Types and refinements:

$$
\begin{array}{rrcl}
\text{Types} & \tau & ::= & \{\nu : \mathbf{int} \mid \varphi\} \mid \tau\,\mathbf{ref}^{r} \\
\text{Ownership} & r & \in & [0,1] \\
\text{Refinements} & \varphi & ::= & \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \top \\
 & & \mid & \phi(\widehat{v}_1, .., \widehat{v}_n) \\
 & & \mid & \widehat{v}_1 = \widehat{v}_2 \\
 & & \mid & \mathcal{CP} \\
\text{Refinement Values} & \widehat{v} & ::= & \pi \mid n \mid \nu \\
\text{Access Paths} & \pi & ::= & x\,\vec{\star} \\
\text{Function Types} & \sigma & ::= & \forall\lambda.\, \langle x_1 : \tau_1, \ldots, x_n : \tau_n \rangle \\
 & & & \to \langle x_1 : \tau_1', \ldots, x_n : \tau_n' \mid \tau \rangle \\
\text{Context Variables} & \lambda & \in & \mathbf{CVar} \\
\text{Concrete Context} & \vec{\ell} & ::= & \ell : \vec{\ell} \mid \epsilon \\
\text{Pred. Context} & \mathcal{C} & ::= & \ell : \mathcal{C} \mid \lambda \mid \epsilon \\
\text{Context Query} & \mathcal{CP} & ::= & \vec{\ell} \subseteq \mathcal{C} \\
\text{Typing Context} & \mathcal{L} & ::= & \lambda \mid \vec{\ell}
\end{array}
$$

An access path denotes a path through memory by a root variable and a potentially empty sequence of references $\vec{\star}$. The empty sequence is denoted ϵ. We abbreviate $x\,\epsilon$ as x.

Well-formedness:

$$\frac{\forall\, x \in dom(\mathit{\Gamma}).\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \mathit{\Gamma}(x)}{\mathcal{L} \vdash_{WF} \mathit{\Gamma}} \quad \text{(WF-Env)}$$

$$\frac{\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \varphi}{\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \{\nu : \mathbf{int} \mid \varphi\}} \quad \text{(WF-Int)}$$

$$\frac{\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \tau}{\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \tau\,\mathbf{ref}^{r}} \quad \text{(WF-Ref)}$$

$$\frac{\begin{array}{c}\mathit{\Gamma} \vdash \varphi \\ \mathbf{FCV}\,(\varphi) \subseteq \mathbf{CV}\,(\mathcal{L})\end{array}}{\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \varphi} \quad \text{(WF-Phi)}$$

$$\frac{\mathcal{L} \mid \mathit{\Gamma} \vdash_{WF} \tau \qquad \mathcal{L} \vdash_{WF} \mathit{\Gamma}}{\mathcal{L} \vdash_{WF} \tau \Rightarrow \mathit{\Gamma}} \quad \text{(WF-Result)}$$

$$\frac{\begin{array}{c}\lambda \vdash_{WF} x_1 : \tau_1, \ldots, x_n : \tau_n \\ \lambda \vdash_{WF} \tau \Rightarrow x_1 : \tau_1', \ldots, x_n : \tau_n'\end{array}}{\vdash_{WF} \forall\lambda.\, \langle x_1 : \tau_1, \ldots, x_n : \tau_n \rangle \to \langle x_1 : \tau_1', \ldots, x_n : \tau_n' \mid \tau \rangle} \quad \text{(WF-FunType)}$$

$$\frac{\forall\, f \in dom(\mathit{\Theta}).\, \vdash_{WF} \mathit{\Theta}(f)}{\vdash_{WF} \mathit{\Theta}} \quad \text{(WF-FunEnv)}$$

Well-typed predicates:

$$\frac{}{\Gamma \vdash \top}\ (\textsc{Pr-Top}) \qquad \frac{}{\Gamma \vdash \mathcal{CP}}\ (\textsc{Pr-Top}) \qquad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \neg\varphi}\ (\textsc{Pr-Not}) \qquad \frac{\Gamma \vdash \varphi_1 \qquad \Gamma \vdash \varphi_2}{\Gamma \vdash \varphi_1 \vee \varphi_2}\ (\textsc{Pr-Or})$$

$$\frac{\Gamma \vdash \widehat{v}_1 \qquad \Gamma \vdash \widehat{v}_2}{\Gamma \vdash \widehat{v}_1 = \widehat{v}_2}\ (\textsc{Pr-Eq}) \qquad \frac{\Gamma \vdash \widehat{v}_1 \qquad \cdots \qquad \Gamma \vdash \widehat{v}_n}{\Gamma \vdash \phi(\widehat{v}_1, .., \widehat{v}_n)}\ (\textsc{Pr-App})$$

Well-typed predicate values

$$\frac{}{\Gamma \vdash n}\ (\textsc{Pv-Int}) \qquad \frac{}{\Gamma \vdash \nu}\ (\textsc{Pv-Nu}) \qquad \frac{\vec{\star} \Downarrow \Gamma(x)}{\Gamma \vdash x\,\vec{\star}}\ (\textsc{Pv-AP})$$

$$\frac{}{\epsilon \Downarrow \{\nu : \mathbf{int} \mid \_\}}\ (\textsc{AP-Eps}) \qquad \frac{\vec{\star} \Downarrow \tau \qquad r > 0}{\star\vec{\star} \Downarrow \tau\,\mathbf{ref}^r}\ (\textsc{AP-Cons})$$

The addition operator is defined as in the ESOP 2020 paper.

We assume that $x\,\vec{\star}$ is a valid variable in the underlying logic; it can be lifted to one using consistent substitution.

The denotation operation is defined as:

$$\begin{aligned}
[\![\Gamma, x : \tau]\!] &= [\![\tau]\!]_x \wedge [\![\Gamma]\!] \\
[\![\bullet]\!] &= \top \\
[\![\{\nu : \mathbf{int} \mid \varphi\}]\!]_\pi &= [\pi/\nu]\,\varphi \\
[\![\tau\,\mathbf{ref}^r]\!]_{x\,\vec{\star}} &= [\![\tau]\!]_{x\,\vec{\star}\,\star}
\end{aligned}$$

We define a new strengthening operation $\tau \wedge \nu = \pi$ as:

$$\begin{aligned}
\{\nu : \mathbf{int} \mid \varphi\} \wedge \nu = \pi &\triangleq \{\nu : \mathbf{int} \mid \varphi \wedge \nu = \pi\} \\
\tau\,\mathbf{ref}^0 \wedge \nu = \pi &\triangleq \tau\,\mathbf{ref}^0 \\
\tau\,\mathbf{ref}^r \wedge \nu = \pi &\triangleq (\tau \wedge \nu = \pi\,\star)\,\mathbf{ref}^r \ \text{ if } (r > 0)
\end{aligned}$$

We now describe the type rules for the extended type system. We omit the rules for T-Assert, T-Seq, T-If, T-LetInt, T-Var, T-Alias, T-AliasPtr, T-Sub as they are unchanged.

$$\frac{\begin{array}{c}\text{(The shapes of } \tau' \text{ and } \tau_2 \text{ are similar)} \\ \mathcal{L} \vdash_{WF} \Gamma \setminus y \\ \Theta \mid \mathcal{L} \mid \Gamma[x \hookleftarrow \tau_1 \wedge \nu = y\,\star][y : (\tau_2 \wedge \nu = x)\,\mathbf{ref}^1] \vdash e : \tau \Rightarrow \Gamma'\end{array}}{\Theta \mid \mathcal{L} \mid \Gamma[x : \tau_1 + \tau_2][y : \tau'\,\mathbf{ref}^1] \vdash y := x \,;\, e : \tau \Rightarrow \Gamma'}\ (\textsc{T-Assign})$$

$$\frac{\Theta \mid \mathcal{L} \mid \Gamma[x \hookleftarrow \tau_1 \wedge \nu = y], y : \tau_2 \wedge \nu = x \vdash e : \tau \Rightarrow \Gamma' \qquad x \notin dom(\Gamma)}{\Theta \mid \mathcal{L} \mid \Gamma[x : \tau_1 + \tau_2] \vdash \mathbf{let}\, x = y\, \mathbf{in}\, e : \tau \Rightarrow \Gamma'} \quad \text{(T-Let)}$$

$$\frac{\begin{array}{c} \tau_1' = \begin{cases} \tau_1 \wedge \nu = x & r > 0 \\ \tau_1 & r = 0 \end{cases} \\ \tau_2' = \begin{cases} \tau_2 \wedge \nu = y\star & r > 0 \\ \tau_2 & r = 0 \end{cases} \\ \Theta \mid \mathcal{L} \mid \Gamma[y \hookleftarrow \tau_1'\, \mathbf{ref}^r], x : \tau_2' \vdash e : \tau \Rightarrow \Gamma' \\ x \notin dom(\Gamma') \end{array}}{\Theta \mid \mathcal{L} \mid \Gamma[y : (\tau_1 + \tau_2)\, \mathbf{ref}^r] \vdash \mathbf{let}\, x = *y\, \mathbf{in}\, e : \tau \Rightarrow \Gamma'} \quad \text{(T-Deref)}$$

$$\frac{\begin{array}{c} \Theta \mid \mathcal{L} \mid \Gamma[y \hookleftarrow \tau_1 \wedge \nu = x\star], x : (\tau_2 \wedge \nu = y)\, \mathbf{ref}^1 \vdash e : \tau \Rightarrow \Gamma' \\ x \notin dom(\Gamma') \end{array}}{\Theta \mid \mathcal{L} \mid \Gamma[y : \tau_1 + \tau_2] \vdash \mathbf{let}\, x = \mathbf{mkref}\, y\, \mathbf{in}\, e : \tau \Rightarrow \Gamma'} \quad \text{(T-MkRef)}$$

$$\frac{\begin{array}{c} \sigma_\alpha = [\ell : \mathcal{L}/\lambda] \qquad \sigma_x = [y_1/x_1] \cdots [y_n/x_n] \\ \Theta(f) = \forall\lambda.\, \langle x_1 : \tau_1, \ldots, x_n : \tau_n \rangle \to \langle x_1 : \tau_1', \ldots, x_n : \tau_n' \mid \tau \rangle \\ \Gamma_1(y_i) = \tau_i'' + \sigma_\alpha\, \sigma_x\, \tau_i \\ \Gamma_2[y_i \hookleftarrow \tau_i''] \qquad \mathcal{L} \vdash_{WF} \Gamma_2 \\ \Gamma_3 = \Gamma_1[y_i \hookleftarrow \tau_i'' + \sigma_\alpha\, \sigma_x\, \tau_i'], z : \sigma_\alpha\, \sigma_x\, \tau \\ \Theta \mid \mathcal{L} \mid \Gamma_3 \vdash e : \tau' \Rightarrow \Gamma_4 \qquad z \notin dom(\Gamma_4) \end{array}}{\Theta \mid \mathcal{L} \mid \Gamma_1 \vdash \mathbf{let}\, z = f^\ell(y_1, \ldots, y_n)\, \mathbf{in}\, e : \tau' \Rightarrow \Gamma_4} \quad \text{(T-Call)}$$

$$\frac{\begin{array}{c} \mathcal{L} \vdash_{WF} \Gamma_p \\ \Theta \mid \mathcal{L} \mid \Gamma \vdash e : \tau \Rightarrow \Gamma' \end{array}}{\Theta \mid \mathcal{L} \mid \Gamma + \Gamma_p \vdash e : \tau \Rightarrow \Gamma' + \Gamma_p} \quad \text{(T-Frame)}$$

1 Proofs

Define the partial type lookup operation $\Gamma(\pi)$ as:

$$\Gamma(x\,\vec{\star}) = \Gamma(x)(\vec{\star})$$
$$\tau(\epsilon) = \tau$$
$$(\tau'\, \mathbf{ref}^r)(\star\,\vec{\star}) = \tau'(\vec{\star})$$

[JT: defining this traversal as a map operation on τ is gross] ⟵

$[H, v]$ is the partial function from $\vec{\star}$ to values v defined by

$$[H, v](\epsilon) = v \qquad [H, v](\star\,\vec{\star}) = \begin{cases} H(a) & \text{if } [H, v](\vec{\star}) = a \wedge a \in dom(H) \\ \mathit{undef} & \mathit{o.w.} \end{cases}$$

$[H, R]$ is the partial map from π to values v defined by $[H, R](x\vec{\star}) = [H, R(x)](\vec{\star})$

Lemma 1. *If $\mathcal{L} \mid \Gamma \backslash x \vdash_{WF} \varphi$ and for all $y \neq x$ we have* $\mathbf{own}\,(H, R(y), \Gamma(y))(a) = 0$*, then $[H, R]\,[n/\nu]\varphi$ is equivalent to $[H\{a \hookleftarrow v'\}, R]\,[n/\nu]\varphi$ where $R(x) = a$.*

Proof. Suppose not. Then there must be some access path π in φ such that for some prefix of the path (called π') we have $[H, R](\pi') = a$. From $\mathcal{L} \mid \Gamma \setminus x \vdash_{WF} \varphi$ we must have that π' cannot be rooted in x, and must therefore be rooted in some other variable z, whereby $\mathbf{own}\,(H, R(z), \Gamma(z))(a) = 0$. But we must then have $\Gamma(\pi') = \tau'\,\mathbf{ref}^0$, which contradicts our assumption that $\mathcal{L} \mid \Gamma \setminus x \vdash_{WF} \varphi$.

Lemma 2. *For any $x, a, R, H,\ \Gamma,$ and n such that $R(x) = a$, $H \vdash v' \Downarrow n$, $H \vdash H(a) \Downarrow n$ and where for all $y \neq x$ we have* $\mathbf{own}\,(H, R(y), \Gamma(y))(a) = 0$*:*

1. *$H\{a \hookleftarrow v'\} \vdash v' \Downarrow n$*
2. *If $\mathcal{L} \mid \Gamma \setminus x \vdash_{WF} \tau$,* $\mathbf{own}\,(H, v, \tau)(a) = 0$*, and* $\mathbf{SATv}(H, R, v, \tau)$ *then* $\mathbf{SATv}(H\{a \hookleftarrow v'\}, R, v, \tau)$.
3. *If $\mathcal{L} \vdash_{WF} \Gamma \backslash x$, and* $\mathbf{SATv}(H, R, v, \Gamma(z))$*, then* $\mathbf{SATv}(H\{a \hookleftarrow v\}, R, v, \Gamma(z))$

Proof.

1. From $H \vdash v' \Downarrow n$ and $H \vdash H(a) \Downarrow n$, we must have that for any possible sequence $\vec{\star}$, $[H, v'](\vec{\star}) \neq a$ (if we did, then we would have that v reaches an integer along paths of different lengths, a clear contradiction). Then the value of a in H is irrelevant to the derivation of $H \vdash v' \Downarrow n$, giving $H\{a \hookleftarrow v'\} \vdash v' \Downarrow n$.
2. By induction on the shape of τ. In the base case where $\tau = \{\nu : \mathbf{int} \mid \varphi\}$, from $\mathcal{L} \mid \Gamma \setminus x \vdash_{WF} \tau$ we have $\mathcal{L} \mid \Gamma \setminus x \vdash_{WF} \varphi$, where by from Lemma 1 we have $[H, R]\,[n/\nu]\varphi$ is equivalent to $[H\{a \hookleftarrow v'\}, R]\,[n/\nu]\varphi$ whereby the result holds by assumption.
   In the inductive step, we have $\tau = \tau'\,\mathbf{ref}^r$, and $v = a'$. Suppose $a = a'$: from $\mathbf{own}\,(H, v, \tau)(a) = 0$ we must then have $r = 0$, whereby $\tau' = \top_n$. From **??**, item 1 above, [JT: the lemma that any shape consistent values satisfy the top type], we have $\mathbf{SATv}(H\{a \hookleftarrow v'\}, R, a, \tau)$.
   Otherwise $a \neq a'$ in which case the result holds by inversion on $\mathcal{L} \mid \Gamma \backslash x \vdash_{WF} \tau$, $\mathbf{own}\,(H, v, \tau'\,\mathbf{ref}^r)(a) = 0$ and the inductive hypothesis.
3. Immediate result of item 2.

Lemma 3 (Preservation). *For any e where $\Theta \mid \mathcal{L} \mid \Gamma_1 \vdash e : \tau \Rightarrow \Gamma_2$, for all e' and E such that $\Theta \mid [\,] : \tau \Rightarrow \Gamma_2 \mid \mathcal{L} \vdash_{ectx} E : \tau' \Rightarrow \Gamma_3$ if $\left\langle H, R, \vec{F}, E[e] \right\rangle \longrightarrow_D \left\langle H, R, \vec{F}, E[e'] \right\rangle$, $\mathcal{L} \vdash_{WF} \Gamma_p$ and* $\mathbf{Cons}\,(H, R, \Gamma_1 + \Gamma_p)$ *then there exists some Γ_4 such that*

1. $\mathbf{Cons}\,(H', R', \Gamma_4 + \Gamma_p)$
2. *$\Theta \mid \mathcal{L} \mid \Gamma_4 \vdash e' : \tau \Rightarrow \Gamma_2$*

Proof. By induction on the derivation of $\Theta \mid \mathcal{L} \mid \Gamma_1 \vdash e : \tau \Rightarrow \Gamma_2$.

Case T-Sub**:**

By the inductive hypothesis, that **Own** is anti-monotone w.r.t the subtyping relation **Admitted**, and the preservation of **Cons** by subtyping **Admitted** (**??**).

Case T-Frame**:**

Then we have that $\Theta \mid \mathcal{L} \mid \Gamma_1' \vdash e : \tau \Rightarrow \Gamma_2'$ where $\Gamma_1 = \Gamma_1' + \Gamma_1''$ and $\Gamma_2 = \Gamma_2' + \Gamma_1'$ and where $\mathcal{L} \vdash_{WF} \Gamma_1'$. We have $\mathbf{Cons}\,(H, R, \Gamma_1' + \Gamma_1'' + \Gamma_p)$. We must then have that $\mathcal{L} \vdash_{WF} \Gamma_1' + \Gamma_p$ by **[Admitted: that WF is closed under** $+$]. Taking Γ_p in the inductive hypothesis to be $\Gamma_p + \Gamma_1'$, we then have that $\mathbf{Cons}\,(H', R', \Gamma_4' + \Gamma_p + \Gamma_1')$ and $\Theta \mid \mathcal{L} \mid \Gamma_4' \vdash e' : \tau \Rightarrow \Gamma_2'$. We take $\Gamma_4 = \Gamma_4' + \Gamma_1'$. Then, by an application of T-Frame we have $\Theta \mid \mathcal{L} \mid \Gamma_4 \vdash e' : \tau \Rightarrow \Gamma_2$, and we then have $\mathbf{Cons}\,(H', R', \Gamma_4 + \Gamma_p)$ from $\mathbf{Cons}\,(H', R', \Gamma_4' + \Gamma_1' + \Gamma_p)$.

Case T-Assign**:**

$$
\begin{array}{llll}
e = y := x \,;\, e'' & \Gamma_1(x) = \tau_1 + \tau_2 & \Gamma_1(y) = \tau'\,\mathbf{ref}^1 & \\
|\tau'| = |\tau_1 + \tau_2| & \mathcal{L} \vdash_{WF} \Gamma_1 \setminus y & & \\
\multicolumn{4}{l}{\Theta \mid \mathcal{L} \mid \Gamma[x \hookleftarrow \tau_1 \wedge \nu = y\star][y \hookleftarrow (\tau_2 \wedge \nu = x)\,\mathbf{ref}^1] \vdash e' : \tau \Rightarrow \Gamma_2} \\
a = R(y) & H' = H\{a \hookleftarrow R(x)\} & R = R' & e'' = e'
\end{array}
$$

From $\mathbf{Cons}\,(H, R, \Gamma_1 + \Gamma_p)$ and from $\Gamma_1(y) = \tau'\,\mathbf{ref}^1$ we must have that for any variable $z \in dom(\Gamma_1), z \neq y$ that $\mathbf{own}\,(H, R(z), \Gamma_1(z))(a) = 0$ and similarly for all variables in $dom(\Gamma_p)$.

We must also have that if $y \in dom(\Gamma_p)$ that $\Gamma(y) = \top_n\,\mathbf{ref}^0$. Then by **[Admitted: that 0 references are not referenced in types]**, we have $\mathcal{L} \vdash_{WF} \Gamma_p \setminus y$.

Next, from **[Admitted: that SATv implies shape consistency]**, from $\mathbf{SATv}(H, R, R(y), \tau'\,\mathbf{ref}^1)$ we have that $H \vdash R(y) \Downarrow |\tau'\,\mathbf{ref}^1|$, whereby we have $H \vdash H(R(y)) \Downarrow |\tau'|$. Similarly, from $\mathbf{SATv}(H, R, R(x), \tau_1 + \tau_2)$ we have $H \vdash R(x) \Downarrow |\tau_1 + \tau_1|$.

From the above, our assumption $\mathcal{L} \vdash_{WF} \Gamma_1 \setminus y$ and Lemma 1 we then have $\mathbf{SATv}(H', R, R(z), \Gamma_1(z))$ for any $z \neq x$ and $z \neq y$.

Similarly, we must have that $\mathbf{SATv}(H', R, R(z), \Gamma_p(z))$ by the reasoning above and Lemma 1.

We must also have that $\mathbf{SATv}(H', R, R(x), \tau_1 + \tau_2)$. From **[Admitted: that SATv distributes over** $+$], we therefore have $\mathbf{SATv}(H', R, R(x), \tau_1)$ and $\mathbf{SATv}(H', R, R(x), \tau_2)$. It is then immediate that $\mathbf{SATv}(H', R, R(x), \tau_1 \wedge \nu = y\star)$ and $\mathbf{SATv}(H', R, R(x), \tau_2 \wedge \nu = x)$. From the latter we then have $\mathbf{SATv}(H', R, R(y), (\tau_2 \wedge \nu = x)\,\mathbf{ref}^1)$.

[JT: The ownership reasoning is entirely similar to the ESOP paper. We can use that $\mathbf{Cons}\,(H, R, \Gamma_1 + \Gamma_p)$ and that ownership is only lost in Γ_1 to re-establish ownership consistency for $\Gamma_4 + \Gamma_p$] ⟵

We take $\Gamma_4 = \Gamma[x \hookleftarrow \tau_1 \wedge \nu = y\star][y \hookleftarrow (\tau_2 \wedge \nu = x)\,\mathbf{ref}^1]$ whereby from **[Admitted: that adding SATv envs is Cons]** and the previous reasoning we have $\mathbf{Cons}\,(H', R', \Gamma_4 + \Gamma_p)$. That $\Theta \mid \mathcal{L} \mid \Gamma_4 \vdash e' : \tau \Rightarrow \Gamma_2$ is immediate from our assumption.