Some observations on hypercollecting semantics and subset closed hyperproperties

Marc Gotliboym and Dave Naumann

November 14, 2017

This note is based on Assaf's dissertation work [Ass15] as presented in [ANS+17]. We explore the sense in which the technique is suited to subset closed hyperproperties.

The ***hypercollecting semantics*** is introduced as basis for the calculational derivation of abstract interpretations of hyperproperties. It is formulated (almost) compositionally, at the level of sets of sets.

Hypercollecting semantics $(\!| c |\!) \in \mathcal{P}(\mathcal{P}(\mathbf{Trc})) \to \mathcal{P}(\mathcal{P}(\mathbf{Trc}))$

$$(\!| x := e |\!)\mathbb{T} \triangleq \{\{\!| x := e |\!\}T \mid T \in \mathbb{T}\} \qquad (\!| c_1; c_2 |\!)\mathbb{T} \triangleq (\!| c_2 |\!) \circ (\!| c_1 |\!)\mathbb{T} \qquad (\!|\mathbf{skip}|\!)\mathbb{T} \triangleq \mathbb{T}$$

$$(\!|\mathbf{if}\ b\ \mathbf{then}\ c_1\ \mathbf{else}\ c_2|\!)\mathbb{T} \triangleq \{\{\!| c_1 |\!\} \circ \{\!|\, \mathrm{grd}^b \,|\!\}T \cup \{\!| c_2 |\!\} \circ \{\!|\, \mathrm{grd}^{\neg b} \,|\!\}T \ \mid\ T \in \mathbb{T}\}$$

$$(\!|\mathbf{while}\ b\ \mathbf{do}\ c |\!)\mathbb{T} \triangleq (\!|\mathrm{grd}^{\neg b}|\!)\left(\mathrm{lfp}^{\subseteq}_{\mathbb{T}}(\!|\mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else\ skip}|\!)\right)$$

$$(\!|\mathrm{grd}^b|\!)\mathbb{T} \triangleq \{\{\!|\, \mathrm{grd}^b \,|\!\}T \mid T \in \mathbb{T}\}$$

Here $\{\!| c |\!\}$ is the ordinary collecting semantics. Refer to [ANS+17] for notations not defined here (specifically, v2 of the long version in arXiv).

That paper notes that the hypercollecting semantics is an approximation of the direct image of the collecting semantics: "For a singleton $\{T\}$, the set $(\!| c |\!)\{T\} \in \mathcal{P}(\mathcal{P}(\mathbf{Trc}))$ is not necessarily a singleton set containing only the element $\{\!| c |\!\}T$. If c is a loop, $(\!| c |\!)\{T\}$ yields a set of sets R of traces, where each set R of traces contains only traces that exit the loop after less than k iterations, for $k \in \mathbb{N}$."

Mastroeni and Pasqua [MP17] say that the hypercollecting semantics of [ANS+17] is exactly the direct image of collecting semantics, when applied to subset closed (***ssc***) hyperproperties. Subset closure is mentioned in passing in the appendix of [ANS+17]. In particular, the fact that $\gamma_{\mathrm{crdtr}}(\mathscr{C})$ is ssc is used to facilitate a step in the derivation of the cardinality abstract interpreter, for the case of the conditional command. That seems to be the only mention of subset closure in [ANS+17], aside from the quote above which is suggestive. In this note we investigate these observations.

Theorem 1 of [ANS+17] says for all c and all $T \in \mathcal{P}(\mathbf{Trc})$, $\{\!| c |\!\}T$ is in $(\!| c |\!)\{T\}$. It is a consequence of this relation with the direct image of collecting semantics:

$$\forall \mathbb{T} \in \mathcal{P}(\mathcal{P}(\mathbf{Trc})),\ \{\{\!| c |\!\}T \mid T \in \mathbb{T}\} \subseteq (\!| c |\!)\mathbb{T} \tag{1}$$

which is proved by structural induction on commands. The Theorem suffices to justify the derivation of abstract interpreters from $(\!|c|\!)$, but it raises the question how to avoid starting from a concrete semantics $(\!|c|\!)$ that itself already abstracts from the "true" image-of-image semantics.

We will show that if $\mathbb{T}$ is ssc then the condition (1) strengthens to an equality. This in turn leads to the observation that the hypercollecting semantics preserves ssc. This is in accord with the observation by Clarkson and Schneider [CS10, sec 2.6] that refinement works for exactly the ssc hyperproperties. We begin by showing that one of the leading examples is ssc.

Dependency is ssc

We recall a few definitions with respect to a given program P together with $\Gamma \in \mathrm{Var_P} \to \mathcal{L}$ that maps each variable to a security level $l \in \mathcal{L}$ for its initial value.

Initial l-equivalence $T \models_\Gamma l$

$$T \models_\Gamma l \text{ iff } \forall t_1, t_2 \in T,\ \forall x \in \mathrm{Var_P},\ \Gamma(x) \sqsubseteq l \implies [\![x]\!]_{\mathrm{pre}} t_1 = [\![x]\!]_{\mathrm{pre}} t_2$$

l-variety $\mathcal{O}^l\{\!|e|\!\} \in \mathcal{P}(\mathbf{Trc}) \to \mathcal{P}(\mathcal{P}(\mathbf{Val}))$ $\quad$ $\mathcal{O}^l(\!|e|\!) \in \mathcal{P}(\mathcal{P}(\mathbf{Trc})) \to \mathcal{P}(\mathcal{P}(\mathbf{Val}))$

$$\mathcal{O}^l\{\!|e|\!\}T \triangleq \{\{\!|e|\!\}R \mid R \subseteq T \text{ and } R \models_\Gamma l\} \qquad \mathcal{O}^l(\!|e|\!)\mathbb{T} \triangleq \cup_{T \in \mathbb{T}}\, \mathcal{O}^l\{\!|e|\!\}T$$

The following may be of interest but is not the main point.

Lemma 1. $\mathcal{O}^l(\!|e|\!)\mathbb{T}$ is ssc for all $\mathbb{T}$.

Proof. This follows directly from the fact that $\mathcal{O}^l\{\!|e|\!\}T$ is ssc for all T. To prove the latter, suppose $V' \subseteq V$. We have

$$\begin{array}{ll} & V \in \mathcal{O}^l\{\!|e|\!\}T \\ \iff & \quad \wr \text{ def } \int \\ & \exists R \subseteq T,\ R \models_\Gamma l \text{ and } V = \{\!|e|\!\}R \\ \implies & \quad \wr \text{ let } R' := \{\!|e|\!\}^{-1}V', \text{ note } R' \subseteq R \text{ and } R \models_\Gamma l \text{ imply } R' \models_\Gamma l \ \int \\ & \exists R' \subseteq T,\ R' \models_\Gamma l \text{ and } V' = \{\!|e|\!\}R' \\ \iff & \quad \wr \text{ def } \int \\ & V' \in \mathcal{O}^l\{\!|e|\!\}T \end{array}$$

□

At the level of commands it is not the case that $(\!|c|\!)\mathbb{T}$ is always ssc. For example, choose $\mathbb{T}$ to be a singleton $\{T\}$ where T is non-empty. Then $\mathbb{T}$ is not ssc and neither is $(\!|x := e|\!)\mathbb{T}$ (for any expression e).

Lattice of dependence constraints Dep $\mathscr{D} \in \text{Dep}$

$$\text{Dep} \triangleq \mathcal{P}(\{l \rightsquigarrow x \mid l \in \mathcal{L}, x \in \text{Var}_\text{P}\})$$
$$\mathscr{D}_1 \sqsubseteq^\natural \mathscr{D}_2 \triangleq \mathscr{D}_1 \supseteq \mathscr{D}_2 \qquad \mathscr{D}_1 \sqcup^\natural \mathscr{D}_2 \triangleq \mathscr{D}_1 \cap \mathscr{D}_2$$

Agreements abstraction agree α_{agree} γ_{agree}

$$\begin{array}{lcl}
\text{agree} & \in & \mathcal{P}(\mathbf{Val}) \to \{\text{tt}, \text{ff}\} \\
\text{agree}(V) & \triangleq & (\forall v_1, v_2 \in V,\ v_1 = v_2) \\
\alpha_{\text{agree}} & \in & \mathcal{P}(\mathcal{P}(\mathbf{Val})) \to \{\text{tt}, \text{ff}\} \\
\alpha_{\text{agree}}(\mathbb{V}) & \triangleq & \wedge_{V \in \mathbb{V}} \text{agree}(V) \\
\gamma_{\text{agree}} & \in & \{\text{tt}, \text{ff}\} \to \mathcal{P}(\mathcal{P}(\mathbf{Val})) \\
\gamma_{\text{agree}}(\text{bv}) & \triangleq & \{V \in \mathcal{P}(\mathbf{Val}) \mid \text{agree}(V) \Longleftarrow \text{bv}\}
\end{array}$$

$$(\mathcal{P}(\mathcal{P}(\mathbf{Val})), \subseteq) \underset{\alpha_{\text{agree}}}{\overset{\gamma_{\text{agree}}}{\leftrightarrows}} (\{\text{tt}, \text{ff}\}, \Longleftarrow)$$

Dependence abstraction deptr α_{deptr} γ_{deptr}

$$\begin{array}{lcl}
\text{deptr} & \in & \mathcal{P}(\mathbf{Trc}) \to \text{Dep} \\
\text{deptr}(T) & \triangleq & \{l \rightsquigarrow x \mid l \in \mathcal{L},\ x \in \text{Var}_\text{P},\ \alpha_{\text{agree}}(\mathcal{O}^l\{\!|x|\!\}T)\} \\
\alpha_{\text{deptr}} & \in & \mathcal{P}(\mathcal{P}(\mathbf{Trc})) \to \text{Dep} \\
\alpha_{\text{deptr}}(\mathbb{T}) & \triangleq & \sqcup^\natural_{T \in \mathbb{T}} \text{deptr}(T) \\
\gamma_{\text{deptr}} & \in & \text{Dep} \to \mathcal{P}(\mathcal{P}(\mathbf{Trc})) \\
\gamma_{\text{deptr}}(\mathscr{D}) & \triangleq & \{T \mid \text{deptr}(T) \sqsubseteq^\natural \mathscr{D}\}
\end{array}$$

$$(\mathcal{P}(\mathcal{P}(\mathbf{Trc})), \subseteq) \underset{\alpha_{\text{deptr}}}{\overset{\gamma_{\text{deptr}}}{\leftrightarrows}} (\text{Dep}, \sqsubseteq^\natural)$$

We spell out a fact not highlighted in the paper.

Lemma 2. $T' \subseteq T \implies \text{deptr}(T') \supseteq \text{deptr}(T)$

Proof. Observe for any l, x, T, T' that

$$T' \subseteq T \implies \mathcal{O}^l\{\!|x|\!\}T' \subseteq \mathcal{O}^l\{\!|x|\!\}T \implies (\alpha_{\text{agree}}(\mathcal{O}^l\{\!|x|\!\}T') \Longleftarrow \alpha_{\text{agree}}(\mathcal{O}^l\{\!|x|\!\}T))$$

by monotonicity of $\mathcal{O}^l\{\!|x|\!\}$ and of α_{agree}. Now if $T' \subseteq T$ then

$$\text{deptr}(T') = \{l \rightsquigarrow x \mid \alpha_{\text{agree}}(\mathcal{O}^l\{\!|x|\!\}T')\} \supseteq \{l \rightsquigarrow x \mid \alpha_{\text{agree}}(\mathcal{O}^l\{\!|x|\!\}T)\} = \text{deptr}(T)$$

by definition of deptr and the observation. □

Proposition 3. $\gamma_{\text{deptr}}(\mathscr{D})$ is ssc for any $\mathscr{D}$.

Proof. Suppose $T' \subseteq T$. Then

$$\begin{array}{ll} & T' \in \gamma_{\text{deptr}}(\mathscr{D}) \\ \iff & \quad \wr \text{ def } \gamma_{\text{deptr}} \int \\ & \text{deptr}(T') \supseteq \mathscr{D} \\ \impliedby & \quad \wr \text{ Lemma 2, } T' \subseteq T \int \\ & \text{deptr}(T) \supseteq \mathscr{D} \\ \iff & \quad \wr \text{ def } \int \\ & T \in \gamma_{\text{deptr}}(\mathscr{D}) \end{array}$$

□

Clarkson and Schneider [CS10] note that a number of noninterference properties are ssc, and Lemma 3 confirms this for dependence. By a similar argument, $\gamma_{\text{crdtr}}(\mathscr{C})$ is ssc for any set of cardinality constraints $\mathscr{C}$.

Precision of hypercollecting semantics

Returning to Theorem 1 of [ANS+17], inspection of the proof of (1) shows that inequality only arises in the case of loops. We recall the argument (with minor typos fixed).

Proof of Theorem 1 of [ANS+17], case of while (b) do c

Let $(\mathbb{X}_n^{\mathbb{T}})_{n\in\mathbb{N}}$ be the sequence defined as

$$\mathbb{X}_n^{\mathbb{T}} \triangleq \left\{\{\mathcal{F}^{(n)}(\bot)(t) \in \mathbf{Trc} \mid t \in T\} \mid T \in \mathbb{T}\right\} \text{ for } n \geq 1, \quad \mathbb{X}_0^{\mathbb{T}} = \emptyset$$

where:

$$\mathcal{F}(w)(t) \triangleq \begin{cases} t & \text{if } [\![b]\!]t = 0 \\ w \circ [\![c]\!]t & \text{otherwise} \end{cases}$$

The limit of the sequence $x_n^T \triangleq \{\mathcal{F}^{(n)}(\bot)(t) \in \mathbf{Trc} \mid t \in T\}$ is the ordinary collecting semantics $\{\!|\mathbf{while}\ (b)\ \mathbf{do}\ c\ |\!\}T$ of the while loop (as proved in, for example, [CP10, AN16] and [ANS+17, Lemma 8]). Thus, the sequence $\mathbb{X}_n^{\mathbb{T}}$ converges to $\{\{\!|\mathbf{while}\ (b)\ \mathbf{do}\ c\ |\!\}T \mid T \in \mathbb{T}\}$.

Let $(\mathbb{Y}_n^{\mathbb{T}})_{n\in\mathbb{N}}$ and $(\mathbb{G}_n^{\mathbb{T}})_{n\in\mathbb{N}}$ be the sequences defined as follows (omitting "**else skip**").

$$\mathbb{G}_{n+1}^{\mathbb{T}} \triangleq \mathbb{T} \cup (\!|\textbf{if } (b) \textbf{ then } c |\!)\mathbb{G}_n^{\mathbb{T}} \text{ for } n \geq 0, \qquad \mathbb{G}_0^{\mathbb{T}} \triangleq \emptyset$$
$$\mathbb{Y}_n^{\mathbb{T}} \triangleq (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{G}_n^{\mathbb{T}}$$

The limit of $\mathbb{Y}_n^{\mathbb{T}}$ is the hypercollecting semantics of the loop, $(\!|\textbf{while } (b) \textbf{ do } c |\!)\mathbb{T}$. Thus to show (1) it suffices to prove that the sequences $\mathbb{X}_n^{\mathbb{T}}$ and $\mathbb{Y}_n^{\mathbb{T}}$ satisfy

$$\forall \mathbb{T} \in \mathcal{P}(\mathcal{P}(\mathbf{Trc})),\ \forall n \in \mathbb{N},\ \mathbb{X}_{n+1}^{\mathbb{T}} \subseteq \mathbb{Y}_{n+1}^{\mathbb{T}}$$

Passing to the limit in this inequality leads to the required result

$$\forall \mathbb{T} \in \mathcal{P}(\mathcal{P}(\mathbf{Trc})),\ \{\{\!|\textbf{while } (b) \textbf{ do } c |\!\}T \mid T \in \mathbb{T}\} \subseteq (\!|\textbf{while } (b) \textbf{ do } c |\!)\mathbb{T}$$

We prove the following more precise characterisation of the sequences $\mathbb{X}_n^{\mathbb{T}}$ and $\mathbb{Y}_n^{\mathbb{T}}$ (which implies $\mathbb{X}_{n+1}^{\mathbb{T}} \subseteq \mathbb{Y}_{n+1}^{\mathbb{T}}$):

$$\forall \mathbb{T} \in \mathcal{P}(\mathcal{P}(\mathbf{Trc})),\ \forall n \in \mathbb{N},\ \mathbb{Y}_{n+1}^{\mathbb{T}} = \mathbb{Y}_n^{\mathbb{T}} \cup \mathbb{X}_{n+1}^{\mathbb{T}} \tag{2}$$

To this end, first observe that

$$\forall n \in \mathbb{N},\ \mathbb{G}_{n+1}^{\mathbb{T}} = \cup_{0\leq k\leq n} (\!|\textbf{if } (b) \textbf{ then } c |\!)^{(k)}\mathbb{T} \tag{3}$$

The remainder of the proof of (2) proceeds by induction on $n \in \mathbb{N}$.

- case $n = 0$:

$$\begin{array}{ll} & \mathbb{Y}_1^{\mathbb{T}} \\ = & (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{G}_1^{\mathbb{T}} \\ = & (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{T} \\ = & \{\{\!|\,\mathrm{grd}^{\neg b}\,|\!\}T \mid T \in \mathbb{T}\} \\ = & \{\{\mathcal{F}^{(1)}(\bot)(t) \in \mathbf{Trc} \mid t \in T\} \mid T \in \mathbb{T}\} \\ = & \quad \wr \text{ by definition of } \mathbb{X}_1^{\mathbb{T}} \ \int \\ & \mathbb{X}_1^{\mathbb{T}} \\ = & \quad \wr \text{ since } \mathbb{Y}_0^{\mathbb{T}} = \emptyset \int \\ & \mathbb{Y}_0^{\mathbb{T}} \cup \mathbb{X}_1^{\mathbb{T}} \end{array}$$

- Let $n \in \mathbb{N}$ such that $\mathbb{Y}_{n+1}^{\mathbb{T}} = \mathbb{Y}_n^{\mathbb{T}} \cup \mathbb{X}_{n+1}^{\mathbb{T}}$. Then:

$$
\begin{array}{ll}
 & \mathbb{Y}^{\mathbb{T}}_{n+2} \\
= & (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{G}^{\mathbb{T}}_{n+2} \\
= & (\!|\mathrm{grd}^{\neg b}|\!)\left(\mathbb{T} \cup (\!|\textbf{if } (b) \textbf{ then } c \,|\!)\mathbb{G}^{\mathbb{T}}_{n+1}p\right) \\
= & (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{T} \;\cup\; (\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)\mathbb{G}^{\mathbb{T}}_{n+1} \\
= & \quad \wr \text{ using (3) } \int \\
 & (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{T} \;\cup\; (\!|\mathrm{grd}^{\neg b}|\!)\left(\cup_{1\le k\le n+1}(\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(k)}\mathbb{T}\right) \\
= & \cup_{0\le k\le n+1}(\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(k)}\mathbb{T} \\
= & \left(\cup_{0\le k\le n}(\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(k)}\mathbb{T}\right) \;\cup\; (\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(n+1)}\mathbb{T} \\
= & (\!|\mathrm{grd}^{\neg b}|\!) \circ \left(\cup_{0\le k\le n}(\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(k)}\mathbb{T}\right) \;\cup\; (\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(n+1)}\mathbb{T} \\
= & (\!|\mathrm{grd}^{\neg b}|\!)\mathbb{G}^{\mathbb{T}}_{n+1} \;\cup\; (\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(n+1)}\mathbb{T} \\
= & \mathbb{Y}^{\mathbb{T}}_{n+1} \;\cup\; (\!|\mathrm{grd}^{\neg b}|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(n+1)}\mathbb{T} \\
= & \mathbb{Y}^{\mathbb{T}}_{n+1} \;\cup\; \{(\!|\,\mathrm{grd}^{\neg b}\,|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(n+1)}T \mid T \in \mathbb{T}\} \\
= & \quad \wr \text{ using the definition of } \mathcal{F}\text{, see below } \int \\
 & \mathbb{Y}^{\mathbb{T}}_{n+1} \;\cup\; \left\{\{\mathcal{F}^{(n+2)}(\bot)(t) \mid t \in T\} \mid T \in \mathbb{T}\right\} \\
= & \mathbb{Y}^{\mathbb{T}}_{n+1} \;\cup\; \mathbb{X}^{\mathbb{T}}_{n+2}
\end{array}
$$

This concludes the proof of (2). Apropos the penultimate step, the set $(\!|\,\mathrm{grd}^{\neg b}\,|\!) \circ (\!|\textbf{if } (b) \textbf{ then } c \,|\!)^{(n+1)}T$ is the traces that exit the loop body after at most $n+1$ iterations.

Marc Gotliboym observed that if $\mathbb{T}$ is ssc, we can show $\mathbb{Y}^{\mathbb{T}}_n = \mathbb{X}^{\mathbb{T}}_n$ for all n. As a first step, recall that the sequence $(x^T_n)_{n\ge 0}$ satisfies $x^T_n \subseteq x^T_{n+1}$ for any T.

Lemma 4. If $\mathbb{T}$ is ssc then $\mathbb{X}^{\mathbb{T}}_n \subseteq \mathbb{X}^{\mathbb{T}}_{n+1}$ for all n.

Proof. Recall that $\mathbb{X}^{\mathbb{T}}_n = \{x^T_n \mid T \in \mathbb{T}\}$. Define $T\lfloor n \triangleq \{t \in T \mid \mathcal{F}^{(n)}(\bot)(t) \in \mathbf{Trc}\}$ so that by definitions we have $x^{T\lfloor n}_{n+1} = x^T_n$ and $T\lfloor n \subseteq T$ (for all n, T). To show $\mathbb{X}^{\mathbb{T}}_n \subseteq \mathbb{X}^{\mathbb{T}}_{n+1}$, observe for any S

$$
\begin{array}{rl}
 & S \in \mathbb{X}^{\mathbb{T}}_n \\
\iff & \quad \wr \text{ def } \mathbb{X}^{\mathbb{T}}_n \int \\
 & \exists T \in \mathbb{T},\ S = x^T_n \\
\iff & \quad \wr \text{ by } x^{T\lfloor n}_{n+1} = x^T_n \int \\
 & \exists T \in \mathbb{T},\ S = x^{T\lfloor n}_{n+1} \\
\implies & \quad \wr \text{ taking } T' = T\lfloor n \text{ and using } T\lfloor n \subseteq T \text{ and } \mathbb{T} \text{ is ssc } \int \\
 & \exists T' \in \mathbb{T},\ S = x^{T'}_{n+1} \\
\iff & \quad \wr \text{ def } \int \\
 & S \in \mathbb{X}^{\mathbb{T}}_{n+1}
\end{array}
$$

□

Theorem 5. If $\mathbb{T}$ is ssc then $\mathbb{Y}_n^{\mathbb{T}} = \mathbb{X}_n^{\mathbb{T}}$ for all n.

Proof. By induction on n. For the base case, we have $\mathbb{Y}_0^{\mathbb{T}} = \mathbb{X}_0^{\mathbb{T}}$ by definitions. For the induction step, suppose $\mathbb{Y}_n^{\mathbb{T}} = \mathbb{X}_n^{\mathbb{T}}$ and observe

$$\begin{array}{ll} & \mathbb{Y}_{n+1}^{\mathbb{T}} \\ = & \quad \wr \text{ by (2) } \int \\ & \mathbb{Y}_n^{\mathbb{T}} \cup \mathbb{X}_{n+1}^{\mathbb{T}} \\ = & \quad \wr \text{ induction hypothesis } \int \\ & \mathbb{X}_n^{\mathbb{T}} \cup \mathbb{X}_{n+1}^{\mathbb{T}} \\ = & \quad \wr \text{ Lemma 4 } \int \\ & \mathbb{X}_{n+1}^{\mathbb{T}} \end{array}$$

□

To apply the Theorem about loops to the hypercollecting semantics of other commands, the following property of the double direct image is helpful. For any relation $R \subseteq A \times B$ between sets, let $\langle R \rangle : \mathcal{P}(A) \to \mathcal{P}(B)$ the direct image function.

Lemma 6. If R is a partial function then $\langle\langle R \rangle\rangle : \mathcal{P}(\mathcal{P}(A)) \to \mathcal{P}(\mathcal{P}(B))$ preserves ssc.

Proof. Suppose $\mathbb{T}$ is ssc. Suppose $S \in \langle\langle R \rangle\rangle \mathbb{T}$, so there is $T \in \mathbb{T}$ with $S = \langle R \rangle T$. Let $S' \subseteq S$. To show $S' \in \langle\langle R \rangle\rangle \mathbb{T}$, define T' by $x \in T' \iff x \in T \wedge \exists y \in S',\ xRy$. We have $T' \in \mathbb{T}$ by ssc. We have $S' = \langle R \rangle T'$ because for any y

$$\begin{array}{ll} & y \in \langle R \rangle T' \\ \iff & \quad \wr \text{ def } \langle - \rangle \int \\ & \exists x,\ x \in T' \wedge xRy \\ \iff & \quad \wr \text{ def } T' \int \\ & \exists x,\ (x \in T \wedge \exists y' \in S',\ xRy') \wedge xRy \\ \iff & \quad \wr \ R \text{ is a partial function } \int \\ & \exists x,\ x \in T \wedge y \in S' \wedge xRy \\ \iff & \quad \wr \ y \in S' \text{ and } S' \subseteq S = \langle R \rangle T \text{ imply } \exists x \in T,\ xRy \int \\ & y \in S' \end{array}$$

□

Corollary 7. If $\mathbb{T}$ is ssc then (1) holds as an equality, i.e., $(\!|c|\!)\mathbb{T} = \{\{\!|c|\!\}T \mid T \in \mathbb{T}\}$ for any c.

Proof. By induction on c. The base cases (skip and assignment) are immediate, as is the conditional command which is defined as a double direct image. For loop we appeal to Theorem 5. For sequence, recall that $(\!|c_1; c_2|\!)\mathbb{T}$ is defined to be $(\!|c_2|\!) \circ (\!|c_1|\!)\mathbb{T}$.

By induction, $(\!|c_1|\!)\mathbb{T} = \langle\{\!|c_1|\!\}\rangle\mathbb{T}$ which is ssc by Lemma 6.[1] So we can appeal to the induction hypothesis for $(\!|c_2|\!)$ and we get $(\!|c_1; c_2|\!)\mathbb{T} = \{\{\!|c_1; c_2|\!\}T \mid T \in \mathbb{T}\}$ because direct images distribute over composition. □

What is the upshot?

Recall that the goal is to prove c satisfies hyperproperty $HP \in \mathcal{P}(\mathcal{P}(\mathbf{Trc}))$, i.e. $\{\!|c|\!\}\,\mathbf{IniTrc} \in HP$, by an argument of the form

$$\{\!|c|\!\}\,\mathbf{IniTrc} \quad\in\quad (\!|c|\!)(\gamma(a)) \quad\subseteq\quad \gamma((\!|c|\!)^\sharp(a)) \quad\subseteq\quad HP$$

where a is some abstract value such that $\mathbf{IniTrc} \in \gamma(a)$. The middle containment expresses soundness of the abstract interpretation $(\!|-|\!)^\sharp$. In case the abstraction is such that images of γ are ssc, the membership on the left is losing no precision.

Finally, recall that the hypercollecting semantics is not compositional, owing to the case of conditionals which is defined as the direct image of the collecting semantics:

$$(\!|\mathbf{if}\ b\ \mathbf{then}\ c_1\ \mathbf{else}\ c_2|\!)\mathbb{T} \triangleq \{\{\!|c_1|\!\} \circ \{\!|\,\mathrm{grd}^b\,|\!\}T \cup \{\!|c_2|\!\} \circ \{\!|\,\mathrm{grd}^{\neg b}\,|\!\}T \mid T \in \mathbb{T}\} \tag{4}$$

A peculiar consequence is that if c is a loop, $(\!|c|\!)$ is not equal to $(\!|\mathbf{if}\ (true)\ \mathbf{then}\ c\ \mathbf{else\ skip}|\!)$ in general. One may consider alternatives to (4), such as this one:

$$\begin{array}{l}(\!|\mathbf{if}\ b\ \mathbf{then}\ c_1\ \mathbf{else}\ c_2|\!)\mathbb{T}\\ \triangleq \{T_1 \cup T_2 \mid \exists T \in \mathbb{T},\ T_1 \in (\!|c_1|\!)\{\{\!|\,\mathrm{grd}^b\,|\!\}T\} \text{ and } T_2 \in (\!|c_2|\!)\{\{\!|\,\mathrm{grd}^{\neg b}\,|\!\}T\}\}\end{array} \tag{5}$$

Corollary 7 justifies the use of (4) at least for ssc hyperproperties.

The derivation of the cardinality abstraction in the arXiv version is slightly obscure, in that the induction hypothesis is about $(\!|-|\!)$ not $\{\!|-|\!\}$, yet (4) is used. But there's no problem because the concretisation γ_{crdtr} yields ssc sets-of-sets (as does γ_{deptr} according to Prop. 3), and ssc is preserved by $(\!|-|\!)$ according to Corollary 7 and Lemma 6. So we have explained the remark in the appendix of [ANS+17].

References

[AN16] Mounir Assaf and David Naumann. Calculational design of information flow monitors. In *IEEE Computer Security Foundations Symposium*, pages 210–224, 2016. Full version `https://arxiv.org/abs/1605.02778`.

[ANS+17] Mounir Assaf, David A. Naumann, Julien Signoles, Éric Totel, and Frédéric Tronel. Hypercollecting semantics and its application to static analysis of information flow. In *ACM Symposium on Principles of Programming Languages*, pages 874–887, 2017. Full version `https://arxiv.org/abs/1608.01654`.

[1] Recall that $\{\!|c|\!\}$ is defined in terms of the denotational semantics $[\![c]\!]$ by discarding the $\bot$ outcomes, effectively treating $[\![c]\!]$ as a partial function.

[Ass15] Mounir Assaf. From qualitative to quantitative program analysis: Permissive enforcement of secure information flow. Technical report, Université Rennes 1, 2015.

[CP10] David Cachera and David Pichardie. A certified denotational abstract interpreter. In *Interactive Theorem Proving (ITP)*, pages 9–24, 2010.

[CS10] Michael R Clarkson and Fred B Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010.

[MP17] Isabella Mastroeni and Michele Pasqua. Hyperhierarchy of semantics - A formal framework for hyperproperties verification. In Francesco Ranzato, editor, *Static Analysis Symposium*, volume 10422 of *LNCS*, pages 232–252, 2017.