

Incremental Fixpoint Computation: A Two-Level Architecture

Contents

1 Motivation: DCE as Incremental Fixpoint	2
2 The General Pattern	2
3 Level 1: Low-Level Incremental Fixpoint API	3
3.1 API Specification	3
3.1.1 Types	3
3.1.2 Configuration (User Provides)	3
3.1.3 State (System Maintains)	3
3.1.4 Required Properties	3
3.2 Algorithms	4
3.2.1 Expansion (BFS)	4
3.2.2 Contraction (Worklist Cascade)	4
3.2.3 Why Ranks Break Cycles	5
3.3 Correctness and Analysis	5
3.3.1 Proven Properties (Lean, all complete)	5
3.3.2 Complexity Analysis	5
3.3.3 Gap Between Proofs and Algorithms	5
3.4 Formal Definitions (Reference)	5
4 Worked Example: DCE in Detail	6
4.1 Setup	6
4.2 Example: Expansion (Adding an Edge)	6
4.3 Example: Contraction (Removing an Edge)	7
4.4 Example: Contraction with Cycles	7
4.5 Summary	8
5 Level 2: DSL with Automatic Derivation (Future)	8
5.1 Analogy: Automatic Differentiation	8
5.2 Potential DSL Primitives	8
5.3 Connection to Datalog	9
6 Examples Beyond DCE	9
7 Relationship to Reactive Systems	10
8 Future Work	10

Abstract

We observe that the incremental dead code elimination (DCE) algorithm from our reactive DCE work is an instance of a more general pattern: *incremental fixpoint computation*. This note proposes a two-level architecture for incremental fixpoints: (1) a low-level API that assumes user-provided incremental operations, and (2) a potential high-level DSL where these operations are derived automatically from a structured definition of the fixpoint operator. The relationship between these levels is analogous to that between manual gradient computation and automatic differentiation.

1 Motivation: DCE as Incremental Fixpoint

In reactive DCE, the live set is defined as the least fixpoint of a monotone operator:

$$F_G(S) = G.\text{roots} \cup \{v \mid \exists u \in S. (u, v) \in G.\text{edges}\}$$

That is, $\text{liveSet}(G) = \text{lfp}(F_G)$.

When the graph changes ($G \rightarrow G' = G \pm f$), we want to update the fixpoint incrementally rather than recomputing from scratch. The key observations are:

- **Expansion** ($G \rightarrow G \oplus f$): The operator grows, so $\text{lfp}(F_G) \subseteq \text{lfp}(F_{G'})$. The old fixpoint is an underapproximation; we iterate upward.
- **Contraction** ($G \rightarrow G \ominus f$): The operator shrinks, so $\text{lfp}(F_{G'}) \subseteq \text{lfp}(F_G)$. The old fixpoint is an overapproximation; we must remove unjustified elements.

This pattern—incremental maintenance of a least fixpoint under changes to the underlying operator—arises in many domains beyond DCE.

2 The General Pattern

Definition 1 (Monotone Fixpoint Problem). *Given a complete lattice (L, \sqsubseteq) and a monotone operator $F : L \rightarrow L$, the least fixpoint is $\text{lfp}(F) = \bigcap\{x \mid F(x) \sqsubseteq x\}$.*

For set-based fixpoints (our focus), $L = \mathcal{P}(A)$ for some element type A , ordered by \subseteq , and F is typically of the form:

$$F(S) = \text{base} \cup \text{step}(S)$$

where **base** provides seed elements and **step** derives new elements from existing ones.

Definition 2 (Incremental Fixpoint Problem). *Given:*

- *A current fixpoint $S = \text{lfp}(F)$*
- *A change that transforms F into F'*

Compute $S' = \text{lfp}(F')$ efficiently, in time proportional to $|S' \Delta S|$ rather than $|S'|$.

3 Level 1: Low-Level Incremental Fixpoint API

3.1 API Specification

Remark 1 (Two API Levels). *The API has two levels depending on which operations are needed:*

- **Simple API** (*expansion only*): Supports adding elements to base or edges. Requires only `base` and `stepFwd`.
- **Full API** (*expansion + contraction*): Also supports removing elements. Additionally requires `stepInv` and `rank`.

Many applications only need expansion (e.g., monotonically growing graphs). The simple API suffices and is easier to implement.

3.1.1 Types

A	Element type (e.g., graph nodes)
$\text{Set}(A)$	Finite sets of elements
$\text{Map}(A, \mathbb{N})$	Map from elements to natural numbers (ranks)

3.1.2 Configuration (User Provides)

<code>base</code> : $\text{Set}(A)$	Seed elements (e.g., roots)	required
<code>stepFwd</code> : $A \rightarrow \text{Set}(A)$	Forward derivation	required
<code>stepInv</code> : $A \rightarrow \text{Set}(A)$	Inverse derivation	for contraction

Define $\text{step}(S) = \bigcup_{x \in S} \text{stepFwd}(x)$ and $F(S) = \text{base} \cup \text{step}(S)$.

Note: If `stepInv` is not provided, the system can build it from `stepFwd`:

$$\text{stepInv}[y] = \{x \in \text{current} \mid y \in \text{stepFwd}(x)\}$$

This is computed once during initialization and maintained incrementally.

3.1.3 State (System Maintains)

<code>current</code> : $\text{Set}(A)$	Current live set = $\text{lfp}(F)$	always
<code>rank</code> : $\text{Map}(A, \mathbb{N})$	BFS distance from base	for contraction

3.1.4 Required Properties

1. **stepInv correctness** (if provided): $y \in \text{stepInv}(x) \Leftrightarrow x \in \text{stepFwd}(y)$
2. **Element-wise** (automatic): step decomposes via `stepFwd`
3. **Additive** (automatic): $\text{step}(A \cup B) = \text{step}(A) \cup \text{step}(B)$

Example 1 (DCE Instance).

$$\begin{aligned} \text{base} &= \text{roots} \\ \text{stepFwd}(u) &= \{v \mid (u, v) \in \text{edges}\} \quad (\text{successors}) \\ \text{stepInv}(v) &= \{u \mid (u, v) \in \text{edges}\} \quad (\text{predecessors, optional}) \end{aligned}$$

3.2 Algorithms

3.2.1 Expansion (BFS)

When the operator grows ($F \sqsubseteq F'$: base or edges added), propagate new elements:

```
expand(state, config'):
    frontier = config'.base \ state.current
    r = 0
    while frontier != {}:
        for x in frontier:
            state.current.add(x)
            state.rank[x] = r
        nextFrontier = {}
        for x in frontier:
            for y in config'.stepFwd(x):
                if y not in state.current:
                    nextFrontier.add(y)
        frontier = nextFrontier
        r += 1
```

3.2.2 Contraction (Worklist Cascade)

When the operator shrinks ($F' \sqsubseteq F$: base or edges removed), remove unsupported elements:

```
contract(state, config'):
    // Initialize: nodes that lost base membership or an incoming edge
    worklist = { x | x lost support }
    dying = {}

    while worklist != {}:
        x = worklist.pop()
        if x in dying or x in config'.base: continue

        // Check for well-founded deriver (strictly lower rank)
        hasSupport = false
        for y in config'.stepInv(x):
            if y in (state.current \ dying) and state.rank[y] < state.rank[x]:
                hasSupport = true
                break

        if not hasSupport:
            dying.add(x)
            // Notify dependents
            for z where x in config'.stepInv(z):
                worklist.add(z)

    state.current == dying
```

3.2.3 Why Ranks Break Cycles

The rank check $\text{rank}[y] < \text{rank}[x]$ is essential:

- Cycle members have *equal* ranks (same BFS distance from base)
- Therefore, they cannot provide well-founded support to each other
- An unreachable cycle has no well-founded support and is correctly removed

3.3 Correctness and Analysis

3.3.1 Proven Properties (Lean, all complete)

Theorem 1 (Expansion Correctness). *If $F \sqsubseteq F'$ and expansion terminates, then $\text{current} = \text{lfp}(F')$.*

Theorem 2 (Contraction Correctness). *If $F' \sqsubseteq F$ and contraction terminates, then $\text{current} = \text{lfp}(F')$.*

Theorem 3 (Soundness). *At all intermediate states: expansion gives $\text{current} \subseteq \text{lfp}(F')$; contraction gives $\text{lfp}(F') \subseteq \text{current}$.*

All proofs complete in Lean with no `sorry`.¹

3.3.2 Complexity Analysis

Operation	Time	Space
Expansion	$O(\text{new} + \text{edges from new})$	$O(\text{new})$
Contraction	$O(\text{dying} + \text{edges to dying})$	$O(\text{dying})$
Rank storage	—	$O(\text{current})$ integers

For DCE, this matches the complexity of dedicated graph reachability algorithms.

3.3.3 Gap Between Proofs and Algorithms

Gap	Description	Status
Refinement	Pseudo-code implements the spec	Visually obvious
Termination stepInv	Algorithms halt on finite sets User provides correct inverse	Clear (monotonic) Assumed

These gaps are mechanical to close. A good engineer can implement with confidence.

3.4 Formal Definitions (Reference)

For completeness, the formal definitions used in Lean proofs.

Definition 3 (Decomposed Operator). $F(S) = B \cup \text{step}(S)$ where `step` is monotone.

Definition 4 (Rank). $\text{rank}(x) = \min\{n \mid x \in F^n(\emptyset)\}$.

Definition 5 (Well-Founded Derivation). y wf-derives x if $\text{rank}(y) < \text{rank}(x)$ and $x \in \text{step}(\{y\})$.

Definition 6 (Semi-Naive Iteration). $C_0 = I$, $\Delta_0 = I$, $\Delta_{n+1} = \text{step}(\Delta_n) \setminus C_n$, $C_{n+1} = C_n \cup \Delta_{n+1}$.

Definition 7 (Well-Founded Cascade). $K_0 = I$, $K_{n+1} = K_n \setminus \{x \mid x \notin B \wedge \text{no wf-deriver in } K_n\}$.

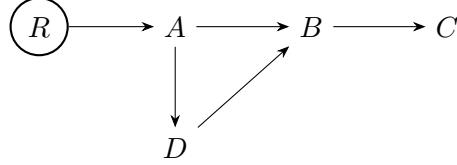
¹See `lean-formalisation/IncrementalFixpoint.lean`.

4 Worked Example: DCE in Detail

We illustrate the API and algorithms with Dead Code Elimination (DCE), showing how expansion and contraction work on concrete graphs.

4.1 Setup

Consider a program represented as a directed graph where nodes are code units and edges represent dependencies (“ $u \rightarrow v$ ” means u uses v).



- $\text{base} = \{R\}$ (R is the root/entry point)
- $\text{stepFwd}(R) = \{A\}$, $\text{stepFwd}(A) = \{B, D\}$, $\text{stepFwd}(B) = \{C\}$, $\text{stepFwd}(D) = \{B\}$

Initial state after BFS expansion:

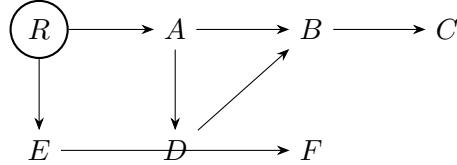
$$\begin{aligned}\text{current} &= \{R, A, B, C, D\} \\ \text{rank} &= \{R \mapsto 0, A \mapsto 1, B \mapsto 2, C \mapsto 3, D \mapsto 2\}\end{aligned}$$

Note: B and D have the same rank (both at distance 2 from R).

For contraction we also write $\text{steplnv}(x)$ for the set of predecessors y with an edge $y \rightarrow x$, and maintain a set dying of nodes scheduled for removal.

4.2 Example: Expansion (Adding an Edge)

Suppose we add an edge $R \rightarrow E$ where E is a new node with $\text{stepFwd}(E) = \{F\}$.



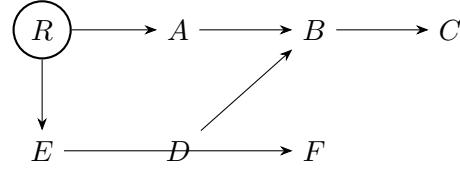
Expansion algorithm:

1. $\text{frontier} = \{E\}$ (new successors of R), $r = 1$
2. Add E with $\text{rank}[E] = 1$
3. $\text{frontier} = \{F\}$, $r = 2$
4. Add F with $\text{rank}[F] = 2$
5. $\text{frontier} = \{\}$, done

Result: current = {R, A, B, C, D, E, F}

4.3 Example: Contraction (Removing an Edge)

Now suppose we remove the edge $A \rightarrow D$.



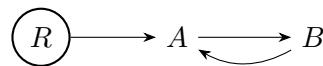
Contraction algorithm:

1. worklist = {D} (lost its incoming edge from A)
2. Process D:
 - $D \notin \text{base}$
 - Check for wf-deriver: $\text{stepInv}(D) = \{A\}$, but edge $A \rightarrow D$ removed
 - No wf-deriver found, so dying = {D}
 - All dependents of D already have another wf-deriver, so no additional nodes are added to the worklist
3. worklist = {}, done

Result: current = {R, A, B, C, E, F} (D removed)

4.4 Example: Contraction with Cycles

This example shows why *ranks* are essential. Consider:



- rank = {R $\mapsto 0$, A $\mapsto 1$, B $\mapsto 2$ }
- A has a wf-deriver: R with $\text{rank}[R] = 0 < 1$
- B has a wf-deriver: A with $\text{rank}[A] = 1 < 2$

Now remove edge $R \rightarrow A$:



Contraction:

1. $\text{worklist} = \{A\}$ (lost edge from R)
2. Process A :
 - $\text{stepInv}(A) = \{R, B\}$
 - $R \rightarrow A$ removed, so R doesn't count
 - B is in current, but $\text{rank}[B] = 2 > 1 = \text{rank}[A]$ — **not a wf-deriver!**
 - No wf-deriver, so A dies. Add B to worklist.
3. Process B :
 - $\text{stepInv}(B) = \{A\}$
 - A is dying, so doesn't count
 - No wf-deriver, so B dies.
4. $\text{worklist} = \{\}$, done

Result: $\text{current} = \{R\}$ (entire cycle removed)

Key insight: Without rank checking, A and B would keep each other alive (each derives the other). The rank check $\text{rank}[y] < \text{rank}[x]$ breaks this mutual support because cycle members have equal or increasing ranks along cycle edges.

4.5 Summary

Operation	Algorithm	Key Property
Add edge/root	BFS expansion	Assigns increasing ranks
Remove edge/root	Worklist cascade	Rank check breaks cycles

5 Level 2: DSL with Automatic Derivation (Future)

The low-level API requires the user to provide `stepFromDelta` and prove that `step` is element-wise and additive. A higher-level approach would let users define F in a structured DSL, from which these properties are derived automatically.

5.1 Analogy: Automatic Differentiation

	Differentiation	Incremental Fixpoint
Low-level	User provides $f(x)$ and $\frac{df}{dx}$	User provides F , <code>stepFromDelta</code> , proofs
High-level (DSL)	User writes expression; system derives gradient	User writes F in DSL; system derives incremental ops
Requirement	f given as expression tree	F given as composition of primitives
Black-box	Finite differences (slow)	Full recomputation (slow)

Just as automatic differentiation requires f to be expressed as a composition of differentiable primitives, automatic incrementalization requires F to be expressed as a composition of “incrementalizable” primitives.

5.2 Potential DSL Primitives

A DSL for fixpoint operators might include:

- $\text{const}(B)$: constant base set
- $\text{union}(F_1, F_2)$: union of two operators
- $\text{join}(R, S, \pi)$: join S with relation R , project via π
- $\text{filter}(P, S)$: filter S by predicate P
- $\text{lfp}(\lambda S.F(S))$: least fixpoint

Each primitive would come with:

- Its incremental step function (for semi-naive)
- Its derivation counting semantics (for deletion)

Example 2 (DCE in DSL). `live = lfp(S =>`

```
union(
    const(roots),
    join(edges, S, (u, v) => v)
)
)
```

The system derives:

- $\text{stepFromDelta}(\Delta) = \text{join}(\text{edges}, \Delta, (u, v) \mapsto v)$
- *Proof that step is element-wise (each edge provides a single derivation)*
- *Proof that step is additive (union distributes over step)*

5.3 Connection to Datalog

Datalog engines already perform similar derivations:

- Rules are the structured representation of F
- Semi-naive evaluation is derived from rule structure
- Well-founded cascade generalizes deletion handling

A general incremental fixpoint DSL would extend this beyond Horn clauses to richer operators (aggregation, negation, etc.).

6 Examples Beyond DCE

The incremental fixpoint pattern applies to many problems:

Problem	Base	Step	Derivation Count
DCE/Reachability	roots	successors	in-degree from live
Type Inference	base types	constraint propagation	# constraints implying type
Points-to Analysis	direct assignments	transitive flow	# flow paths
Call Graph	entry points	callees of reachable	# callers
Datalog	base facts	rule application	# rule firings

7 Relationship to Reactive Systems

In a reactive system like Skip:

- **Layer 1** (reactive aggregation) handles changes to the *parameters* of F (e.g., the graph structure).
- **Layer 2** (incremental fixpoint) maintains the fixpoint as those parameters change.

The two layers compose: reactive propagation delivers deltas to the fixpoint maintainer, which incrementally updates its state and emits its own deltas (added/removed elements) for downstream consumers.

8 Future Work

1. **Design Level 2 DSL:** Define a language of composable fixpoint operators with automatic incrementalization.
2. **Integrate with Skip:** Implement the incremental fixpoint abstraction as a reusable component in the Skip reactive framework.
3. **Explore stratification:** Extend to stratified fixpoints (with negation) where layers must be processed in order.
4. **Benchmark:** Compare incremental vs. recompute performance on realistic workloads.

9 Conclusion

The incremental DCE algorithm is an instance of a general pattern: maintaining least fixpoints incrementally under changes to the underlying operator. We propose a two-level architecture:

1. A **low-level API** where users provide `stepFromDelta` and prove step is element-wise and additive.
2. A **high-level DSL** (future work) where these proofs are derived automatically from a structured definition of F , analogous to how automatic differentiation derives gradients from expression structure.

The key contribution is *well-founded cascade*: using the iterative construction rank to handle cycles correctly. Elements not in the new fixpoint have no finite rank, so they have no well-founded drivers and are removed.

This abstraction unifies incremental algorithms across domains (program analysis, databases, reactive systems) and provides a foundation for building efficient, correct incremental computations.