Strong Normalization for the Safe Fragment of a Minimal Rewrite System:
A Triple-Lexicographic Proof and a Conjecture on the Unprovability of Full Termination for Any Relational Operator-Only TRS

Moses Rahnama
Mina Analytics

November 24, 2025

Abstract

We present a minimal operator-only term rewriting system with seven constructors and eight reduction rules. Our main contribution is a mechanically-verified proof of strong normalization for a guarded fragment using a novel triple-lexicographic measure combining a phase bit, multiset ordering (Dershowitz-Manna), and ordinal ranking. From strong normalization, we derive a certified normalizer with proven totality and soundness. Assuming local confluence (verified through critical pair analysis), Newman's Lemma yields confluence and therefore unique normal forms *for the safe fragment.* We establish impossibility results showing that simpler measures, such as additive counters, polynomial interpretations, and single-bit flags, provably fail for rules with term duplication. The work demonstrates fundamental limitations in termination proving for self-referential systems. We state a conjecture: no *relational* operator-only TRS can have its full-system termination proved by internally definable methods. Here "relational" is equivalent to "capable of ordered computation": systems with a recursor enabling iteration over successors, comparison, or sequential counting. Such recursors necessarily redistribute step arguments across recursive calls, defeating all additive termination measures. This structural limitation applies to any TRS expressive enough to encode ordered data. All theorems have been formally verified in a proof assistant. The Lean formalization is available at `https://github.com/MosesRahnama/OperatorKO7`.

1 Introduction

This paper presents a minimal *operator-only* rewrite calculus (**KO7**) where the object language contains only constructors and operators with rewrite rules. There are no binders, types, external axioms, or semantic predicates; the rules *are* the semantics. The primary goals are: (i) a clean, duplication-robust proof of *strong normalization* (SN); (ii) a *certified normalizer* that always returns a normal form; (iii) *unique* normal forms via Newman's Lemma under a local-confluence assumption; and (iv) a conjecture regarding the unprovability of termination for relational operator-only systems using internal methods.

Scope. The formal results apply to a *guarded safe subrelation.* This restriction is necessary because the full relation is not locally confluent at the root peak eqW $a\,a$ when $\kappa^M(a) = 0$. The safe fragment employs guarded/context joiners to ensure unique normal forms (§6).

A second conceptual goal is to situate KO7 against results about *fixed-target* reachability in terminating TRSs. If an internal provability predicate is defined by "t reduces to $\top$", then under SN the set t — t =¿* top is decidable by normalization/backtracking. With confluence, decision reduces to normal-form equality. This explains why single-level Gödel encodings cannot coexist with globally terminating proof search; stratification is required.

Contributions. We prove strong normalization for a guarded fragment of KO7 using a novel triple-lexicographic measure that combines a phase bit, multiset ordering (Dershowitz-Manna), and ordinal ranking. This result supports a certified normalizer with proven totality and soundness. Furthermore, we establish confluence for the safe fragment via Newman's Lemma given verified local confluence. The work also includes formally verified impossibility results for additive and polynomial measures under duplication, demonstrating fundamental limitations in termination proving for self-referential systems.

Highlights (formalization summary).

- **SN (SafeStep) via triple lex**: Formally proven using a lexicographic measure combining a δ-phase bit, a Dershowitz-Manna multiset rank, and an ordinal.
- **Certified normalizer**: A total and sound normalization function is defined by well-founded recursion.
- **Newman (SafeStep)**: Confluence is established via Newman's Lemma using a verified local confluence property for the safe fragment.
- **Full Step caveat**: We exhibit a specific peak ($\mathrm{eqW}\,a\,a$ with $\kappa^M(a) = 0$) where local join fails, justifying the restriction to the safe subrelation.
- **Impossibility results**: The failure of simpler additive and polynomial measures is formally witnessed by counterexamples.

2 Background: TRSs, SN, reachability, and Newman

Standard abstract reduction and term rewriting notions apply [2, 11]. A term is in *normal form* if no rule applies. A TRS is *strongly normalizing* (SN) if there are no infinite reductions. A relation is *confluent* if for any $t \Rightarrow^* u$ and $t \Rightarrow^* v$ there exists w with $u \Rightarrow^* w$ and $v \Rightarrow^* w$. *Local confluence* requires this only for single-step forks. *Newman's Lemma* asserts SN + local confluence ⇒ confluence [10], yielding unique normal forms.

Fixed-target ("small-term") reachability in terminating TRSs has well-charted complexity: NP-complete for length-reducing systems (dropping to P under confluence), NExpTime/N2ExpTime for (linear) polynomial interpretations, and PSPACE for KBO-terminating TRSs [1]. Modularity holds in certain linear, non-collapsing combinations [4], while even *flat* non-linear systems exhibit undecidable reachability and confluence [9]. Termination under duplication typically requires orders beyond plain sizes; a naive size can increase under duplicating rules. The cure is a *multiset* extension of a base order [6] or (recursive) path orders [5].

3 The KO7 calculus

KO7 is a finite TRS over a small signature (7 constructors) with 8 rules (including the equality-witness operator `eqW`). For concreteness we list the kernel rule shapes below.

Kernel signature (7 constructors). Terms are generated by the constructors:

$$t ::= \mathrm{void} \mid \delta\, t \mid \mathrm{integrate}\, t \mid \mathrm{merge}\, t\, t \mid \mathrm{app}\, t\, t \mid \mathrm{rec}\Delta\, t\, t\, t \mid \mathrm{eqW}\, t\, t.$$

The full kernel relation `Step` is generated by the 8 rules in Table 1, while the certified artifact is proved for a guarded subrelation `SafeStep`.

Rule	Head	Arity	Shape	Dup?
`R_merge_void_left`	merge	2	merge void $t \to t$	No
`R_merge_void_right`	merge	2	merge t void $\to t$	No
`R_merge_cancel`	merge	2	merge $t\ t \to t$	No
`R_rec_zero`	recΔ	3	rec $\Delta\, b\, s$ void $\to b$	No
`R_rec_succ`	recΔ	3	rec $\Delta\, b\, s\,(\text{delta}\, n) \to \text{app}\, s\,(\text{rec}\,\Delta\, b\, s\, n)$	No*
`R_int_delta`	integrate	1	integrate $(\text{delta}\, t) \to$ void	No
`R_eq_refl`	eqW	2	eqW $a\ a \to$ void	No
`R_eq_diff`	eqW	2	eqW $a\ b \to$ integrate $(\text{merge}\, a\, b)$	No

Table 1: KO7's 8 kernel rules. In the full kernel relation, `R_eq_refl` and `R_eq_diff` overlap at `eqW a a`. The certified safe fragment guards `R_eq_diff` by $a \neq b$. `R_merge_cancel` is collapsing. *`R_rec_succ` redistributes s to two RHS positions.

Tiny example (trace consequences). Using the verified normalizer, we observe:

- Integrate/delta: integrate$(\delta\, t) \Rightarrow^*$ void (verified).
- Equality (meta-level consequence under confluence):
  - If $\text{nf}(a) = \text{nf}(b)$ then eqW $a\, b \Rightarrow^*$ void.
  - Otherwise eqW $a\, b \Rightarrow^*$ integrate(merge $a\, b$).

  Note: In the safe fragment, confluence ensures these outcomes are unique.

Note. We prove SN and Newman-based confluence for the *safe fragment*.

4 Strong normalization

The termination argument relies on a *triple-lexicographic* measure

$$\mu^3(t) := (\delta\text{-flag}(t),\ \kappa^M(t),\ \mu_{\text{ord}}(t))$$

ordered by the lex product of: (i) a phase bit dropping on the successor recursion; (ii) a *multiset* of ranks κ^M (Dershowitz-Manna) with an explicit precedence/status orienting redex > pieces; and (iii) an ordinal payload μ_{ord} for non-duplicating ties. Ordinal hazards are formally handled (right-addition is not strictly monotone; absorption $\alpha + \beta = \beta$ requires $\omega \leq \beta$). Duplicating branches use a compact MPO-style head precedence.

Step vs SafeStep (measure unification). For the *SafeStep* relation, a single unified triple lex order $(\delta, \kappa^M, \mu_{\text{ord}})$ suffices. Steps in the *full* relation are covered by a disjunctive decrease certificate: each step corresponds to either a KO7 lex drop or an MPO triple drop.

Theorem 1 (Per-step decrease (SafeStep))**.** *For every rule instance $t \Rightarrow t'$ in the guarded* `SafeStep` *relation, we have $\mu^3(t') <_{\text{Lex}} \mu^3(t)$.*

Proof idea. By rule head. For collapsing rules (e.g., merge-cancel) we use the multiset component with the chosen precedence so that *every RHS piece is strictly smaller than the removed LHS redex* in the base order. For rec-succ the δ bit drops (1→0). In the formalization, each branch is a one-liner dispatched by a wrapper lemma.

DM vs MPO on rules (explicit). For **merge-cancel**, we use a DM multiset lift over a base order where merge $t\,t$ strictly dominates t. For **eqW**, we use a compact MPO-leaning measure where the head precedence orients eqW $a\,b$ strictly above integrate(merge $a\,b$).

- Base-order premise (merge-cancel): in merge $t\,t \to t$, the RHS is strictly smaller than the LHS.
- Base-order premise (eqW): in eqW $a\,b \to$ integrate(merge $a\,b$), the RHS is strictly smaller under head precedence.

No-Go for constant bumps on κ (generic duplicator).

Lemma 1 (No fixed $+k$ or boolean flag orients a generic duplicator)**.** *Let κ be a max-depth-style counter and fix any $k \in \mathbb{N}$. For a duplicating rule of the shape $r(S) \to C[S, S]$ (one redex replaced by two occurrences of a subterm S), there exists an instance where $\kappa(LHS)+k = \kappa(RHS)+k$, so no strict lex drop occurs. The same holds for a boolean phase flag alone.*

Proof sketch. Choose S with $\kappa(S) \geq 1$ and let base bound the context. Then $\kappa(\text{LHS}) =$ base+1 while $\kappa(\text{RHS}) = \max(\kappa(C[S]), \kappa(C[S])) =$ base+1. Adding a fixed k preserves equality; a single flag does not alter the tie. □

Remark 1. In `R_rec_succ` (rec-succ), the step argument s appears once on the LHS and twice on the RHS: once as the argument to `app` and once inside the recursive call. This structural redistribution defeats additive measures when s contains redexes. Orientation relies on the δ phase bit (1→0), which drops because the `delta` wrapper is consumed.

Duplication stress identity. For any additive counter ρ that counts a single removed redex and sums subpieces, generic duplicators satisfy

$$\rho(\text{after}) = \rho(\text{before}) - 1 + \rho(S),$$

so there is no strict drop when $\rho(S) \geq 1$. The robust fix uses DM/MPO: replace one element by a multiset of strictly smaller elements (DM), or use RPO/MPO with a precedence/status such that the LHS redex strictly dominates each RHS piece.

Corollary 1 (Strong normalization)**.** *The guarded relation `SafeStep` for KO7 is strongly normalizing.*

Genealogy of failures (why DM/MPO). We record minimal counterpatterns that motivate the multiset/path components:

- Pure ordinal (μ) only: shape-blind bounds fail to separate nested δ from its context.
- Additive bumps on κ: ties persist on duplicators (Lemma 1).
- Additive counters ρ: by the identity $\rho(\text{after}) = \rho(\text{before}) - 1 + \rho(S)$ there is no strict drop when $\rho(S) \geq 1$.
- Polynomial interpretations that rely on imported arithmetic or hard-coded constants: the duplicating rules force case splits that cannot be oriented without stepping outside the operator language, so these methods fail within the allowed internal toolbox.

The fix is DM/MPO: ensure each RHS piece is strictly smaller than the removed redex in a base order and lift via a multiset/path extension.

5 A certified normalizer

A normalization function is defined by well-founded recursion on μ^3. Properties proven in the formalization include:

$$\textbf{(Totality)}\ \forall t\,\exists n.\ \mathrm{Normalize}(t) = n$$
$$\textbf{(Soundness)}\ \forall t.\ \mathrm{normal}(\mathrm{Normalize}(t))\ \wedge\ t \Rightarrow^{*}\ \mathrm{Normalize}(t).$$

No specific efficiency claim is made: worst-case normalization cost follows the termination witness (cf. the small-term reachability bounds in [1]). Under confluence, decision reduces to one normalization and an equality check.

6 Local confluence and Newman (guarded safe relation)

Local confluence is discharged by joining the finite set of critical pairs. Combining Cor. 1 with Newman's Lemma [10] yields:

Theorem 2 (Confluence and unique normal forms)**.** *If a relation is strongly normalizing and locally confluent, then it is confluent. Hence every term reduces to a unique normal form.*

Instantiation (SafeStep). Combining Cor. 1 (SN for `SafeStep`) with local-join lemmas yields confluence and unique normal forms for the *safe* fragment by Newman's Lemma. In contrast, the *full* relation is not locally confluent at the root peak $\mathrm{eqW}\,a\,a$ under $\kappa^M(a) = 0$; thus full confluence does not hold. The `SafeStep` relation restricts `eqW` to cases where arguments are guarded, preventing this divergence.

The star-star join proof follows the standard accessibility (Acc) recursion at the source, with a case split over star shapes ("head step + tail") and composition via transitivity. The module also provides corollaries for uniqueness of normal forms and equality of normalizers under star.

Scope and Guarantees (formalization-accurate). We work with a guarded safe subrelation `SafeStep` for which we prove:

- **SN (SafeStep).** The KO7 triple measure μ^3 strictly drops on every `SafeStep`. This yields a *certified normalizer* that is total and sound for the safe fragment.
- **Local Confluence (SafeStep).** We provide local-join lemmas per root shape and context wrappers. Newman then yields confluence and unique NFs for the safe fragment.
- **Full Step per-rule decreases (Hybrid).** For each kernel rule, there is a per-step decrease witnessed either by KO7's $\delta/\kappa^M/\mu$ lex or by an MPO-leaning μ-first triple. A uniform global aggregator for *all* of `Step` is left as future work.

Critical-pair coverage. The following table covers the *safe* root configurations with explicit local-join lemmas. This is exhaustive for `SafeStep` *except* the reflexive $\mathrm{eqW}\,a\,a$ peak under $\kappa^M(a) = 0$, which we show is *not* locally joinable at the root. We discharge many `eqW` cases via guarded/context wrappers.

Source	Lemma
integrate$(\delta\, t)$	`localJoin_int_delta` (unique target `void`)
merge void t	`localJoin_merge_void_left` (unique target t)
merge t void	`localJoin_merge_void_right` (unique target t)
merge $t\ t$	`localJoin_merge_tt` (unique target t)
rec $\Delta\, b\, s$ void	`localJoin_rec_zero` (unique target b)
rec $\Delta\, b\, s\, (\delta\, n)$	`localJoin_rec_succ` (unique target app s (rec $\Delta\, b\, s\, n$))
eqW $a\, b$, $a \neq b$	`localJoin_eqW_ne` (unique target integrate(merge $a\, b$))
eqW $a\, a$, $\kappa^M(a) = 0$	*not locally joinable at root*

Guarded variants exclude spurious branches. Contextual wrappers lift root joins to context.

δ-guard: definition and decidability. Define the safe-phase predicate by δ-guard$(t) \iff$ deltaFlag$(t) = 0$. Here deltaFlag : Term $\to \mathbb{N}$ is a structurally recursive function defined on terms in the artifact (tracking split parity), so the predicate is *decidable*. Facts: deltaFlag(eqW $a\, b$) $= 0$; merge-void rules require deltaFlag$(t) = 0$.

Tiny δ-flag walk-through (1→0).

$$\mathrm{rec\_}\Delta\, b\, s\, (\delta\, n) \xrightarrow{\delta\text{-flag drop}} \mathrm{app}\ s\ (\mathrm{rec\_}\Delta\, b\, s\, n)$$

7 Impossibility results

The formal development establishes the failure of several simpler measure strategies, necessitating the use of DM multiset orders or MPO:

- **Additive bumps fail**: No measure of the form $\kappa(t) + k$ strictly decreases on generic duplicating rules.
- **Bare flags fail**: A single boolean flag is insufficient to orient rules that lift depth.
- **Polynomial interpretations fail**: Any polynomial interpretation involving fixed constants requires external arithmetic axioms to "orient" the rule, violating the operator-only constraint.

Polynomial Impossibility. Consider polynomial interpretations of the form $M(t) \in \mathbb{N}$ for a duplicating rule $f(x) \to g(x, x)$. A polynomial measure assigning $M(f(x)) = M(x) + p$ requires $M(x) + p > 2M(x)$ for strict decrease, implying $p > M(x)$. This fails for unbounded $M(x)$.

More generally: any polynomial proof for a system with duplicating rules must hardcode specific constants (e.g., $M(\text{void}) = 2$) to satisfy inequalities like $2M(s) > M(s) + 1$. Such proofs import external arithmetic properties and impose arbitrary values on operators, violating the principle that operators' semantics should be defined solely by rewrite rules. Changing the hardcoded constant (e.g., $M(\text{void}) = 1$) collapses the proof. This structural failure is why polynomial interpretations cannot orient generic duplicating rules without external axioms.

Internally definable measures. We use a simple contract for internally defined termination measures to structure these negative results:

Definition 1 (Internally definable measure)**.** *An internally definable measure for a type α consists of (β, $<\_\beta$, wf, m, ctxMono, piecesLt) where: β is a base order carrier; $<\_\beta$ is a well-founded relation with witness wf; $m : \alpha \to \beta$ is the measure; ctxMono expresses context compatibility; and piecesLt asserts that in each rule instance, every RHS piece is strictly smaller than the removed LHS redex w.r.t. $<\_\beta$.*

8 Decidability of Reachability

Theorem 3 (Fixed-target reachability)**.** *In a strongly normalizing TRS, the set* $\{t \mid t \Rightarrow^* c\}$ *for any constant* c *is decidable via normalization.*

This connects the work to classical results: encoding undecidable properties through reduction to constants violates known theoretical limits. This motivates stratified approaches in proof assistants where object-level and meta-level reasoning are kept separate.

Assumptions (model). The model assumes a finite first-order TRS over finite terms. The decision procedure computes a normal form (by SN) and checks whether it is $\top$; with local confluence, this reduces to one normalization and an equality test.

Complexity context. Small-term reachability in terminating TRSs ranges from NP (length-reducing) to NExpTime/N2ExpTime (polynomial interpretations) and PSPACE (KBO), with confluence lowering the length-reducing class to P [1]. This situates our "normalize and compare" decision procedure for KO7 within the established landscape.

Moreover, decidability can be *modular* for disjoint unions under left-linearity/non-collapsing assumptions [4], while termination alone does not guarantee decidability: even *flat* non-linear TRSs have undecidable reachability/joinability/confluence [9].

9 Conjecture: Full Termination of Any Relational Operator-Only TRS

What "relational" means. A *relational* operator-only TRS is, by definition, one capable of *ordered computation*. The terms are equivalent: "relational" = "capable of ordered computation." Such systems can express iteration over successors, comparison of structure depths, or any form of sequential counting. The minimal signature for such capability includes a recursor, an operator that applies a step function iteratively across a successor-structured argument. Examples include primitive recursion over natural numbers, fold over lists, and any construct that steps through an ordered index. A TRS that cannot express such iteration (e.g., a flat pattern-matching system with no recursive structure) is not relational in this sense.

The critical property of relational systems is that their recursor *redistributes* its step argument across recursive calls. This redistribution is not optional: it is what makes ordered computation possible. But it also defeats all additive termination measures.

The structural barrier. Any operator system capable of ordered computation requires a recursor. A recursor redistributes its step argument across recursive calls. This redistribution defeats additive termination measures: $M(\text{after}) = M(\text{before}) - 1 + M(s)$, yielding no strict drop when $M(s) \geq 1$.

Definition 2 (Internally definable measure)**.** *An internally definable termination method for signature* Σ *uses only: simplification orders with fixed precedence/status on* Σ *(LPO/RPO/MPO), DM-multiset lifts of* $\mathbb{N}$*-valued ranks, and algebraic interpretations definable without importing external axioms. No encodings into external arithmetic, no borrowed logic, and no hard-coded constants outside the operator language.*

Conjecture 1 (Full Termination Conjecture for Relational TRSs)**.** *No relational operator-only TRS can have its full-system termination proved by internally definable methods. Specifically: let* R *be an operator-only TRS with a recursor rule of the form*

$$\mathrm{rec}(b, s, \sigma(n)) \to f(s, \mathrm{rec}(b, s, n)).$$

No internally definable measure (Definition 2) proves termination of R when the step argument s is unrestricted. The structural redistribution of s into both the function application and the recursive call defeats every additive, polynomial, or path-order measure that does not import external arithmetic or ordinal axioms. Any proof that relies on external axioms, imported arithmetic, or meta-level encodings is outside scope and does not count as an internal termination argument.

Scope of the conjecture. The conjecture applies to any TRS expressive enough to encode ordered data (natural numbers, lists, trees with successor structure, or any type supporting iteration). Systems without such structure (purely ground, non-recursive, or lacking a step-iteration pattern) fall outside the conjecture's scope. The claim is that *once a system has enough structure for ordered computation, its full termination escapes internal proof methods.*

Evidence. In KO7, the `rec-succ` rule has the critical shape: the step argument s appears twice on the RHS, and when s contains nested redexes, every additive measure fails to decrease strictly. The redistribution identity $M(\text{after}) = M(\text{before}) - 1 + M(s)$ yields no strict drop when $M(s) \geq 1$. The guarded SafeStep fragment terminates because the δ-phase bit restricts allowable step arguments; without such restriction, the full system admits unbounded recursive depth. The gap between internally definable ranking functions and what would be required cannot be closed without external methods (axioms, encodings, or borrowed arithmetic).

10 Formalization structure

The formal verification is implemented in a proof assistant. The project structure separates the kernel definitions, meta-theory proofs, and impossibility results:

- **Termination proofs:** Establishes the per-rule decreases and strong normalization for the safe fragment using the triple-lexicographic measure.
- **Normalization:** Defines the normalization function and proves its totality and soundness.
- **Confluence:** Implements the Newman engine and the star-star join, relying on local join lemmas.
- **Impossibility results:** Contains the verified counterexamples for additive measures and the proofs that simple measures fail under duplication.

All claimed results are formally proven without reliance on unproven postulates in the current build. The formal development is available at `https://github.com/MosesRahnama/OperatorKO7`.

Acknowledgments

AI has been a great help with this project.

References

[1] Franz Baader and Jürgen Giesl. Term rewriting (survey), 2024. Complexity of reachability results summary.

[2] Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[3] Wilfried Buchholz. A new system of proof-theoretic ordinal functions. *Annals of Pure and Applied Logic*, 32:195–207, 1986.

[4] Anne-Cécile Caron and Jean-Luc Coquidé. Decidability of reachability for term rewriting systems. In *Rewriting Techniques and Applications (RTA)*, pages 16–30. Springer, 1994.

[5] Nachum Dershowitz. Termination of rewriting. *Journal of Symbolic Computation*, 3(1–2):69–115, 1987.

[6] Nachum Dershowitz and Zohar Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, 1979.

[7] R. L. Goodstein. On the restricted ordinal theorem. *Journal of Symbolic Logic*, 9(2):33–41, 1944.

[8] L. Kirby and J. Paris. Accessible independence results for peano arithmetic. *Bulletin of the London Mathematical Society*, 14:285–293, 1982.

[9] Ichiro Mitsuhashi, Michio Oyamaguchi, and Yoshikatsu Ohta. On the undecidability of reachability for flat term rewriting systems. *IEICE Transactions on Information and Systems*, E89-D(2):1000–1007, 2006.

[10] M. H. A. Newman. On theories with a combinatorial definition of "equivalence". *Annals of Mathematics*, 43(2):223–243, 1942.

[11] TeReSe. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.

Appendix: Addendum

Lean kernel location

The authoritative mechanized kernel is the Lean file `OperatorKO7/Kernel.lean` in the repository `https://github.com/MosesRahnama/OperatorKO7`. The safe fragment and proofs are under `OperatorKO7/Meta/`.

Triple-lexicographic measure and duplication handling (DM/MPO)

We order $\mu^3(t) = (\delta\text{-flag}(t),\ \kappa^M(t),\ \mu_{\mathrm{ord}}(t))$ by lex:

- δ-flag: phase bit dropping on the successor recursion branch.
- Multiset κ^M: a Dershowitz-Manna multiset extension over a base precedence/status (or MPO head precedence) orienting redexes strictly above pieces; covers duplicators.
- Ordinal μ_{ord}: resolves non-duplicating ties; right-addition is not strictly monotone; absorption $\alpha + \beta = \beta$ needs $\omega \leq \beta$.

Per-rule lemmas show every RHS component is strictly smaller than the removed redex in the base order.

Aggregation for κ^M (union, not sum). We emphasize that κ^M aggregates via *multiset union* ($\cup$), not numeric addition. For duplicating rules, the multiset of piece-weights on the RHS is DM-smaller than the singleton multiset containing the LHS redex weight, yielding a strict drop in the κ^M component. For non-duplicating rules, κ^M ties by definitional equality and the ordinal μ_{ord} resolves the branch. In particular, for unguarded instances of `eqW`-refl and merge-cancel we use a κ-branch: when $\kappa^M(a) \neq 0$ we obtain a left-lex drop via DM; when $\kappa^M(a) = 0$ the κ^M component ties by `rfl` and the strict decrease is witnessed in the μ_{ord} coordinate (right branch of `Prod.Lex`).

Short witness snippets (toy duplication). Toy rule: $\mathrm{pair}(\mathrm{s}\,x,\ y) \to \mathrm{pair}(x,\ \mathrm{pair}(y,\ y))$.

DM multiset on sizes. Let $S(x,y) = \mathrm{size}(\mathrm{pair}(\mathrm{s}\,x,\ y)) = \mathrm{size}(x) + \mathrm{size}(y) + 2$. Then $\mathrm{size}(x) < S(x,y)$ and $\mathrm{size}(y) < S(x,y)$. Use $X = \varnothing$, $Y = \{\mathrm{size}(x), \mathrm{size}(y)\}$, $Z = \{S(x,y)\}$ to conclude $Y <_{\mathrm{DM}} Z$.

MPO triple weight. $\mathrm{weight}(\mathrm{pair}\,a\,b) = (\mathrm{headRank}(a),\ \mathrm{size}(a),\ \mathrm{size}(b))$ with $\mathrm{headRank}(\mathrm{s}\,\_) = 2$, else 1. If x is unit/pair then first components decrease (1¡2). If $x = \mathrm{s}\,t$ then tie on 2; the second components satisfy $\mathrm{size}(t) + 1 < \mathrm{size}(t) + 2$.

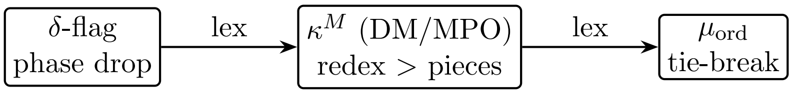

Figure 1: Triple-lex measure components. Duplicators decrease via κ^M; non-duplicating ties via μ_{ord}.

Newman scope (guarded safe relation)

SN + local confluence implies confluence; in the artifact this is instantiated for the *safe* relation via an Acc-based star-star join. Scope note: all confluence statements and their Newman instantiations are for *SafeStep* only. Full Step is *not* locally joinable at root for `eqW` a a with $\kappa^M(a) = 0$; accordingly we do not claim full-step confluence.

Module map

The verification logic is distributed across key modules for SN, normalizer, and confluence engine. Local confluence lemmas are proved separately. Note: context closure and local-join lemmas are explicitly instantiated for the *SafeStep* fragment (`SafeStepCtx`) rather than the full relation.

Per-rule orientation (DM/MPO/δ/μ)

Rule	Base component	Precedence/Status	Witness	Source
merge void left	μ (ordinal)	(n/a)	Theorem 4.1	Termination
merge void right	μ (ordinal)	(n/a)	Theorem 4.2	Termination
merge cancel	DM on κ^M (redex > pieces)	head precedence	Theorem 4.3	Termination
rec zero	DM on κ^M	rec > pieces	Theorem 4.4	Termination
rec succ	δ phase bit ($1 \to 0$)	(n/a)	Theorem 4.5	Termination
eqW refl	MPO (μ-first triple)	head precedence	Theorem 4.6	Termination
eqW diff	MPO (μ-first triple)	head precedence	Theorem 4.7	Termination
integrate (delta t)	μ (unique target)	(n/a)	Theorem 4.8	Termination
toy duplication	DM on size	s > pair	Lemma 7.1	Impossibility
toy duplication	MPO triple	headRank(s) > headRank(pair)	Lemma 7.2	Impossibility

Table 2: Per-rule orientation summary.

Parenthetical aliases: for substitution convenience we expose simp forms alongside the main rec lemmas.

Local-join report (critical peaks and unique-target cases)

Ctx-local join wrappers

When needed in context, the root local-join lemmas lift to context via wrappers:

Shape	Join lemma name	Notes
merge void void	`localJoin_merge_void_void`	both branches to void
merge t t	`localJoin_merge_tt`	joins at t (context-lifted)
integrate (delta t)	`localJoin_int_delta`	unique target void
recΔ b s void	`localJoin_rec_zero`	unique target b
recΔ b s (delta n)	`localJoin_rec_succ`	unique target app s (recΔ b s n)
eqW a b, a $\neq$ b	`localJoin_eqW_ne`	only diff applies (unique target)
eqW a a, guard kappaM a $\neq$ 0	`localJoin_eqW_refl_guard_ne`	refl blocked; only diff
merge a b (no void, a $\neq$ b)	`localJoin_merge_no_void_neq`	no root step; vacuous
integrate non-delta	`localJoin_integrate_non_delta`	no root step; vacuous
recΔ b s n (n $\neq$ void, not delta)	`localJoin_rec_other`	no root step; vacuous

Table 3: Local-join witnesses for the safe relation (root).

Shape	Ctx wrapper lemma	Notes
merge a b (no void, a $\neq$ b)	`localJoin_ctx_merge_no_void_neq`	from root 'merge' lemma
eqW a b, a $\neq$ b	`localJoin_ctx_eqW_ne`	only diff applies
eqW a a, kappaM guard	`localJoin_ctx_eqW_refl_guard_ne`	refl blocked
eqW a a if merge→delta	`localJoin_ctx_eqW_refl_if_merge_normalizes_to_delta`	via normalizeSafe
eqW a a if integrate→void	`localJoin_ctx_eqW_refl_if_integrate_merge_to_void`	via ctx star
eqW (delta n) (delta n)	`localJoin_ctx_eqW_refl_when_a_is_delta`	literal delta case

Table 4: Ctx-local join wrappers.

Appendix: Orientation Strategy

This summarizes the exact orientation strategy realized in the proofs (no global RPO required):

- Non-duplicating rules use a *μ-first* lex measure: triples $(\mu, \text{sizeMPO}, \delta)$ decrease directly via lemmas.
- The rule `rec_zero` uses a *DM multiset* drop on κ^M, wrapped by `drop_R_rec_zero`.
- The rule `rec_succ` drops the δ *phase bit* $(1 \to 0)$ via `drop_R_rec_succ`.
- Merge-cancel decreases via DM on κ^M under a base precedence where the redex strictly dominates its pieces.
- Conceptual precedence (if one prefers an MPO reading) aligns with rec > merge > app > integrate > eqW > delta > void, but the formal proofs do not require a global precedence declaration.

Formal anchors:

- Merge void left/right: μ-first or DM tie plus μ.
- Merge cancel: DM multiset drop on κ^M.
- Rec zero: `drop_R_rec_zero` with `dm_drop_R_rec_zero` for the inner DM piece.
- Rec succ: `drop_R_rec_succ` via the δ phase bit $(1 \to 0)$.
- EqW refl/diff: μ-first MPO triple.
- Integrate delta: unique target `void`.

A Related work

This work follows standard expositions in Baader-Nipkow and Terese [2, 11]. Termination under duplication relies on DM multiset orders [6] and (recursive) path orders [5]. Newman's Lemma is used in its classic ARS form [10]. For independence via termination, see Goodstein and Kirby-Paris and ordinal tools due to Buchholz [7, 8, 3]. For fixed-target reachability complexity and modularity results, see [1, 4]; for undecidability at shallow depth in non-linear systems, see [9].

B Conclusion

This paper presented an operator-only kernel and proved *strong normalization and confluence for the guarded safe subrelation*, yielding a certified normalizer and unique normal forms via Newman's Lemma. An explicit non-local-join witness at the eqW reflexive peak (under $\kappa^M = 0$) was established, blocking confluence for the *full* relation and motivating the SafeStep fragment. The decidability result explains the clash between single-level Gödel encodings and global termination. The impossibility of additive bumps under duplication was formally verified. Future directions include completing a stratified meta-layer, developing arithmetic encodings within KO7, and mapping the boundary between internally definable measures and external ordinal strength.