Automated Monotone GC for Distributed Programming

Xinghao Pan
xinghao@eecs.berkeley.edu

Abstract

Edelweiss [1] provides automatic garbage collection for event log exhanges, programs which monotonically accumulate logs. However, in the process of doing so, it introduced additional points of coordination through non-monotone operations, thereby defeating the original purpose of ELEs to avoid synchronization and coordination. In this paper, we show that garbage collection for ELEs can in fact be monotone and coordination-free. We explicitly recast Edelweiss techniques as monotone operations on lattices defined over the input sets.

1 Approach

Plan of attack:

1. Promote all operations to tombstone sets.
2. Add (logical) GC rules.
   - Require that GC rules maintain a GC invariant, are monotone, and conservative (only promotes $\exists$ to $\top$ and not create new tuples)
   - Show that rewritten (logical) program is correct, monotone, and preserves GC invariant.
3. Instantiate representation, add instantiated GC (GCI) rules.
   - Require GCI rules delete only things that are (logically) tombstoned.
   - Show that representation maintains invariant – always keeps $\exists$ but possibly also tombstoned tuples.

Our approach proceeds in two phases. Firstly, we add (logical) rules that identifies 'tombstone' tuples – these are tuples whose removal does not affect the correctness of the program, in the sense that the output sets in the rewritten program are unaffected. We further require that the GC rules are monotone.

The second phase then rewrites the program to perform the actual deletion. Here, we ensure that deleted tuples are tombstoned, but tombtoned tuples are not necessarily deleted. This invariance ensures that the instantiated representation corresponds to the logical program in the first phase, and in particular, instantiated representations of the output sets (which have no tombstones) are correct.

However, we do not require the representation to be monotone; in particular, a deleted tombstone tuple could potentially be re-instantiated without affecting the correctness of the program. Nevertheless, since we are maintaining equivalence to the logical, monotone program, we may execute operations in a coordination-free manner.

2 Logical rewrite

In this section, we present a logical rewrite of the original program. We first endow all sets with 'tombstone' sets – intuitively, tombstoned tuples are that which we may safely delete without affecting the outcome of our program. We then add logical GC rules that define how we can identify and mark tombstoned tuples. The logical GC rules have to obey certain properties which will ensure correctness and monotonicity.

In the remainder of this write-up, we will consider rewrite the general rule, for arbitrary `A`:

```
B <= f(A)
```
(2.1)

Note that we do not require `f` to be monotone. In cases where `f` is non-monotone, the program remains non-monotone; however, our rewrites do not introduce additional non-monotone operations, and thus there are no

new points of order added. [1] For simplicity, we will assume that each input set only participates in one rule – we avoid multi-output situations by using copy rules, and handle copy rules separately.

2.1 Adding tombstones

Our first step is to lift all sets to a 3-phase set by endowing with an additional 'tombstone' state. Instead of having a single set $\texttt{A}$, we use a tuple $\texttt{A}_{\text{TS}} = (\texttt{A}_\neg, \texttt{A}_\exists, \texttt{A}_\top)$ of three mutually exclusive sets. Intuitively, tuples in $\texttt{A}_\top$ are those that would have been in the original set $\texttt{A}$, but are now also marked for reclamation. Conversely, tuples in $\texttt{A}_\exists$ are also in $\texttt{A}$ but not marked for reclamation.

2.2 Logical garbage collection

Armed with this lifted representation, we can now provide a rewrite of the original program, together with an additional GC rule for each rule.

$$\text{Forward rule:} \qquad \texttt{B}_{\text{TS}} \texttt{ <= } \exists(\texttt{f}(\texttt{A}_\exists \cup \texttt{A}_\top)) \tag{2.2}$$

$$\text{GC rule:} \qquad \texttt{A}_{\text{TS}} \texttt{ <= GC}(\texttt{A}_{\text{TS}}\texttt{, f, B}_{\text{TS}}) \tag{2.3}$$

The function $\exists(\texttt{S})$ takes a set $\texttt{S}$ and returns $(\emptyset, \texttt{S}, \emptyset)$, and is a monotone function. The $\texttt{GC}$ function takes TS sets and the functional relationship, and returns a new TS set with additional tombstoned tuples. We will make this notion formal below.

For this rewrite to preserve correctness and monotonicity, we will require that the following invariance is maintained by the forward rule, the GC rule, and under arbitrary merges.

Invariant 2.1 (GC Invariance) *For any set A that participates in rules B_i <= $f_i(A)$ for $i = 1, \ldots, k$, we require*

$$\forall i, \quad \forall \hat{A} \supseteq A_\exists, \quad f_i(\hat{A}) \cup B_{i,\exists} \cup B_{i,\top} = f_i(\hat{A} \cup A_\top) \cup B_{i,\exists} \cup B_{i,\top} \tag{2.4}$$

Furthermore, for A_{TS} and A'_{TS} satisfying Eq (2.4), it must be that

$$\forall i, \quad \forall \hat{A} \supseteq A_\exists \cup A'_\exists - (A_\top \cup A'_\top), \quad f_i(\hat{A}) \cup B_{i,\exists} \cup B_{i,\top} = f_i(\hat{A} \cup A_\top \cup A'_\top) \cup B_{i,\exists} \cup B_{i,\top} \tag{2.5}$$

Eq (2.4) ensures that any tombstoned tuple can be safely deleted, since any tuple it may generate (for any possible future input) is already present in the output set, and thus the tombstoned tuple has no downstream effect. The second condition Eq (2.5) is required to ensure that Eq (2.4) is preserved under merges for input sets $\texttt{A}_{\text{TS}}$.

Additionally, we require that the $\texttt{GC}$ rule have the properties stated below.

Property 2.2 (GC Rule Invariance) *Any GC rule must maintain Invariant 2.1.*

Property 2.3 (GC Rule Monotonicity) *Suppose $A_{TS} \leq A'_{TS}$, and $B_{TS} \leq B'_{TS}$. If (A_{TS}, B_{TS}) and (A'_{TS}, B'_{TS}) both satisfy GC Invariant 2.1, then GC(A, f, B) $\leq$ GC(A', f, B').*

Property 2.4 (GC Rule Conservation) *Let $G_{TS} = (G_\neg, G_\exists, G_\top) =$ GC(A, f, B). Then it must be the case that $G_\exists \subseteq A_\exists$, and $A_\top \subseteq G_\top \subseteq A_\exists \cup A_\top$, and $G_\exists \cup G_\top = A_\exists \cup A_\top$.*

Property 2.3 ensures that the GC rules are monotone, and Property 2.4 only moves tuples from $\texttt{A}_\exists$ to $\texttt{A}_\top$.

[1] I believe, however, that we will require that any set that appears as an input is monotonically growing, i.e. there are no deletions. This should be guaranteed by Edelweiss's requirement that there are no deletion rules.

2.2.1 Examples

While the above properties are reasonable expectations of garbage collection rules, it is not obvious that there are useful rules that satisfy them. We now show some examples of such rules.

Example 2.1 (Trivial GC) $\mathit{GCtrivial}(A_{TS}, f, B_{TS}) = A_{TS}$.

Example 2.2 (Copy GC) $\mathit{GCcopy}(A_{TS}, Id, B_{1,TS}, \ldots, , B_{k,TS}) = (\emptyset, A_\exists - B_\cap, A_\top \cup B_\cap)$, *where* $B_\cap = A_\exists \cap \bigcap_{i=1}^{k}(B_{i,\exists} \cup B_{i,\top})$.

For the copy rule, the GC Invariant 2.1 reduces to

$$\forall i, \mathtt{A}_\top \subseteq \mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top}, \tag{2.6}$$

$$\forall i, \mathtt{A}_\top \cup \mathtt{A}'_\top \subseteq \mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top}. \tag{2.7}$$

Suppose $\mathtt{A}_{\mathrm{TS}}$ satisfies the GC invariant Eq (2.6). Then, $\forall i, \mathtt{A}_\top \cup \mathtt{B}_\cap \subseteq \mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top}$, so `GCcopy` preserves Eq (2.6). Suppose $\mathtt{A}'_{\mathrm{TS}}$ satisfies the GC invariant Eq (2.6). Then $\forall i, \mathtt{A}_\top \cup \mathtt{B}_\cap \cup \mathtt{A}'_\top \subseteq \mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top}$, so `GCcopy` preserves Eq (2.7).

The GC Rule Conservation Property 2.4 is straightforward.

Suppose $\mathtt{A}'_{\mathrm{TS}} \geq \mathtt{A}_{\mathrm{TS}}$, i.e., $\mathtt{A}'_\top \supseteq \mathtt{A}_\top$ and $\mathtt{A}'_\top \cup \mathtt{A}'_\exists \supseteq \mathtt{A}_\top \cup \mathtt{A}_\exists$. Suppose also $\mathtt{A}'_{\mathrm{TS}}$ satisfies the GC Invariant 2.1 with respect to $\mathtt{B}'_{i,\mathrm{TS}} \geq \mathtt{B}_{i,\mathrm{TS}}$. Then

$$\begin{aligned}
\mathtt{A}_\top \cup \left(\mathtt{A}_\exists \cap \bigcap_{i=1}^{k}(\mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top})\right) &\subseteq \mathtt{A}'_\top \cup \left((\mathtt{A}'_\exists \cup \mathtt{A}'_\top) \cap \bigcap_{i=1}^{k}(\mathtt{B}'_{i,\exists} \cup \mathtt{B}'_{i,\top})\right) \\
&= \mathtt{A}'_\top \cup \left(\mathtt{A}'_\exists \cap \bigcap_{i=1}^{k}(\mathtt{B}'_{i,\exists} \cup \mathtt{B}'_{i,\top})\right) \cup \left(\mathtt{A}'_\top \cap \bigcap_{i=1}^{k}(\mathtt{B}'_{i,\exists} \cup \mathtt{B}'_{i,\top})\right) \\
&= \mathtt{A}'_\top \cup \left(\mathtt{A}'_\exists \cap \bigcap_{i=1}^{k}(\mathtt{B}'_{i,\exists} \cup \mathtt{B}'_{i,\top})\right),
\end{aligned}$$

where the final equality follows because $\forall i = 1, \ldots, k,\ \mathtt{A}'_\top \subseteq \mathtt{B}'_{i,\exists} \cup \mathtt{B}'_{i,\top}$. Furthermore, it follows from the GC Rule Conservation Property 2.4, we also have that $(\mathtt{A}_\exists - \mathtt{B}_\cap) \cup (\mathtt{A}_\top \cup \mathtt{B}_\cap) \subseteq (\mathtt{A}'_\exists - \mathtt{B}'_\cap) \cup (\mathtt{A}'_\top \cup \mathtt{B}'_\cap)$. Hence, `GCcopy` is monotone.

Example 2.3 (Max GC) $\mathit{GCmax}(A_{TS}, f, B_{TS}) = (\emptyset, A_\exists - \tilde{A}, \tilde{A})$ *where* $A_\top \subseteq \tilde{A} \subseteq A_\exists \cup A_\top$ *is the (unique) largest set such that*

$$\forall \hat{A} \supseteq A_\exists - \tilde{A}, \quad f(\hat{A}) \cup B_\exists \cup B_\top = f(\hat{A} \cup \tilde{A} \cup A_\top) \cup B_\exists \cup B_\top, \tag{2.8}$$

and for any A'_{TS} *satisfying the GC Invariant 2.1 Eq* (2.4)*,*

$$\forall \hat{A} \supseteq A_\exists \cup A'_\exists - (\tilde{A} \cup A_\top \cup A'_\top), \quad f(\hat{A}) \cup B_\exists \cup B_\top = f(\hat{A} \cup \tilde{A} \cup A_\top \cup A'_\top) \cup B_\exists \cup B_\top. \tag{2.9}$$

The `GCmax` rule returns the largest set of tombstones that can be safely deleted without interfering with other tombstones. It also most directly attempts to maintain the GC invariant.

For this rule to make sense, we need to show that it is in fact well-defined, i.e., there is a unique largest set that achieves the conditions. Suppose there are sets $\mathtt{X}$ and $\mathtt{Y}$ that achieve both conditions. Then $\mathtt{Z} = \mathtt{X} \cup \mathtt{Y}$ also fulfills our two conditions. First, note that since $\mathtt{X}$ and $\mathtt{Y}$ both satisfy Eq (2.8) and Eq (2.9), the TS sets $(\mathtt{A}_\neg, \mathtt{A}_\exists - \mathtt{X}, \mathtt{X} \cup \mathtt{A}_\top)$ and $(\mathtt{A}_\neg, \mathtt{A}_\exists - \mathtt{Y}, \mathtt{Y} \cup \mathtt{A}_\top)$ satisfy Invariant 2.1. Applying Eq (2.9), we have

$$\begin{aligned}
\forall \hat{\mathtt{A}} \ &\supseteq\ \mathtt{A}_\exists \cup (\mathtt{A}_\exists - \mathtt{Y}) - (\mathtt{X} \cup \mathtt{A}_\top \cup \mathtt{Y} \cup \mathtt{A}'_\top) \ = \ \mathtt{A}_\exists - (\mathtt{X} \cup \mathtt{Y}) \ = \ \mathtt{A}_\exists - \mathtt{Z}, \\
\mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top \ &=\ \mathtt{f}(\hat{\mathtt{A}} \cup \mathtt{X} \cup \mathtt{A}_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top \ = \ \mathtt{f}(\hat{\mathtt{A}} \cup \mathtt{X} \cup \mathtt{Y} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top,
\end{aligned}$$

where we have used the fact that $\hat{\mathtt{A}} \cup \mathtt{X} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top \supseteq \mathtt{A}_\exists - \mathtt{Y}$ and Eq (2.8) for $\mathtt{Y}$. Hence, $\mathtt{Z}$ satisfies Eq (2.8).

Furthermore, for any $\mathtt{A}'_{\mathrm{TS}}$ satisfying the GC Invariant 2.1 Eq (2.4), applying Eq (2.9) to $\mathtt{X}$, we get

$$\forall \hat{\mathtt{A}} \supseteq \mathtt{A}_\exists \cup \mathtt{A}'_\exists - (\mathtt{X} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top), \qquad \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top = \mathtt{f}(\hat{\mathtt{A}} \cup \mathtt{X} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top,$$

so $\mathtt{A}''_{\mathrm{TS}} = (\emptyset, (\mathtt{A}_\exists \cup \mathtt{A}'_\exists) - (\mathtt{X} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top), \mathtt{X} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top)$ satisfies Eq (2.4). We can then apply Eq (2.9) to $\mathtt{Y}$:

$$\begin{aligned}\forall \hat{\mathtt{A}} &\supseteq \mathtt{A}_\exists \cup \mathtt{A}''_\exists - (\mathtt{Y} \cup \mathtt{A}_\top \cup \mathtt{A}''_\top) = \mathtt{A}_\exists \cup \mathtt{A}'_\exists - (\mathtt{X} \cup \mathtt{Y} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top),\\ \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top &= \mathtt{f}(\hat{\mathtt{A}} \cup \mathtt{Y} \cup \mathtt{A}_\top \cup \mathtt{A}''_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top = \mathtt{f}(\hat{\mathtt{A}} \cup \mathtt{X} \cup \mathtt{Y} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top.\end{aligned}$$

Hence $\mathtt{Z}$ also satisfies Eq (2.9). Thus, there is a unique largest set that achieves Eq (2.8) and (2.9).

It is easy to see `GCmax` maintains the GC Invariant 2.1, since Eq (2.8) satisfies Eq (2.4) and Eq (2.9) satisfies Eq (2.5). Similarly, the GC Rule Conservation Property 2.4 is also maintained by the choice of $\mathtt{A}_\top \subseteq \tilde{\mathtt{A}} \subseteq \mathtt{A}_\exists \cup \mathtt{A}_\top$.

To show monotonicity, suppose we have $\mathtt{A}_{\mathrm{TS}} \leq \mathtt{A}'_{\mathrm{TS}}$ and $\mathtt{B}_{\mathrm{TS}} \leq \mathtt{B}'_{\mathrm{TS}}$. Monotonicity in the $\mathtt{B}$ argument is easy: Eq (2.8) and (2.9) for $\mathtt{B}_{\mathrm{TS}}$ immediately implies the same for $\mathtt{B}'_{\mathrm{TS}}$. For the $\mathtt{A}$ argument, we observe that $\tilde{\mathtt{A}} \cup \mathtt{A}'_\top$ satisfies conditions Eq (2.8) and Eq (2.9) as applied to $\mathtt{A}'_{\mathrm{TS}}$. For condition Eq (2.8),

$$\begin{aligned}\forall \hat{\mathtt{A}} \supseteq \mathtt{A}'_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top) &= (\mathtt{A}'_\exists \cup (\mathtt{A}_\exists - \mathtt{A}'_\top)) - (\tilde{\mathtt{A}} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top) = \mathtt{A}'_\exists \cup \mathtt{A}_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}_\top \cup \mathtt{A}'_\top),\\ f(\hat{\mathtt{A}}) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top &= f(\hat{\mathtt{A}} \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top,\end{aligned}$$

where we have applied Eq (2.9) for $\mathtt{A}_{\mathrm{TS}}$ and $\mathtt{B}'_{\mathrm{TS}}$. Also, for any $\mathtt{A}''_{\mathrm{TS}}$ that satisfies Eq (2.4),

$$\begin{aligned}\forall \hat{\mathtt{A}} &\supseteq \mathtt{A}_\exists \cup \mathtt{A}''_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}_\top \cup \mathtt{A}''_\top) = \mathtt{A}_\exists \cup \mathtt{A}''_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top),\\ \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top &= \mathtt{f}(\hat{\mathtt{A}} \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}_\top \cup \mathtt{A}''_\top) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top = \mathtt{f}(\hat{\mathtt{A}} \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top,\end{aligned}$$

so $(\emptyset, \mathtt{A}_\exists \cup \mathtt{A}''_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top), \tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top)$ satisfies Eq (2.4). Repeating the process for $\mathtt{A}'_{\mathrm{TS}}$,

$$\begin{aligned}\forall \hat{\mathtt{A}} &\supseteq \mathtt{A}'_\exists \cup (\mathtt{A}_\exists \cup \mathtt{A}''_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top)) - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top \cup \mathtt{A}''_\top) = \mathtt{A}'_\exists \cup \mathtt{A}''_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top),\\ \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top &= \mathtt{f}(\hat{\mathtt{A}} \cup \mathtt{A}'_\top \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top = \mathtt{f}(\hat{\mathtt{A}} \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top \cup \mathtt{A}''_\top) \cup \mathtt{B}'_\exists \cup \mathtt{B}'_\top,\end{aligned}$$

satisfying Eq (2.9). Therefore, $\tilde{\mathtt{A}} \cup \mathtt{A}'_\top$ is a valid set of tombstones for `GCmax(A_TS', f, B_TS')`, and so `GCmax(A_TS', f, B_TS')` $\supseteq \tilde{\mathtt{A}} \cup \mathtt{A}'_\top \supseteq \tilde{\mathtt{A}} =$ `GCmax(A_TS, f, B_TS)`.

We also point out that `GCmax` is complete in the sense that any $\tilde{\mathtt{A}}$ that satisfies Eq (2.8) and (2.9) will necessarily be $\tilde{\mathtt{A}} \subseteq$ `GCmax(A_TS, f, B_TS)` due to the maximality of `GCmax`, so any tuple that could be deleted (per Eq (2.8) and (2.9)) will be tombstoned. (However, it may not be truly complete. For example, if we have $C <= A \bowtie B$, $D <= \pi_A(C)$, then we can always delete any tuple of B, but our rule does not allow for this.)

The `GCmax` rule may be hard to evaluate in practice, so we provide an easier rule below.

Example 2.4 (Tuple-based GC) *`GC(A_TS, f, B_TS)` $= (\emptyset, \mathtt{A}_\exists - \tilde{\mathtt{A}}, \tilde{\mathtt{A}})$ where $\tilde{\mathtt{A}} = \mathtt{A}_\top \cup \{t \in \mathtt{A}_\exists : \forall X, \mathtt{f}(X \cup \{t\}) - \mathtt{f}(X) \subseteq \mathtt{B}_\exists \cup \mathtt{B}_\top\}$.*

2.3 Invariance, Correctness, Monotonicity

Theorem 2.1 (GC Invariance) *The GC Invariant 2.1 is maintained by the rewritten program.*

Proof: Our proof proceeds by showing that the initial conditions satisfy the invariant, and the forward, GC rules and merges preserve the invariant.

The program is initialized with $\mathtt{A}_\exists = \mathtt{A}$ and $\mathtt{A}_\top = \emptyset$, so the invariant is immediately satisfied.

There are two forward rules that we consider: `B_TS <= ∃(f(A_∃ ∪ A_⊤))` as well as rules that merge into $\mathtt{A}_{\mathrm{TS}}$. In the first case, we increase $\mathtt{B}_\exists$ while keeping $\mathtt{B}_\top$ constant, so Eq (2.4) and (2.5) are preserved. In the second case, $\mathtt{A}_\exists$ is increased while $\mathtt{A}_\top$ is kept constant – let $\mathtt{A}^{t+1}_\exists$ be the new value of $\mathtt{A}_\exists$. Since $\mathtt{A}^{t+1}_\exists \supseteq \mathtt{A}_\exists$, the GC invariance of $\mathtt{A}_{\mathrm{TS}}$ implies the GC invariance of $\mathtt{A}^{t+1}_{\mathrm{TS}}$.

GC on $\mathtt{A}_{\mathrm{TS}}$ maintains the GC invariance due to the GC Rule Invariance Property 2.2. GC on $\mathtt{B}_{\mathrm{TS}}$ maintains the GC invariance due to the GC Rule Conservation Property 2.4.

Merges on $\mathtt{B}_{\mathrm{TS}}$ increases $\mathtt{B}_\exists \cup \mathtt{B}_\top$, so the GC invariance is immediately preserved.

Finally, we consider a merge of $\mathtt{A}_{\mathrm{TS}}$ and $\mathtt{A}'_{\mathrm{TS}}$. Due to Eq (2.9), the merge of $\mathtt{A}_{\mathrm{TS}}$ and $\mathtt{A}'_{\mathrm{TS}}$ preserves Eq (2.4). Now if we have a further $\mathtt{A}''_{\mathrm{TS}}$ satisfying Eq (2.4), we note that (1) Eq (2.5) for $\mathtt{A}_{\mathrm{TS}}$ implies that the merge of $\mathtt{A}_{\mathrm{TS}}$ and $\mathtt{A}''_{\mathrm{TS}}$ preserves Eq (2.4), and thus (2) Eq (2.5) for $\mathtt{A}''_{\mathrm{TS}}$ implies that the merge of $\mathtt{A}''_{\mathrm{TS}}$ with the merge of $\mathtt{A}_{\mathrm{TS}}$ and $\mathtt{A}''_{\mathrm{TS}}$ preserves Eq (2.4). Together, this implies that Eq (2.5) is maintained through a merge of $\mathtt{A}_{\mathrm{TS}}$ with $\mathtt{A}'_{\mathrm{TS}}$. □

Theorem 2.2 (Monotonicity) *The program rewrite does not introduce new points of order.*

Proof: Monotonicity of GC rules is implied via GC Rule Monotonicity 2.3. Furthermore, if `f` is monotone, then the composition of $\exists \circ \mathtt{f}$ is also monotone, so the forward rule is monotone. □

To show correctness of the logical program rewrite, we will show that the following invariant is maintained.

Invariant 2.5 (Logical Invariant) $A = A_\exists \cup A_\top$.

Theorem 2.3 (Correctness) *The program maintains the Logical Invariant 2.5. In particular, for output sets A which have no downstream operations, we have $A_\top = \emptyset$ so $A = A_\exists$.*

Proof: We will proceed via induction on the execution of the rewritten program. Let $\mathtt{A}^t_{\mathrm{TS}}$ denote the value of $\mathtt{A}_{\mathrm{TS}}$ after executing t rules in the rewritten program. Simultaneously, we run the original program, executing the corresponding step whenever the forward rule or a merge is executed, and performing a noop when we run a GC rule. (Note that every execution of the original program corresponds to some execution of the rewritten program.) Using analogous notation, let $\mathtt{A}^t$ denote the value of `A` after executing t rules of the rewritten program (so $\mathtt{A}^{t+1} = \mathtt{A}^t$ if we run a GC rule).

Observe that the initialization gives $\mathtt{A}^0 = \mathtt{A}^0_\exists$.

Consider the execution of the forward rule $\mathtt{B_{TS}} \texttt{ <= } \exists(\mathtt{f}(\mathtt{A}_\exists \cup \mathtt{A}_\top)$, which we can equivalently write as $\mathtt{B}^t_\exists = \mathtt{B}^{t-1}_\exists \cup \mathtt{f}(\mathtt{A}^{t-1}_\exists \cup \mathtt{A}^{t-1}_\top)$, and $\mathtt{B}^t_\top = \mathtt{B}^{t-1}_\top$. Thus,

$$\begin{aligned}
\mathtt{B}^t_\exists \cup \mathtt{B}^t_\top &= \mathtt{B}^{t-1}_\exists \cup \mathtt{f}(\mathtt{A}^{t-1}_\exists \cup \mathtt{A}^{t-1}_\top) \cup \mathtt{B}^t_\top \\
&= \mathtt{B}^{t-1}_\exists \cup \mathtt{f}(\mathtt{A}^{t-1}) \cup \mathtt{B}^{t-1}_\top \\
&= \mathtt{B}^{t-1} \cup \mathtt{f}(\mathtt{A}^{t-1}) \\
&= \mathtt{B}^t.
\end{aligned}$$

No other sets are altered by the forward rule.

The GC Rule Conservation Property 2.4 ensures that $\mathtt{A}^t_\exists \cup \mathtt{A}^t_\top = \mathtt{A}^{t-1}_\exists \cup \mathtt{A}^{t-1}_\top = \mathtt{A}^{t-1} = \mathtt{A}^t$.

Finally, consider the merge of $\mathtt{A}^{t-1}_{\mathrm{TS}}$ with $\mathtt{A}'^{(t-1)}_{\mathrm{TS}}$:

$$\mathtt{A}^t_\exists \cup \mathtt{A}^t_\top \;=\; \mathtt{A}^{t-1}_\exists \cup \mathtt{A}^{t-1}_\top \cup \mathtt{A}'^{(t-1)}_\exists \cup \mathtt{A}'^{(t-1)}_\top \;=\; \mathtt{A}^{t-1} \cup \mathtt{A}'^{(t-1)} \;=\; \mathtt{A}^t$$

Thus, we have $\mathtt{A} = \mathtt{A}_\exists \cup \mathtt{A}_\top$. Furthermore, since output sets have no downstream operations, they have no associated GC rules, and never gather any tombstones. Therefore for an output set A, we always maintain $\mathtt{A} = \mathtt{A}_\exists \cup \mathtt{A}_\top = \mathtt{A}_\exists$. □

3 Representation

In the previous section, we described a rewrite with logical GC which ensures correctness and monotonicity. However, the garbage collection only marks tuples for possible deletion, and thus does not actually reclaim any storage. Here, we present a second rewrite that does in fact reclaim storage.

To achieve storage reclamation, our second rewrite will use a representation that is non-monotone. However, the representation maintains an invariance with respect to the first program rewrite, so that an execution of the second rewrite corresponds to some execution of the first. As a result, monotonicity is preserved at the level of the logical program. In practice, this allows us to perform GC in a monotone, coordination-free manner.

3.1 Representation and rewrite

Instead of maintaining two sets $\mathtt{A}_\exists$ and $\mathtt{A}_\top$, we only instantiate a set $\mathtt{A}_I$ which holds all of $\mathtt{A}_\exists$ but possibly some tuples from $\mathtt{A}_\top$. Intuitively, $\mathtt{A}_I$ deletes a subset of the tombstoned tuples, which from the previous section, we know to be safe for deletion.

In place of the forward rule Eq (2.2) and GC rule Eq (2.3), we have *instantiated* rules that operate only on the instantiated sets:

$$\text{Instantiated forward rule:} \qquad \mathtt{B}_I \texttt{ <= f(}\mathtt{A}_I\texttt{)} \tag{3.1}$$

$$\text{Instantiated GC rule:} \qquad \mathtt{A}_I \texttt{ <\# GCI(}\mathtt{A}_I\texttt{, f, }\mathtt{B}_I\texttt{)} \tag{3.2}$$

Here, we use `<#` to represent a non-deferred deletion.

We require that the instantiated GC rule to have the following property, which states that `GCI` only deletes tuples that the corresponding `GC` rule has marked as tombstoned.

Property 3.1 (Instantiated GC Safe Deletion) *GCI(A_I, f, B_I) $\subseteq \tilde{A}$ where $(\emptyset, \hat{A}, \tilde{A}) =$ GC(A_{TS}, f, B_{TS}).*

3.2 Correctness

The correctness of this program rewrite is demonstrated by maintaining the following invariant.

Invariant 3.2 (Representation Invariant) $A_\exists \subseteq A_I \subseteq A_\exists \cup A_\top$.

The Representation Invariant 3.2 states that the instantiated set does not contain superfluous tuples, and it does not delete tuples that are unsafe for deletion.

Theorem 3.1 (Representation Correctness) *The Representation Invariant 3.2 is maintained by the instantiated program. In particular, for output sets A which have no downstream operations, we have $A = A_I$.*

Proof: We initialize the program with $\mathtt{A}_I^0 = \mathtt{A}^0 = \mathtt{A}_\exists^0 = \mathtt{A}_\exists^0 \cup \mathtt{A}_\top^0$ — the final two equalities are due to Thm 2.3.

First, consider the instantiated forward rule $\mathtt{B}_I$ `<= f(`$\mathtt{A}_I$`)`, which only alters $\mathtt{B}_I$ and can be expressed as $\mathtt{B}_I^t = \mathtt{B}_I^{t-1} \cup \mathtt{f}(\mathtt{A}_I^{t-1})$.

$$\begin{aligned}
\mathtt{B}_\exists^t &= \mathtt{B}_\exists^{t-1} \cup \mathtt{f}(\mathtt{A}_\exists^{t-1} \cup \mathtt{A}_\top^{t-1}) - \mathtt{B}_\top^{t-1} \\
&= \mathtt{B}_\exists^{t-1} \cup \mathtt{f}(\mathtt{A}_I^{t-1}) - \mathtt{B}_\top^{t-1} && \text{(Thm 2.1)} \\
&\subseteq \mathtt{B}_I^{t-1} \cup \mathtt{f}(\mathtt{A}_I^{t-1}) && = \mathtt{B}_I^t \\
&\subseteq \mathtt{B}_\exists^{t-1} \cup \mathtt{B}_\top^{t-1} \cup \mathtt{f}(\mathtt{A}_I^{t-1}) \\
&= \mathtt{B}_\exists^{t-1} \cup \mathtt{B}_\top^{t-1} \cup \mathtt{f}(\mathtt{A}_\exists^{t-1} \cup \mathtt{A}_\top^{t-1}) && \text{(Thm 2.1)} \\
&= \mathtt{B}_\exists^{t-1} \cup \mathtt{B}_\top^{t-1}
\end{aligned}$$

Next we show that the instantiated GC rule maintains the invariant.

$$\begin{aligned}
\mathtt{A}_\exists^t &= \mathtt{A}_\exists^{t-1} - \tilde{\mathtt{A}} \\
&\subseteq \mathtt{A}_I^{t-1} - \mathtt{GCI(A}_I\mathtt{, f, B}_I\mathtt{)} && \text{(Property 3.1)} \\
&= \mathtt{A}_I^t \\
&\subseteq \mathtt{A}_\exists^{t-1} \cup \mathtt{A}_\top^{t-1} \\
&= \mathtt{A}_\exists^t \cup \mathtt{A}_\top^t && \text{(Property 2.4)}
\end{aligned}$$

Lastly, we consider the merge $\mathtt{A}_I^t = \mathtt{A}_I^{t-1} \cup \mathtt{A}_I'^{(t-1)}$ with the corresponding merge $\mathtt{A}_{\mathrm{TS}}^t = \mathtt{A}_{\mathrm{TS}}^{t-1} \sqcup \mathtt{A}_{\mathrm{TS}}'^{(t-1)}$.

$$\begin{aligned}
\mathtt{A}_\exists^t &= \mathtt{A}_\exists^{t-1} \cup \mathtt{A}_\exists'^{(t-1)} - (\mathtt{A}_\top^{t-1} \cup \mathtt{A}_\top'^{(t-1)}) \\
&= \mathtt{A}_\exists^{t-1} \cup \mathtt{A}_\exists'^{(t-1)} \\
&\subseteq \mathtt{A}_I^{t-1} \cup \mathtt{A}_I'^{(t-1)} && = \mathtt{A}_I^t \\
&\subseteq \mathtt{A}_\exists^{t-1} \cup \mathtt{A}_\top^{t-1} \cup \mathtt{A}_\exists'^{(t-1)} \cup \mathtt{A}_\top'^{(t-1)} \\
&= \mathtt{A}_\exists^t \cup \mathtt{A}_\top^t.
\end{aligned}$$

Hence, we have shown that the Representation Invariant 3.2 is maintained by the instantiated program. Furthermore, Thm 2.3 tells us that for output sets with no downstream operations, we have $\mathtt{A}_\top = \emptyset$, so $\mathtt{A}_I = \mathtt{A}_\exists = \mathtt{A}$. □

3.3 Examples

Example 3.1 (Instantiated Trivial GC) $\mathit{GCIcopy}(A_I,\ f,\ B_I) = \emptyset$.

Example 3.2 (Instantiated Copy GC) $\mathit{GCIcopy}(A_I,\ \mathit{Id},\ B_{1,I},\ \ldots,\ B_{k,I}) = A_I \cap \bigcap_{i=1}^{k} B_{i,I}$.

The GCcopy rule creates tombstones for $\mathtt{A}_\top \cup \left(\mathtt{A}_\exists \cap \bigcap_{i=1}^{k}(\mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top})\right)$. From the Representation Invariant 3.2, we know $\mathtt{A}_\exists \subseteq \mathtt{A}_I \subseteq \mathtt{A}_\exists \cup \mathtt{A}_\top$ and $\mathtt{B}_\exists \subseteq \mathtt{B}_I \subseteq \mathtt{B}_\exists \cup \mathtt{B}_\top$. Thus,

$$\mathtt{A}_I \cap \bigcap_{i=1}^{k} \mathtt{B}_{i,I} \ \subseteq\ (\mathtt{A} \cup \mathtt{A}_\top) \cap \bigcap_{i=1}^{k}(\mathtt{B}_\exists \cup \mathtt{B}_\top) \ \subseteq\ (\mathtt{A} \cup \mathtt{A}_\top) \cap \left(\mathtt{A}_\top \cup \bigcap_{i=1}^{k}(\mathtt{B}_\exists \cup \mathtt{B}_\top)\right) \ =\ \mathtt{A}_\top \cup \left(\mathtt{A}_\exists \cap \bigcap_{i=1}^{k}(\mathtt{B}_{i,\exists} \cup \mathtt{B}_{i,\top})\right),$$

so GCIcopy satisfies the Instantiated GC Safe Deletion Property 3.1.

Example 3.3 (Instantiated Max GC) $\mathit{GCImax}(A_I,\ f,\ B_I) = \tilde{A}$, *where* $\tilde{A} \subseteq A_I$ *is a set satisfying*

$$\forall \hat{A} \supseteq A_I - \tilde{A}, \quad f(\hat{A}) \cup B_I = f(\hat{A} \ \cup\ \tilde{A}) \cup B_I, \tag{3.3}$$

and for all A'_{TS} *satisfying the GC Invariant 2.1 Eq 2.4,*

$$\forall \hat{A} \supseteq A_I \cup A'_\exists - (\tilde{A} \cup A'_\top), \quad f(\hat{A}) \cup B_I = f(\hat{A} \ \cup\ \tilde{A} \ \cup\ A'_\top) \cup B_I \tag{3.4}$$

We first point out that the GCImax rule does not require knowledge of the value of any actual $\mathtt{A}'_{\mathrm{TS}}$, as it has to hold true for *all* such sets.

Next, we show that $\tilde{\mathtt{A}} \cup \mathtt{A}_\top$ satisfies conditions Eq (2.8) and (2.9). The first condition Eq (3.3), together with the fact that $\mathtt{B}_I \subseteq \mathtt{B}_\top \cup \mathtt{B}_\exists$ implies that

$$\forall \hat{\mathtt{A}} \supseteq \mathtt{A}_I - \tilde{\mathtt{A}}, \quad \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top = \mathtt{f}(\hat{\mathtt{A}} \ \cup\ \tilde{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top,$$

so $(\emptyset, \mathtt{A}_I - \tilde{\mathtt{A}}, \tilde{\mathtt{A}})$ satisfy GC Invariant 2.1 Eq 2.4. Applying Eq 2.5, we get

$$\begin{aligned} \forall \hat{\mathtt{A}} \ &\supseteq\ \mathtt{A}_\exists \cup (\mathtt{A}_I - \tilde{\mathtt{A}}) - (\mathtt{A}_\top \cup \tilde{\mathtt{A}}) \ =\ \mathtt{A}_\exists - (\mathtt{A}_\top \cup \tilde{\mathtt{A}}), \\ \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top \ &=\ \mathtt{f}(\hat{\mathtt{A}} \ \cup\ \mathtt{A}_\top \ \cup\ \tilde{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top, \end{aligned}$$

thus satisfying Eq (2.8) with tombstones $\tilde{\mathtt{A}} \cup \mathtt{A}_\top$. Similarly, Eq (3.3) implies

$$\forall \hat{\mathtt{A}} \supseteq \mathtt{A}_I \cup \mathtt{A}'_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top), \quad \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top = \mathtt{f}(\hat{\mathtt{A}} \ \cup\ \tilde{\mathtt{A}} \ \cup\ \mathtt{A}'_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top, \tag{3.5}$$

so $(\emptyset, \mathtt{A}_I \cup \mathtt{A}'_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top), \tilde{\mathtt{A}} \cup \mathtt{A}'_\top)$ satisfy GC Invariant 2.1 Eq 2.4. Applying Eq 2.5, we get

$$\begin{aligned} \forall \hat{\mathtt{A}} \ &\supseteq\ \mathtt{A}_\exists \cup (\mathtt{A}_I \cup \mathtt{A}'_\exists - (\tilde{\mathtt{A}} \cup \mathtt{A}'_\top)) - (\mathtt{A}_\top \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top) \ =\ \mathtt{A}_\exists \cup \mathtt{A}'_\exists - (\mathtt{A}_\top \cup \tilde{\mathtt{A}} \cup \mathtt{A}'_\top), \\ \mathtt{f}(\hat{\mathtt{A}}) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top \ &=\ \mathtt{f}(\hat{\mathtt{A}} \ \cup\ \mathtt{A}_\top \ \cup\ \tilde{\mathtt{A}} \ \cup\ \mathtt{A}'_\top) \cup \mathtt{B}_\exists \cup \mathtt{B}_\top \end{aligned}$$

thus satisfying Eq (2.9) with tombstones $\tilde{\mathtt{A}} \cup \mathtt{A}_\top$. We have therefore shown that $\mathtt{GCImax}(\mathtt{A}_I,\ \mathtt{f},\ \mathtt{B}_I) = \tilde{\mathtt{A}} \subseteq \tilde{\mathtt{A}} \cup \mathtt{A}_\top \subseteq \mathtt{GCmax}(\mathtt{A}_{\mathtt{TS}},\ \mathtt{f},\ \mathtt{B}_{\mathtt{TS}})$ due to the maximality of GCmax.

Example 3.4 (Instantiated Tuple-based GC) $\mathit{GCItuple}(A_I,\ f,\ B_I) = \{t \in A_I \ :\ \forall X, f(X \cup \{t\}) - f(X) \subseteq B_I\}$

4 Putting it together

References

[1] N. Conway, P. Alvaro, E. Andrews, and J. M. Hellerstein. Edelweiss: Automatic storage reclamation for distributed programming. *Proceedings of the VLDB Endowment*, 7(6):481–492, 2014.