.\ \boxed{\exists A.\ arena(A\uplus\{\mathtt{ap}\mapsto n\})}\ *\ (\mathtt{ap}-1)_{|1}\overset{.5}{\mapsto}(\mathtt{ap}+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\}$$

```
//begin existential
```

$$\{\boxed{arena(A\uplus\{\mathtt{ap}\mapsto n\})}\ *\ (\mathtt{ap}-1)_{|1}\overset{.5}{\mapsto}(\mathtt{ap}+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\}$$

```
//begin "Free x" action
{
```

$$\{arena(A\uplus\{\mathtt{ap}\mapsto n\})\ *\ (\mathtt{ap}-1)_{|1}\overset{.5}{\mapsto}(\mathtt{ap}+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\}$$

$$\left\{\begin{array}{l}\exists B, U, S, b.\ block^*\ \mathtt{s}\,\mathtt{t}\,B\ *\ B=U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus\{\mathtt{ap}\mapsto_{\mathsf{a}}n\}\uplus S_{\mathsf{s}}\ *\ \mathtt{t}_{|1}\mapsto\mathtt{s}\\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ (\mathtt{ap}-1)_{|1}\overset{.5}{\mapsto}(\mathtt{ap}+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2, p, q.\ block^*\ \mathtt{s}\,p\,B_1\ *\ ablock\,p\,q\,\{\mathtt{ap}\mapsto_{\mathsf{a}}n\}\ *\ block^*\ q\,\mathtt{t}\,B_2\\ *\ B=U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus\{\mathtt{ap}\mapsto_{\mathsf{a}}n\}\uplus S_{\mathsf{s}}\ *\ B=B_1\uplus\{\mathtt{ap}\mapsto_{\mathsf{a}}n\}\uplus B_2\ *\ \mathtt{t}_{|1}\mapsto\mathtt{s}\\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ (\mathtt{ap}-1)_{|1}\overset{.5}{\mapsto}(\mathtt{ap}+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{ap}+i)\mapsto\_\end{array}\right\}$$

```
  register struct store *p = (struct store *)ap;
  --p;
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2, q.\ block^*\ \mathtt{s}\,\mathtt{p}\,B_1\ *\ ablock\,\mathtt{p}\,q\,\{(\mathtt{p}+1)\mapsto_{\mathsf{a}}n\}\ *\ block^*\ q\,\mathtt{t}\,B_2\\ *\ B=U_{\mathsf{u}}\uplus A_{\mathsf{a}}\uplus\{(\mathtt{p}+1)\mapsto_{\mathsf{a}}n\}\uplus S_{\mathsf{s}}\ *\ B=B_1\uplus\{(\mathtt{p}+1)\mapsto_{\mathsf{a}}n\}\uplus B_2\\ *\ \mathtt{t}_{|1}\mapsto\mathtt{s}\ *\ b>\mathtt{t}\ *\ brk\,b\ *\ \mathtt{p}_{|1}\overset{.5}{\mapsto}(\mathtt{p}+1+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{p}+1+i)\mapsto\_\end{array}\right\}$$

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2, q.\ block^*\ \mathtt{s}\,\mathtt{p}\,B_1\ *\ q = \mathtt{p}+1+n\ *\ \mathtt{p}_{|1} \overset{.5}{\mapsto} q\ *\ block^*\ q\,\mathtt{t}\,B_2 \\ *\ B = U_{\mathtt{u}} \uplus A_{\mathtt{a}} \uplus \{(\mathtt{p}+1) \mapsto_{\mathtt{a}} n\} \uplus S_{\mathtt{s}}\ *\ B = B_1 \uplus \{(\mathtt{p}+1) \mapsto_{\mathtt{a}} n\} \uplus B_2 \\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ b > \mathtt{t}\ *\ brk\,b\ *\ \mathtt{p}_{|1} \overset{.5}{\mapsto} (\mathtt{p}+1+n)\ *\ \ast_{i=0}^{n-1}.\,(\mathtt{p}+1+i) \mapsto \_ \end{array}\right\}$$

```
  p->ptr = clearbusy(p->ptr);
```

$$\left\{\begin{array}{l}\exists B, U, S, b, B_1, B_2, q.\ block^*\ \mathtt{s}\,\mathtt{p}\,B_1\ *\ ublock\,\mathtt{p}\,q\,\{\mathtt{p}+1 \mapsto_{\mathtt{u}} n\}\ *\ block^*\ q\,\mathtt{t}\,B_2 \\ *\ B = U_{\mathtt{u}} \uplus A_{\mathtt{a}} \uplus \{(\mathtt{p}+1) \mapsto_{\mathtt{u}} n\} \uplus S_{\mathtt{s}}\ *\ B = B_1 \uplus \{(\mathtt{p}+1) \mapsto_{\mathtt{u}} n\} \uplus B_2 \\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ b > \mathtt{t}\ *\ brk\,b \end{array}\right\}$$

$$\left\{\exists B, U, S, b.\ block^*\ \mathtt{s}\,\mathtt{t}\,B\ *\ B = U_{\mathtt{u}} \uplus A_{\mathtt{a}} \uplus S_{\mathtt{s}}\ *\ \mathtt{t}_{|1} \mapsto \mathtt{s}\ *\ b > \mathtt{t}\ *\ brk\,b\right\}$$

$$\left\{arena\,A\right\}$$

```
}
//end "Free x" action
```

$$\left\{\boxed{arena\,A}\right\}$$

```
//end existential
```

$$\left\{\boxed{\exists A.\ arena\,A}\right\}$$

$$\left\{anArena\right\}$$