Formally Verified Semilattice Class for Conflict-free Replicated Data Types (CRDTs)

Madhav Ram

April 2026

1 Introduction

This project implements, formalizes, and verifies the foundational algebraic properties of a Semilattice type class to ensure the mathematical correctness of State-based CRDTs (Conflict-free Replicated Data Types). CRDTs are important data structures that are used by distributed systems that power the Internet.

Using this generalized type class, I will implement and formally prove the safety and eventual consistency of concrete data structures, including Grow-Only Counter (G - Counter), Vector Clock, Positive-Negative (PN) Counter, and Last-Writer-Wins (LWW) Register.

2 Core Properties

The theorem will verify that any valid CRDT update function f is strictly inflationary ($x \leq f(x)$) with respect to the partial order induced by the semilattice. This relies on first proving that the semilattice's join operator ($\sqcup$) is commutative, associative, and idempotent and subsequently proving that its induced relation ($\leq$) forms a valid partially ordered set (reflexive, antisymmetric, and transitive).

3 Challenges

The primary difficulty will lie in generalizing the proofs for the $\sqcup$ and $\leq$ operators to accommodate the differences and complexity of common CRDTs. While proving these properties for simple types like natural numbers is straightforward, handling composite states—such as tuples for PN-Counters or branching conditional logic for LWW-Registers.

4 References

1. https://jhellerstein.github.io/blog/crdt-turtles/
2. https://avichalp.me/posts/2023-05-07-crdts-in-a-nutshell/
3. https://en.wikipedia.org/wiki/Semilattice
4. Conflict-free replicated data types; Shapiro et al. SSS'11