Optimised Maintenance of Datalog Materialisations

Pan Hu and Boris Motik and Ian Horrocks
Department of Computer Science, University of Oxford
Oxford, United Kingdom
firstname.lastname@cs.ox.ac.uk

Abstract
To efficiently answer queries, datalog systems often materialise all consequences of a datalog program, so the materialisation must be updated whenever the input facts change. Several solutions to the materialisation update problem have been proposed. The Delete/Rederive (DRed) and the Backward/Forward (B/F) algorithms solve this problem for general datalog, but both contain steps that evaluate rules ‘backwards’ by matching their heads to a fact and evaluating the partially instantiated rule bodies as queries. We show that this can be a considerable source of overhead even on very small updates. In contrast, the Counting algorithm does not evaluate the rules ‘backwards’, but it can handle only non-recursive rules. We present two hybrid approaches that combine DRed and B/F with Counting so as to reduce or even eliminate ‘backward’ rule evaluation while still handling arbitrary datalog programs. We show empirically that our hybrid algorithms are usually significantly faster than existing approaches, sometimes by orders of magnitude.

1 Introduction
Datalog (Abiteboul, Hull, and Vianu 1995) is a rule language that is widely used in modern information systems. Datalog rules can declaratively specify tasks in data analysis applications (Luteberget, Johansen, and Steffen 2016; Piro et al. 2016), allowing application developers to focus on the objective of the analysis—that is, on specifying what needs to be computed rather than how to compute it (Markl 2014). Datalog can also capture OWL 2 RL (Motik et al. 2009) ontologies possibly extended with SWRL rules (Horrocks et al. 2004). It is implemented in systems such as WebPIE (Urbani et al. 2012), VLog (Urbani, Jacobs, and Krötzsch 2016), Oracle’s RDF Store (Wu et al. 2008), OWLIM (Bishop et al. 2011), and RDFox (Nenov et al. 2015), and it is extensively used in practice.

When performance is critical, datalog systems usually precompute the materialisation (i.e., the set of all consequences of a program and the explicit facts) in a preprocessing step so that all queries can later be evaluated directly over the materialisation. Recomputing the materialisation from scratch whenever the explicit facts change can be expensive. Systems thus typically use an incremental maintenance algorithm, which aims to avoid repeating most of the work. Fact insertion can be effectively handled using the seminaïve algorithm (Abiteboul, Hull, and Vianu 1995), but deletion is much more involved since one has to check whether deleted facts have derivations that persist after the update. The Delete/Rederive (DRed) algorithm (Gupta, Mumick, and Subrahmanian 1993; Staudt and Jarke 1996), the Backward/Forward (B/F) algorithm (Motik et al. 2015), and the Counting algorithm (Gupta, Mumick, and Subrahmanian 1993) are well-known solutions to this problem.

The DRed algorithm handles deletion by first overdeleting all facts that depend on the removed explicit facts, and then rederiving the facts that still hold after overdeletion. The rederivation stage further involves rederiving all overdeleted facts that have alternative derivations, and then recomputing the consequences of the rederived facts until a fixpoint is reached. The algorithm and its variants have been extensively used in practice (Urbani et al. 2013; Ren and Pan 2011). In contrast to DRed, the B/F algorithm searches for alternative derivations immediately (rather than after overdeletion) using a combination of backward and forward chaining. This makes deletion exact and avoids the potential inefficiency of overdeletion. In practice, B/F often, but not always, outperforms DRed (Motik et al. 2015).

Both DRed and B/F search for derivations of deleted facts by evaluating rules ‘backwards’: for each rule whose head matches the fact being deleted, they evaluate the partially instantiated rule body as a query; each query answer thus corresponds to a derivation. This has two consequences. First, one can examine rule instances that fire both before and after the update, which is redundant. Second, evaluating rules ‘backwards’ can be inherently more difficult than matching the rules during initial materialisation: our experiments show that this step can, in some cases, prevent effective materialisation maintenance even for very small updates.

In contrast, the Counting algorithm (Gupta, Mumick, and Subrahmanian 1993) does not evaluate rules ‘backwards’, but instead tracks the number of distinct derivations of each fact: a counter is incremented when a new derivation for the fact is found, and it is decremented when a derivation no longer holds. A fact can thus be deleted when its counter drops to zero, without the potentially costly ‘backward’ rule evaluation. The algorithm can also be made optimal in the
sense that it considers precisely the rule instances that no longer fire after the update and the rule instances that only fire after the update. The main drawback of Counting is that, unlike DRed and B/F, it is applicable only to nonrecursive rules (Nicolas and Yazdanian 1983). Recursion is a key feature of datalog, allowing one to express common properties such as transitivity. Thus, despite its favourable properties, the Counting algorithm does not provide us with a general solution to the materialisation maintenance problem.

Towards the goal of developing efficient general-purpose maintenance algorithms, in this paper we present two hybrid approaches that combine DRed and B/F with Counting. The former tracks the nonrecursive and the recursive derivations separately, which allows the algorithm to eliminate all ‘backward’ rule evaluation and also limit overdeletion. The latter tracks nonrecursive derivations only, which eliminates ‘backward’ rule evaluation for nonrecursive rules; however, recursive rules can still be evaluated ‘backwards’ to eagerly identify alternative derivations. Both combinations can handle recursive rules, and they exhibit ‘pay-as-you-go’ behaviour in the sense that they become equivalent to Counting on nonrecursive rules. Apart from the modest cost of maintaining counters, our algorithms never involve more computation steps than their unoptimised counterparts. Thus, our algorithms combine the best aspects of DRed, B/F, and Counting: without incurring a significant cost, they eliminate or reduce ‘backward’ rule evaluation, are optimal for nonrecursive rules, and can also handle recursive rules.

We have implemented our hybrid algorithms and have compared them with the original DRed and B/F algorithms on several synthetic and real-life benchmarks. Our experiments show that the cost of counter maintenance is negligible, and that our hybrid algorithms typically outperform existing solutions, sometimes by orders of magnitude. Our test system and datasets are available online.\(^1\)

2 Preliminaries

We now introduce datalog with stratified negation. We fix countable, disjoint sets of constants and variables. A term is a constant or a variable. A vector of terms is written \(\vec{t} \), and we often treat it as a set. A (positive) atom has the form \(P(t_1, \ldots, t_k)\) where \(P\) is a \(k\)-ary predicate and each \(t_i\), \(1 \leq i \leq k\), is a term. A term or an atom is ground if it does not contain variables. A fact is a ground atom, and a dataset is a finite set of facts. A rule \(r\) has the form

\[
B_1 \land \cdots \land B_m \land \neg B_{m+1} \land \cdots \land \neg B_n \rightarrow H,
\]

where \(m \geq 0\), \(n \geq 0\), and \(B_i\) and \(H\) are atoms. The head \(h(r)\) of \(r\) is the atom \(H\), the positive body \(b^+(r)\) of \(r\) is the set of atoms \(B_1, \ldots, B_m\), and the negative body \(b^-(r)\) of \(r\) is the set of atoms \(B_{m+1}, \ldots, B_n\). Rule \(r\) must be safe: each variable occurring in \(r\) must occur in a positive body atom.

A substitution \(\sigma\) is a mapping of finitely many variables to constants. For \(\alpha\) a term, literal, rule, conjunction, or a vector or set thereof, \(\alpha\sigma\) is the result of replacing each occurrence of a variable \(x\) in \(\alpha\) with \(\sigma(x)\) (if the latter is defined).

A stratification \(\lambda\) of a program \(\Pi\) maps each predicate of \(\Pi\) to a positive integer such that, for each rule \(r \in \Pi\) with

\[
h(r) = P(\vec{t}),
\]

(i) \(\lambda(P) \geq \lambda(R)\) for each atom \(R(\vec{s}) \in b^+(r)\), and

(ii) \(\lambda(P) > \lambda(R)\) for each atom \(R(\vec{s}) \in b^-(r)\).

Program \(\Pi\) is stratifiable if a stratification \(\lambda\) of \(\Pi\) exists. A rule \(r\) with \(h(r) = P(\vec{t})\) is recursive w.r.t. \(\lambda\) if an atom \(R(\vec{s}) \in b^+(r)\) exists such that \(\lambda(P) = \lambda(R)\); otherwise, \(r\) is nonrecursive w.r.t. \(\lambda\). For each positive integer \(s\), program \(\Pi^s = \{ r \in \Pi \mid h(r) = s\}\) is the stratum \(s\) of \(\Pi\), and programs \(\Pi^0\) and \(\Pi^\infty\) are the recursive and the nonrecursive subsets, respectively, of \(\Pi^\infty\). Finally, \(O^\infty\) is the set of all facts that belong to stratum \(s\)—that is, \(O^\infty = \{ P(\vec{e}) \mid \lambda(P) = s\}\).

Rule \(r\) is an instance of a rule \(r'\) if a substitution \(\sigma\) exists mapping all variables of \(r\) to constants such that \(r'\sigma = r\). For \(I\) a dataset, the set \(\text{inst}_r[I]\) of instances of \(r\) obtained by applying a rule \(r\) to \(I\), and the set \(\Pi[I]\) of facts obtained by applying a program \(\Pi\) to \(I\) are defined as follows.

\[
\text{inst}_r[I] = \{ r\sigma \mid b^+(r)\sigma \subseteq I \text{ and } b^-(r)\sigma \cap I = \emptyset \} \quad (1)
\]

\[
\Pi[I] = \bigcup_{r \in \Pi} \{ h(r') \mid r' \in \text{inst}_r[I] \} \quad (2)
\]

We often say that each instance in \(\text{inst}_r[I]\) fires on \(I\). We are now ready to define the semantics of stratified datalog. Given a dataset \(E\) of explicit facts and a stratification \(\lambda\) of \(\Pi\) with maximum stratum index number \(S\), we define the following sequence of datasets: let \(I^0 = E\); let \(I^n = I^{n-1}_\infty\) for index \(s\) with \(1 \leq s \leq S\); let \(I^s_i = I^s_{i-1} \cup I^i_s\) for each integer \(i > 0\); and let \(I^\infty_s = \bigcup_{i \geq 0} I^i_s\). Set \(I^\infty_s\) is called the materialisation of \(\Pi\) w.r.t. \(E\) and \(\lambda\). It is well known that \(I^\infty_s\) does not depend on \(\lambda\), so we usually write it as \(\text{mat}(\Pi, E)\). In this paper, we consider the problem of maintaining \(\text{mat}(\Pi, E)\): given \(\text{mat}(\Pi, E)\) and datasets \(E^-\) and \(E^+\), our algorithm computes \(\text{mat}(\Pi, (E \setminus E^-) \cup E^+)\) incrementally while minimising the amount of work.

3 Motivation and Intuition

As motivation for our work, we next discuss how evaluating rules ‘backwards’ can be a significant source of inefficiency during materialisation maintenance. We base our discussion on the DRed algorithm for simplicity, but our conclusions apply to the B/F algorithm as well.

3.1 The DRed Algorithm

To make our discussion precise, we first present the DRed algorithm (Gupta, Mumick, and Subrahmanian 1993; Staudt and Jarke 1996). Let \(\Pi\) be a program with a stratification \(\lambda\), let \(E\) be a set of explicit facts, and assume that the materialisation \(I = \text{mat}(\Pi, E)\) of \(\Pi\) w.r.t. \(E\) has been computed. Moreover, assume that \(E\) should be updated by deleting \(E^-\) and inserting \(E^+\). The DRed algorithm efficiently modifies the ‘old’ materialisation \(I\) to the ‘new’ materialisation \(I' = \text{mat}(\Pi, (E \setminus E^-) \cup E^+)\) by deleting some facts and adding others; we call such facts affected by the update.

Due to the update, some rule instances that fire on \(I\) will no longer fire on \(I'\), and some rule instances that do not fire on \(I\) will fire on \(I'\); we also call such rule instances affected by the update. A key problem in materialisation maintenance
is to identify the affected rule instances. Clearly, the body of each affected rule instance must contain an affected fact. Based on this observation, the affected rule instances can be efficiently identified by the following generalisation of the operators inst, [I] and Π[I] from Section 2. In particular, let IP, IP, I, and N be datasets such that P ⊆ IP and N ∩ IP = ∅; then, let

\[\text{inst}_{IP, IP} : P, N] = \{ r | b^+(r) σ ∩ IP = ∅ and b^−(r) σ ∩ IP = ∅ \} \tag{3}\]

and let

\[\Pi[IP, IP : P, N] = \bigcup_{r ∈ Π} \{ h(r') | r' ∈ \text{inst}_{IP, IP} : P, N] \} .\]

Intuitively, the positive and the negative rule atoms are evaluated in IP and IP, sets P and N identify the affected positive and negative facts; inst [IP, IP] : P, N] are the affected instances of r; and Π [IP, IP] : P, N] are the affected consequences of Π. We define inst [IP, IP] and Π [IP, IP] analogously to above, but without the condition ‘b^+(r) σ ∩ P = ∅ or b^−(r) σ ∩ N = ∅’. We omit for readability Π whenever IP = IP, and furthermore we omit N when N = ∅. Sets Π [IP, IP] and Π [IP, IP] : P, N] can be computed efficiently in practice by evaluating the body of each rule r ∈ Π as a conjunctive query and instantiating the head as needed.

Algorithm 1 formalises DRed. The algorithm processes each stratum s and accumulates the necessary changes to I in the set D of overdeleted and the set A of added facts. The materialisation is updated in line 6, so, prior to that, I and (I \ D) ∪ A are the ‘old’ and the ‘new’ materialisation, respectively. The computation proceeds in three phases.

In the overdeletion phase, D is extended with all facts that depend on a deleted fact. In line 8 the algorithm identifies the facts that are explicitly deleted (E– ∩ O+) or are affected by deletions in the previous strata (Π[E– ∩ O+) and, then in lines 9–13 it computes their consequences. It uses a form of the seminaive strategy, which ensures that each rule instance is considered only once during overdeletion.

In the one-step rederivation phase, R is computed as the set of facts that have been overdeleted, but that hold nonetheless. To this end, in line 4 the algorithm considers each fact F in D ∩ O+, and it adds F to R if F is explicit or it is rederived by a rule instance. The latter involves evaluating rules ‘backwards’: the algorithm identifies each rule r ∈ Π whose head can be matched to F, and it evaluates over the ‘new’ materialisation the body of r as a query with the head variables bound; fact F holds if the query returns at least one answer. As we discuss shortly, this step can be a major source of inefficiency in practice, and the main contribution of this paper is eliminating ‘backward’ rule evaluation and thus significantly improving the performance.

In the insertion step, in line 15 the algorithm combines the one-step rederived facts (R) with the explicitly added facts (E+ ∪ O+) and the facts added due to the changes in the previous strata (Π[E– ∩ O+]) and, then in lines 16–20 it computes all of their consequences and adds them to A. Again, the seminaive strategy ensures that each rule instance is considered only once during insertion.

### 3.2 Problems with Evaluating Rules ‘Backwards’

The one-step rederivation in line 4 of Algorithm 1 evaluates rules ‘backwards’. In this section we present two examples that demonstrate how this can be a major source of inefficiency. Both examples are derived from datasets we used in our empirical evaluation that we present in Section 6; hence, these problems actually arise in practice.

Our discussion depends on several details. In particular, we assume that all facts are indexed so that all facts matching any given atom (possibly containing constants) can be identified efficiently. Moreover, we assume that conjunctive queries corresponding to rule bodies are evaluated left-to-right: for each match of the first conjunct, we partially instantiate the rest of the body and match it recursively. Finally, we assume that query atoms are reordered prior to evaluation to obtain an efficient evaluation plan.

**Example 1.** Let Π and E be the program and the dataset as specified in (4) and (5), respectively.

\[R(x, y_1) ∧ R(x, y_2) → S(y_1, y_2) \tag{4}\]

\[E = \{ R(a_i, b_i), R(a_i, c_i) | 1 ≤ i ≤ n \} \tag{5}\]

The materialisation mat(Π, E) consists of E extended with facts S(b, b), S(b, c_i), S(c_i, b), and S(c_i, c_i) for 1 ≤ i ≤ n.

During materialisation, the body of rule (4) can be evaluated efficiently left-to-right: we match R(x, y_1) to either R(a_i, b_i) or R(a_i, c_i); this instantiates R(x, y_2) as R(a_i, y_2), and we use the index to find the matching facts R(a_i, b_i) and R(a_i, c_i). Thus, R(x, y_1) has 2n matches, each of which contributes to two matches of R(x, y_2), so the overall cost of rule matching is O(n). The rule body is symmetric, so reordering the body atoms has no effect.

Now assume that we delete all R(a_i, c_i) with 1 ≤ i ≤ n. DRed then overdeletes all S(b, c_i), S(c_i, b) and S(c_i, c_i)
facts in lines 8–13, and this can be done efficiently as in the previous paragraph. Next, in one-step rederivation, the algorithm will match these facts to the head of the rule (4) and obtain queries $R(x, b) \land R(x, c_1), R(x, c_i) \land R(x, b)$, and $R(x, c_j) \land R(x, c_i)$. All but the last of these queries contain atom $R(x, b)$ and, no matter how we reorder the body atoms of (4), we have $n$ queries where $R(x, b)$ is evaluated first. Each of these $n$ queries identifies $n$ candidate matches $R(a_i, b)$ using the index only to find out that the second atom cannot be matched. Thus, $R(x, b)$ is matched to $n^2$ facts in total, so the cost of one-step rederivation is $O(n^2)$—one degree higher than for materialisation.

Example 1 shows that evaluating a rule ‘backwards’ can be inherently more difficult than evaluating it during materialisation, thus giving rise to a dominating source of inefficiency. In fact, evaluating a rule with $m$ body atoms ‘backwards’ can be seen as answering a query with $m + 1$ atoms, where the head of the rule is an extra query atom; since the number of atoms determines the complexity of query evaluation, this extra atom increases the algorithm’s complexity.

Our next example shows that this problem is exacerbated if the space of admissible plans for queries corresponding to rule bodies is further restricted. This is common in systems that provide built-in functions. In particular, to facilitate manipulation of concrete values such as strings or integers, datalog systems often allow rule bodies to contain built-in atoms of the form $(t := \text{exp})$, where $t$ is a term and $\text{exp}$ is an expression constructed using constants, variables, functions, and operators as usual. For example, a built-in atom can have the form $(z := z_1 + z_2)$, and it assigns to $z$ the sum of $z_1$ and $z_2$. The set of supported functions vary among implementations, but a common feature is that all values in $\text{exp}$ must be bound by prior atoms before the built-in atom can be evaluated. As we show next, this can be problematic.

Example 2. Let program $\Pi$ consist of rules (6) and (7). If we read $B(s, t, n)$ as saying that there is an edge from node $s$ to node $t$ of length $n$, then the program entails $D(s, n)$ if there exists a path of length $n$ from node $a$ to node $s$.

$$B(a, y, z) \rightarrow D(y, z) \quad (6)$$

$$D(x, z_1) \land B(x, y, z_2) \land (z := z_1 + z_2) \rightarrow D(y, z) \quad (7)$$

Let $E$ be the dataset as specified below.

$$E = \{B(a, b_1, 1), B(a, c_i, 1), B(b_i, d_j, 1) \mid 1 \leq i, j \leq n\}$$

During materialisation, rule (6) first derives $D(b_1, 1)$ and all $D(c_i, 1)$ with $1 \leq i \leq n$, so the cost of this step is $O(n)$. Next, atom $D(x, z_1)$ in rule (7) is matched to $n$ facts $D(c_i, 1)$ without deriving anything. Atom $D(x, z_1)$ is also matched to $D(b_1, 1)$ once, so atom $B(x, y, z_2)$ is instantiated to $B(b_1, y, z_2)$ and matched to $n$ facts $B(b_i, d_j, 1)$, deriving $n$ facts $D(d_j, 2)$. Thus, the cost of rule matching is $O(n)$.

Now assume that $B(a, b_1, 1)$ is deleted. Then, $D(b_1, 1)$ and all $D(d_j, 2)$ can be efficiently overdeleted as in the previous paragraph, but trying to prove them is much more difficult. Matching each $D(d_j, 2)$ to the head of (6) produces a query $B(a, d_j, 2)$, which does not produce a rule instance. Moreover, matching $D(d_j, 2)$ to the head of (7) produces a query $D(x, z_1) \land B(x, d_j, z_2)$ and $D(x, z_1) \land B(x, d_j, z_2)$ and $B(x, d_j, z_2)$ and $B(x, d_j, z_2)$. Now, as we discussed earlier, $z_1$ and $z_2$ must both be bound before we can evaluate the built-in atom $(2 := z_1 + z_2)$. If we evaluate $B(x, d_j, z_2)$ first, then we try $n$ facts $B(b_i, d_j, 1)$ with $1 \leq i \leq n$; for each of them, atom $D(x, z_1)$ is instantiated as $D(b_i, z_1)$ and is not matched in the surviving facts. In contrast, if we evaluate $D(x, z_1)$ first, then we try $n$ facts $D(c_i, 1)$; for each of them, atom $B(x, d_j, z_2)$ is instantiated as $B(c_i, y, z_2)$ and is not matched. Thus, regardless of how we reorder the body of (7), the first atom considers a total of $n^2$ facts, so the cost of one-step rederivation is $O(n^2)$.

To overcome this, one might rewrite the built-in atom as $(z_1 := z - z_1)$ or $(z_2 := z - z_2)$ so that it can be evaluated immediately after $z$ and either $z_1$ or $z_2$ are bound. Either way, one-step rederivation still takes $O(n^2)$ steps on our example. Also, built-in expressions are often not invertible.

## 4 Combining DRed with Counting

We now address the inefficiencies we outlined in Section 3. Towards this goal, in Section 4.1 we first present the intuitions, and then in Section 4.2 we formalise our solution.

### 4.1 Intuition

As we already mentioned in Section 1, the Counting algorithm (Gupta, Mumick, and Subrahmanian 1993) does not evaluate rules ‘backwards’; instead, it tracks the number of derivations of each fact. The main drawback of Counting is that it cannot handle recursive rules. We now illustrate the intuition behind our DRed\textsuperscript{c} algorithm, which combines DRed with Counting in a way that eliminates ‘backward’ rule evaluation, while still supporting recursive rules.

The DRed\textsuperscript{c} algorithm associates with each fact two counters that track the derivations via the nonrecursive and the recursive rules separately. The counters are decremented (resp., incremented) when the associated fact is derived in overdeletion (resp. insertion), which allows for two important optimisations. First, as in the Counting algorithm, the nonrecursive counter always reflects the number of derivations from facts in earlier strata; hence, a fact with a nonzero nonrecursive counter should never be overdeleted because it clearly remains true after the update. This optimisation captures the behaviour of Counting on nonrecursive rules and it also helps limit overdeletion. Second, if we never overdelete facts with nonzero nonrecursive counters, the only way for a fact to still hold after overdeletion is if its recursive counter is nonzero; hence, we can replace ‘backward’ rule evaluation by a simple check of the recursive counter. Note, however, that the recursive counters can be checked only after overdeletion finishes. This optimisation extends the idea of Counting to recursive rules to completely avoid ‘backward’ rule evaluation. The following example illustrates these ideas and compares them to DRed.

Example 3. Let $\Pi$ be the program containing rule (8).

$$A(x) \land B(x, y) \rightarrow A(y) \quad (8)$$

Moreover, let $E$ be defined as follows:

$$E = \{A(a), A(b), A(d), B(a, c), B(b, c), B(c, d), B(d, e)\}$$
4.2 Formalisation

We now formalise our DRed$^\circ$ algorithm. Our definitions use the standard notion of multisets—a generalisation of sets where each element is associated with a positive integer called the multiplicity specifying the number of the element’s occurrences in the multiset. Moreover, $\oplus$ is the multiset union operator, which adds the elements’ multiplicities. If an operand of $\oplus$ is a set, it is treated as a multiset where all elements have multiplicity one. Finally, we extend the notion of rule matching to correctly reflect the number of times a fact is derived: for $I^p, I^+$, and $N$ datasets with $P \subseteq I^p$ and $N \cap I^p = \emptyset$, we define $\Pi[I^p, I^+; P, N]$ as the multiset containing a distinct occurrence of $h(r')$ for each rule $r \in I^+$ and its instance $r' \in \text{inst}_r[I^p, I^+; P, N]$. This multiset can be computed analogously to $\Pi[I^p, I^+; P, N]$.

Just like DRed, the DRed$^\circ$ takes as input a program $I$, a stratification $\lambda$, a set of explicit facts $E$ and its materialisation $I = \text{mat}(\Pi, E)$, and the sets of facts $E^-$ and $E^+$ to remove from and add to $E$. Additionally, the algorithm also takes as input maps $C_r$ and $C_f$ that associate each fact $F$ with its nonrecursive and recursive counters $C_r[F]$ and $C_f[F]$, respectively. These maps should correctly reflect the relevant numbers of derivations. Formally, $C_r$ and $C_f$ must be compatible with $\Pi$, $\lambda$, and $E$, which is the case if $C_r[F] = C_f[F] = 0$ for each fact $F \notin I$, and for each fact $F \in I$ and $s$ the stratum index such that $F \in O^s$ (i.e., $s$ is the index of the stratum that $F$ belongs to),

- $C_r[F]$ is the multiplicity of $F$ in $E \oplus \Pi[I^p[I]]$, and
- $C_f[F]$ is the multiplicity of $F$ in $\Pi[I^p[I]]$.

For simplicity, we assume that $C_r$ and $C_f$ are defined on all facts, and that $C_r[F] = C_f[F] = 0$ holds for $F \notin I$; thus, we can simply increment the counters for each newly derived fact in procedure INSERT. In practice, however, one can maintain counters only for the derived facts and initialise the counters to zero for the freshly derived facts.

DRed$^\circ$ is formalised in Algorithm 2. Its structure is similar to DRed, with the following main differences: instead of evaluating rules ‘backwards’, one-step derivation simply checks the recursive counters (line 24); a fact is overdeleted only if the nonrecursive derivation counter is zero (line 34); and the derivation counters are decremented in overdeletion (lines 29–32 and 36–37) and incremented in insertion (lines 41–44 and 49–50). The algorithm also accumulates changes to the materialisation in sets $D$ and $A$ by iteratively processing the strata of $\lambda$ in three phases.

In the overdeletion phase, DRed$^\circ$ first considers explicitly deleted facts or facts affected by the changes in earlier strata (lines 29–32). This is analogous to line 8 of DRed, but DRed$^\circ$ must distinguish $\Pi[I^+_r]$ from $\Pi[I_r]$ so it can decrement the appropriate counters. Next, DRed$^\circ$ identifies the set $\Delta_D$ of facts that have not yet been deleted and whose nonrecursive counter is zero (line 34): a fact with a nonzero nonrecursive counter will always be part of the ‘new’ materialisation. Note that recursive derivations can be cyclic, so we cannot use the recursive counter to further constrain overdeletion at this point. Then, in lines 35–38 the algorithm propagates consequences of $\Delta_D$ just like Algorithm 1, with additionally decrementing the recursive counters in line 37.
Algorithm 2 \( \text{DRed}^c(\Pi, \lambda, E, I, E^-, E^+, C_m, C) \)

\begin{align*}
21: & \quad D := A = \emptyset, \quad E = (E^+ \cap E^-) \setminus E^+, \quad E^+ = E^+ \setminus E \\
22: & \quad \text{for each stratnum index } s \text{ with } 1 \leq s \leq S \text{ do} \\
23: & \quad \text{INSERT} \\
24: & \quad R := \{ F \in D \cap O^s \mid C_i[F] > 0 \} \\
25: & \quad \text{INSERT} \\
26: & \quad E := (E \setminus E^-) \cup E^+, \quad I := (I \setminus D) \cup A \\
27: & \quad \text{procedure OVERDELETE} \\
28: & \quad N_D := \emptyset \\
29: & \quad \text{for } F \in (E^+ \cap O^s) \cap \Pi^s \text{ do} \\
30: & \quad N_D := N_D \cup \{ F \}, \quad C_m[F] := C_m[F] - 1 \\
31: & \quad \text{for } F \in \Pi^s[I \setminus D \setminus A, A \setminus D] \text{ do} \\
32: & \quad N_D := N_D \cup \{ F \}, \quad C_i[F] := C_i[F] - 1 \\
33: & \quad \text{loop} \\
34: & \quad \Delta_D := \{ F \in N_D \setminus D \mid C_m[F] = 0 \} \\
35: & \quad \text{if } \Delta_D = \emptyset \text{ then break} \\
36: & \quad \text{for } F \in \Pi^s[I \setminus D \setminus A, I \cup A : \Delta_D] \text{ do} \\
37: & \quad N_D := N_D \cup \{ F \}, \quad C_i[F] := C_i[F] - 1 \\
38: & \quad D := D \cup \Delta_D \\
39: & \quad \text{procedure INSERT} \\
40: & \quad N_A := R \\
41: & \quad \text{for } F \in (E^+ \cap O^s) \cap \Pi^s \text{ do} \\
42: & \quad N_A := N_A \cup \{ F \}, \quad C_m[F] := C_m[F] + 1 \\
43: & \quad \text{for } F \in \Pi^s[I \setminus D \setminus A, A \setminus D] \text{ do} \\
44: & \quad N_A := N_A \cup \{ F \}, \quad C_i[F] := C_i[F] + 1 \\
45: & \quad \text{loop} \\
46: & \quad \Delta_A := \{ N_A \setminus (I \setminus D) \cup A \} \\
47: & \quad \text{if } \Delta_A = \emptyset \text{ then break} \\
48: & \quad A := A \cup \Delta_A \\
49: & \quad \text{for } F \in \Pi^s[I \setminus D \setminus A, A : \Delta_A] \text{ do} \\
50: & \quad N_A := N_A \cup \{ F \}, \quad C_i[F] := C_i[F] + 1
\end{align*}

In the one-step rederivation phase, instead of evaluating rules ‘backswards’, \( \text{DRed}^c \) just checks the recursive counter of each fact \( F \in D \cap O^s \) (line 24); if \( C_i[F] \neq 0 \), then some derivations of \( F \) were not ‘touched’ by overdeletion so \( F \) holds in the ‘new’ materialisation. Conversely, if \( C_i[F] = 0 \), then \( F \in D \) guarantees that \( C_m[F] = 0 \) holds as well, so \( F \) is not one-step rederivable by a rule in \( \Pi \).

The insertion phase of \( \text{DRed}^c \) just uses the seminaive evaluation while incrementing the counters appropriately.

Without recursive rules, \( \text{DRed}^c \) becomes equivalent to Counting, and it is optimal in the sense that only affected rule instances are considered during the update. Moreover, the computational complexities of both \( \text{DRed}^c \) and \( \text{DRed} \) are the same as for the semi-naive materialisation algorithm: Exptime in combined and Ptime in data complexity (Dantsin et al. 2001). Finally, \( \text{DRed}^c \) never performs more inferences than \( \text{DRed} \) and is thus more efficient. Theorem 1 shows that our algorithm is correct, and its proof is given in full in Appendix A.

Theorem 1. Algorithm 2 correctly updates \( I = \text{mat}(\Pi, E) \) to \( I' = \text{mat}(\Pi, E') \) for \( E' = (E \setminus E^-) \cup E^+ \), and it updates \( C_m \) and \( C_i \) so they are compatible with \( \Pi, \lambda, \) and \( E' \).
dure propagates its consequences (line 80–85). In particular, the procedure ensures that each consequence $F'$ of $P$, the facts in the ‘new’ materialisation in the previous strata, and the recursive rules is added to $P$ if $F' \in C$, or is added to the set $Y$ of delayed facts if $F' \notin C$. Intuitively, set $Y$ contains facts that are proved but that have not been checked yet. If a fact in $Y$ is checked at a later point, it is proved in line 79 without having to apply the rules again.

Since the deletion step of $B/F^c$ is ‘exact’ in the sense that it deletes precisely those facts that no longer hold after the update, rederivation is not needed. Thus, $\text{DELETEUNPROVED}$ is directly followed by $\text{INSERT}$, which is the same as in DRed and DRed+, with the only difference that $B/F^c$ maintains only the nonrecursive counters.

Algorithm 3 is correct in the same way as $B/F$ since checking whether a fact has a nonzero nonrecursive counter is equivalent to checking whether a derivation of the fact exists by evaluating nonrecursive rules ‘backwards’.

### 6 Evaluation

We have implemented the unoptimised and optimised variants of DRed and B/F and have compared them empirically.

**Benchmarks** We used the following benchmarks for our evaluation: UOBM (Ma et al. 2006) is a synthetic benchmark that extends the well known LUBM (Guo, Pan, and Helfin 2005) benchmark; Reactome (Croft et al. 2013) models biological pathways of molecules in cells; Uniprot (Bateman et al. 2015) describes protein sequences and their functional information; ChemBL (Gaulton et al. 2011) represents functional and chemical properties of bioactive compounds; and Claros describes archeological artefacts. Each benchmark consists of a set of facts and an OWL 2 DL ontology, which we transformed into datalog programs of different levels of complexity and recursiveness. More specifically, the upper bound (U) programs were obtained using the complete but unsound transformation by Zhou et al. (2013), and they entail all consequences of the original ontology but may also derive additional facts. The recursive (R) programs were obtained using the sound but incomplete transformation by Kaminski, Nenov, and Grau (2016), and they tend to be highly recursive. For Claros, the lower bound extended (LE) program was obtained by manually introducing several ‘hard’ rules, and it was already used by Motik et al. (2015) to compare DRed with B/F. Finally, to estimate the effect of built-in literals on materialisation maintenance, we developed a new synthetic benchmark SSPE (Single-Source Path Enumeration). Its dataset consists of a randomly generated directed acyclic graph of 100 k nodes and 1 M edges, and its program traverses paths from a single source analogously to rules (6)–(7). All the tested programs are recursive, although the percentage of the recursive rules varies. Table 1 shows the numbers of facts ($|E|$), strata ($S$), the nonrecursive rules ($|\Pi_n|$), and the recursive ones ($|\Pi_r|$) for each benchmark.

**Test Setup** We conducted all experiments on a Dell PowerEdge R720 server with 256GB RAM and two Intel Xeon E5-2670 2.6GHz processors, running Fedora 24, kernel version 4.8.12-200.fc24.x86_64. All algorithms handle insertions using the seminaive evaluation. The only overhead is in counter maintenance, which we measured during initial materialisation (which also uses seminaive evaluation). Hence, the main focus of our tests was on comparing the performance of our algorithms on ‘small’ and ‘large’ deletions. In both cases, we first materialised the relevant program on the explicit facts, and then we performed the following tests.

To test small deletions, we measured the performance on
ten randomly selected subsets $E^- \subseteq E$ of 1,000 facts. In all apart from Claros-LE, the running times did not depend significantly on the selected subset of $E$, so in Table 1 we report the average times across all ten runs. On Claros-LE, however, the running times varied significantly, so we report in the table the best, the worst, and the average times.

To test large deletions, we identified the largest subset $E^- \subseteq E$ on which either DRed$^c$ or B/F$^c$ takes roughly the same time as computing the 'new' materialisation from scratch. We measured the performance of all algorithms on $E^-$, as well as the performance of rematerialisation with no counters (Remat), just the nonrecursive counter (Remat-1C), and both counters (Remat-2C). This test allows us to assess the scalability of our algorithms. Table 2 reports the running times and the percentages of the deleted facts.

**Discussion** DRed$^c$ outperformed DRed on all inputs for small deletions. In particular, on SSPE, the average running time for DRed drops from 28 minutes to just over 10 seconds. On Reactome-U, the improvement is by several orders of magnitude, albeit unoptimised DRed is already quite efficient. The improvement is also significant in many other cases, including UOBM-U, Reactome-R, and ChemBL-R. In fact, Reactome-U and SSPE exhibit data and rule patterns outlined in Examples 1 and 2, which clearly demonstrates the benefits of eliminating ‘backward’ rule evaluation. Moreover, the program of Claros-LE contains a symmetric and transitive predicate relatedPlaces, so the materialisation contains several large cliques of constants connected by this predicate (Motik et al. 2015). When a fact relatedPlaces$(a, b)$ is overdeleted, the DRed algorithm overdeletes all relatedPlaces$(c, d)$ where $c$ and $d$ belong to the same clique as $a$ and $b$, which requires a cubic number of derivations. However, DRed$^c$ can sometimes (but not always) prove that relatedPlaces$(a, b)$ holds using the nonrecursive counter; as one can see, this can considerably improve the performance by avoiding costly overdeletion.

B/F$^c$ also outperformed B/F for small deletions in many cases: B/F$^c$ was more than 20 times faster for UOBM-U, Reactome-U, and the ‘best’ case of Claros-LE, which is in line with our observation that ‘backwards’ rule evaluation can be quite costly. In contrast, on the highly recursive datasets (i.e., all R-datasets and SSPE), the performance of B/F$^c$ and B/F is roughly the same: the main source of difficulty is due to the recursive rules, whose evaluation is unaffected by the optimisations proposed in this paper.

B/F$^c$ outperformed DRed$^c$ on all datasets but SSPE. This is so because B/F$^c$ eagerly identifies alternative derivations of facts, which is often easy, and is beneficial since it can considerably reduce overdeletion. However, as we discussed earlier in Section 3, backward rule evaluation can be a dominant source of inefficiency (e.g., on SSPE). In such cases, DRed$^c$ is faster than B/F$^c$ since DRed$^c$ completely eliminates backward rule evaluation, whereas B/F$^c$ only avoids backward evaluation on nonrecursive rules.

The tests for large deletions show that our algorithms can efficiently delete large subsets of the explicit facts on all but two benchmarks: Claros-LE and SSPE. Claros-LE is difficult due to the presence of cliques as explained earlier, and SSPE is difficult because deleting a small percentage of the explicit facts leads to the deletion of about half of the inferred facts. Nevertheless, DRed$^c$ always considerably outperforms DRed; the difference is particularly significant on Reactome-U and SSPE, where DRed$^c$ is several orders of

| Dataset   | $|E^-|/|E|$ | DRed$^c$ | DRed | B/F$^c$ | B/F | Remat | Remat-1C | Remat-2C |
|-----------|-----------|---------|------|--------|-----|-------|----------|----------|
| UOBM-U    | 50%       | 1.54 k  | 3.66 k | 1.64 k | 3.11 k | 1.56 k | 1.60 k    | 1.61 k    |
| UOBM-R    | 36%       | 3.28 k  | 5.75 k | 2.76 k | 2.87 k | 4.14 k | 4.16 k    | 4.19 k    |
| Reactome-U| 68%       | 30.70 k | 6.32 k | 39.16 | 6.33 k | 30.90 | 31.23    | 31.32     |
| Reactome-R| 31%       | 1.78 k  | 1.92 k | 0.92 k | 0.93 k | 0.91 k | 0.91 k    | 0.92 k    |
| Uniprot-R | 47%       | 1.67 k  | 1.92 k | 1.92 k | 2.86 k | 1.98 k | 1.99 k    | 2.00 k    |
| ChemBL-R  | 69%       | 4.74 k  | 3.17 k | 3.25 k | 4.18 k | 2.56 k | 2.57 k    | 2.59 k    |
| Claros-LE | 8%        | 5.01 k  | 17.81 k| 3.49 k | 16.74 k| 3.36 k | 3.49 k    | 3.60 k    |
| SSPE      | 2%        | 74.36 k | 7.24 k | 7.90 k | 7.75 k | 68.28 | 70.18     | 71.81     |

Table 2: Running times for handling large deletions (seconds)
magnitude faster. Similarly, B/F consistently outperforms B/F on all cases apart from SSPE, where the latter is due to the overhead of maintaining the counters.

Finally, the rematerialisation times show that counter maintenance incurs only modest overheads: Remat-2C was in the worst case only several percent slower than Remat.

7 Conclusion
We have presented two novel algorithms for the maintenance of datalog materialisations, obtained by combining the well-known DRed and B/F algorithms with Counting. Our evaluation shows that our algorithms are generally more efficient than the original ones, often by orders of magnitude. Our algorithms could handle both small and large updates efficiently, and have thus been shown to be ready for practical use. In future, we shall develop a modular approach to materialisation and its maintenance that tackles the difficult cases such as Claros-LE using reasoning modules that can be ‘plugged into’ the seminaive evaluation to handle difficult rule combinations using custom algorithms.

Acknowledgments
This work was supported by the EPSRC projects MaSI3, DBOnto, and ED3.

References
Abiteboul, S.; Hull, R.; and Vianu, V. 1995. Foundations of Databases. Addison-Wesley.
Bateman, A.; Martin, M.; O’Donovan, C.; Magrane, M.; Apweiler, R.; Alpi, E.; Antunes, R.; Arganiska, J.; Bely, B.; Bingley, M.; et al. 2015. UniProt: a hub for protein information. Nucleic Acids Research 43(D1):D204–D212.
Bishop, B.; Kiryakov, A.; Ognyanoff, D.; Peikov, I.; Tashev, Z.; and Velkov, R. 2011. OWLIM: A family of scalable semantic repositories. SWJ 2(1):33–42.
Croft, D.; Mundo, A. F.; Haw, R.; Milacic, M.; Weiser, J.; Wu, G.; Caudy, M.; Garapati, P.; Gillespie, M.; Kamdar, M. R.; et al. 2013. The Reactome pathway Knowledgebase. Nucleic acids research 42(D1):D472–D477.
Dantsin, E.; Eiter, T.; Gottlob, G.; and Voronkov, A. 2001. Complexity and Expressive Power of Logic Programming. ACM Computing Surveys 33(3):374–425.
Gaulton, A.; Bellis, L. J.; Bento, A. P.; Chambers, J.; Davies, M.; Hersey, A.; Light, Y.; McGlinchey, S.; Michalovich, D.; Al-Lazikani, B.; et al. 2011. ChEMBL: a large-scale bioactivity database for drug discovery. Nucleic acids research 40(D1):D1100–D1107.
Guo, Y.; Pan, Z.; and Heflin, J. 2005. LUBM: A benchmark for OWL knowledge base systems. Web Semantics: Science, Services and Agents on the World Wide Web 3(2):158–182.
Gupta, A.; Mumick, I. S.; and Subrahmanian, V. S. 1993. Maintaining Views Incrementally. In SIGMOD. ACM.
Horrocks, I.; Patel-Schneider, P. F.; Boley, H.; Tabet, S.; Grosof, B.; Dean, M.; et al. 2004. SWRL: A Semantic Web Rule Language Combining OWL and RuleML. W3C Member Submission.
A Proof of Correctness for Algorithm 2

Theorem 1. Algorithm 2 correctly updates $I = \mathit{mat}(\Pi, E)$ to $I' = \mathit{mat}(\Pi, E')$ for $E' = (E \setminus (E \land E')) \cup E'$, and it updates $C_{nr}$ and $C_r$ so that they are compatible with $\Pi$, $\lambda$, and $E'$.

Proof. Let $\ominus$ be the multiset subtraction operator, and let $\mathit{Occ}(F, M)$ be the multiplicity of $F$ in multiset $M$. Due to line 21 of Algorithm 2, without loss of generality we assume that $E' \subseteq E$ and $E' \cap E = \emptyset$. Let $I'_o = E$ and let $I'_0|_o = \emptyset$. Moreover, for each $1 \leq s \leq S$, let $I'_0|_o, I'_1|_o, \ldots$ be the sequence of sets where $I'_0|_o = I'_{s-1}|_o \cup (E|_o \cap O^s)$, and for $i > 0$, $I'_i|_o = I'_{i-1}|_o \cup I'_i|_o \cap (I'_{i-1}|_o \cap O^s)$. Index $i$ clearly exists at which the sequence reaches the fixpoint (i.e., $I'_i|_o = I'_{i+1}|_o$), so let $I'_n|_o = I'_{i}|_o$. Finally, let $I'_o = I^0|_o$; we clearly have $I'_o = \mathit{mat}(\Pi, E|_o)$—that is, $I'_o$ is the ‘old’ materialisation. Now let $E|_n = (E|_o \setminus (E' \cup E)) \cup E'$, and let $I'_n|_o, I'_n|_n$, and $I'_n|_o$ be defined analogously, so $I'_n|_o$ is the ‘new’ materialisation.

For each $1 \leq s \leq S$ and each $F \in I'_{s}|_o \cap O^s$, let $C_{nr}[F]|_o = \mathit{Occ}(F, E|_o \cup \Pi_{nr}^n[I'_o|_n])$ and $C_r[F]|_o = \mathit{Occ}(F, \Pi_r^e[I'_o|_n])$; we define $C_{nr}[F]|_n$ and $C_r[F]|_n$ analogously using $I'_n|_n$ and $E|_n$.

Now consider a run of Algorithm 2 on $I'_o, E'$, and $E'$. Let $D^0 = A^0 = R^0 = \emptyset$, and for each $s$ with $1 \leq s \leq S$, let $D^s$, $A^s$, and $R^s$ be the values of $D, A$, and $R$, respectively, after the loop in lines 22–25 finishes for stratum index $s$. Note that during the execution of Algorithm 2, the set $I$ is equal to $I_{s+1}^n$ up to before line 26. Furthermore, for each fact $F \in I'_{s}|_o \cap O^s$, let $C_{nr}[F]|_n$ and $C_r[F]|_n$ be the values of $C_{nr}[F]$ and $C_r[F]$, respectively, at the point when $\mathit{OVERDELETE}$ finishes for stratum index $s$; similarly, for each fact $F \in (I'_{s}|_o \setminus D^s) \cup A^s \cap O^s$, let $C_{nr}[F]|_a$ and $C_r[F]|_a$ be the values of $C_{nr}[F]$ and $C_r[F]$, respectively, at the point when $\mathit{INSERT}$ finishes for stratum index $s$.

\[
\Pi^e[I'_o|_n] = \Pi^e[I'_0|_n \cup (D^s \setminus A^s) \cup A^s] \cup \Pi^e[I'_0|_n \cup (D^s \setminus A^s)]
\]
\[
\Pi^e[I'_0|_n] = \Pi^e[I'_0|_n \cup (D^s \setminus A^s) \cup A^s] \cup \Pi^e[I'_0|_n \cup (D^s \setminus A^s)]
\]
\[
C_{nr}[F]|_o - C_{nr}[F]|_n = \mathit{Occ}(F, \Pi^e[I'_0|_n \cup (D^s \setminus A^s) \cup A^s])
\]
\[
C_r[F]|_o - C_r[F]|_n = \mathit{Occ}(F, \Pi^e[I'_0|_n \cup (D^s \setminus A^s)])
\]

We shall prove that properties (13), (15), and (16) hold for each $s$ with $0 \leq s \leq S$, and that the other properties hold for each $s$ with $1 \leq s \leq S$. Then, property (16) for $s = S$ and line 26 of Algorithm 2 imply that $I$ is correctly updated from $I'_o$ to $I'_n|_o$. Moreover, $C_{nr}[F]|_o = \mathit{Occ}(F, E|_o \cup \Pi_{nr}^n[I'_o|_n])$ and properties (16), (9), (11) and (17) for $1 \leq s \leq S$ jointly imply the following:

\[
C_{nr}[F]|_a = C_{nr}[F]|_o - (C_{nr}[F]|_o - C_{nr}[F]|_n) + (C_{nr}[F]|_o - C_{nr}[F]|_d) = \mathit{Occ}(F, E|_o \cup \Pi_{nr}^n[I'_o|_n])
\]

In addition, (16) and (18) imply $C_{nr}[F]|_a = C_{nr}[F]|_n$ for each $F \in (I'_{s}|_o \setminus I'_{s}|_o \cap O^s$. Therefore, we have $C_{nr}[F]|_a = C_{nr}[F]|_n$ for each $F \in I'_{s}|_o \cap O^s$, which means the nonrecursive counts are correctly updated after the execution of the algorithm. $C_r[F]|_a = C_r[F]|_n$ can be shown analogously using properties (16), (10), (12), (19), and (20).

We prove properties (9)–(20) by induction on $s$. The base case where $s = 0$ is trivial since all relevant sets in (13), (15), and (16) are empty. For the inductive step, we consider an arbitrary $s$ with $1 \leq s \leq S$ such that (13), (15), and (16) hold for $s - 1$, and we show that properties (9)–(20) hold for $s$. The proof is lengthy so we break it into several claims.

Claim 2. Properties (9) and (10) hold.
Proof. The way sets $D$ and $A$ are constructed ensures that $(D \setminus D^s) \cap O^<s = \emptyset$ and $A^{s-1} \subseteq O^<s$ hold and so $A^{s-1} \setminus D^s = A^{s-1} \setminus D^s$ holds as well, which in turn implies $I^s \setminus (A^{s-1} \setminus D^s) = I^s \setminus (A^{s-1} \setminus D^s)$. Moreover, the induction assumption $D^{s-1} \subseteq I^{s-1}$ ensures $I^s \setminus (A^{s-1} \setminus D^s) = I^s \setminus (A^{s-1} \setminus D^s)$. Therefore, we have $I^s \setminus (A^{s-1} \setminus D^s) = I^s \setminus A^{s-1}$, which together with the definition of rule application ensures the correctness of the two properties.

Claim 3. Property (11) holds.

Proof. Consider an arbitrary $F \in I^s \cap O^s$, we have two cases here. If $F \notin (E^s \cap O^s) \cup \Pi_{\text{nr}}[I^s] \cup (A^{s-1} \setminus D^s)$, then the right-hand side of the equation in (11) equals zero. Moreover, $\Pi_{\text{nr}}$ contains only nonrecursive rules, and $A^{s-1} \setminus D^s = A^{s-1} \setminus D^s$ holds for the same reason as explained in the proof of claim 2; thus we have $F \notin (E^s \cap O^s) \cup \Pi_{\text{nr}}[I^s] \cup (A^{s-1} \setminus D^s)$; but then, line 29 of Algorithm 2 ensures that the nonrecursive count of $F$ is not decremented during the execution of the OVERDELETE procedure, so the left-hand side of the equation is equal to zero as well. Therefore the property holds in this case.

If $F \in (E^s \cap O^s) \cup \Pi_{\text{nr}}[I^s] \cup (A^{s-1} \setminus D^s) = (E^s \cap O^s) \cup \Pi_{\text{nr}}[I^s] \cup (A^{s-1} \setminus D^s)$, then line 29 and line 30 guarantee that each distinct occurrence of $F$ in $(E^s \cap O^s) \cup \Pi_{\text{nr}}[I^s] \cup (A^{s-1} \setminus D^s)$ results in decrementing the nonrecursive count of $F$ by one. Thus the property also holds in this case.

Claim 4. Property (12) holds.

Proof. Line 34 and line 38 ensure that $\Delta D$ used in line 36 is different between two iterations of the loop in lines 33-38, so the rule instances considered in line 36 are different between iterations. The total number of these rule instances is finite and is bounded by the number of rule instances in $\bigcup_{r \in \Pi^s} \text{inst}[I^s]$, so the proof must terminate, and we let $T$ be the total number of iterations. Moreover, for each $1 \leq i \leq T$, let $D^s$ be the value of $D$ at the beginning of the $i$th iteration of the loop, and let $C_r[F]_i$ be the value of $C_r[F]$ for each $F \in I^s \cap O^s$ at the same time point. We prove by induction on $i$ that (22) holds for $1 \leq i \leq T$. Then (22) for $i = T$ and $A^{s-1} \setminus D^s = A^{s-1} \setminus D^s$ ensure the correctness of property (12).

For the base case, consider an arbitrary $F \in I^s \cap O^s$. It is easy to see that the recursive count of $F$ has never been changed and should be equal to $C_r[F]_i$ before line 31 of procedure OVERDELETE for stratum $s$. But then, line 31 and line 32 ensure that if $F \in \Pi^s_r[I^s] \cup (A^{s-1} \setminus D^s)$, then each distinct occurrence of $F$ in the multiset results in decrementing the corresponding recursive count by one; moreover, if $F \notin \Pi^s_r[I^s] \cup (A^{s-1} \setminus D^s)$, then the corresponding recursive count will not be changed; either way, $D^s = A^{s-1} \setminus D^s$ implies $C_r[F]_i - C_r[F]_i = \text{Occ}(F, \Pi^s_r[I^s] \cup (A^{s-1} \setminus D^s))$, as required.

For the inductive step, assume that (22) holds for $i - 1$ where $1 < i \leq T$, and consider arbitrary $F \in I^s \cap O^s$. Lines 34, 36 and 38 jointly imply (23).

Claim 5. The right-hand inclusion of property (13) holds.
Proof. For each rule \( r \in \Pi^s \), procedure \textsc{Overdelete} for stratum index \( s \) considers in lines 29, 31, and 36 only instances of \( r \) that are contained in \( \text{inst}_s[I^*_o] \), so the facts derived by these rule instances are in \( I^*_o \). Thus, the claim holds by a straightforward induction on the construction of the set \( D^s \).

\begin{claim}
\textbf{The left-hand inclusion of property (13) holds.}
\end{claim}

\begin{proof}
We show by induction that (26) holds for each \( i \).
\[ I^*_i | o \cap I^*_i | n \subseteq D^s \quad (26) \]
For the base case, note that \( I^*_i | o = I^*_i | o \cap (E | o \cap O^s) \) and that \( I^*_i | o \cap I^*_i | n \subseteq D^s \) holds for \( s - 1 \) by the induction assumption. Now consider an arbitrary fact \( F \in E | o \cap O^s \) such that \( F \not\in I^*_i | n \) holds. Then, the latter ensures \( F \not\in E | o \) and so \( F \) is added to \( N_D \) in line 30. We next show that \( F \) is added to \( D \) in line 38: \( F \not\in I^*_i | n \) and \( I^*_i | n = I^*_i | n \cap \Pi^*| I^*_i | n \) imply \( \text{Occ}(F, \Pi^*_o[I^*_i | n]) = 0 \), which in turn implies \( \text{Occ}(F, \Pi^*_o[I^*_i | n]) = 0 \); but then, \( I^*_i | o \cap (D^s \setminus A^s) \subseteq (I^*_i | o \cap D^s) \cup A^s \) and the induction assumption \( (I^*_i | o \cap D^s) \cup A^s = I^*_i | n \) ensure \( \text{Occ}(F, \Pi^*_o[I^*_i | o \cap (D^s \setminus A^s)]) = 0 \), together with (9), (11), and the definition of \( C_n[F] | o \) this implies \( C_n[F] | o = 0 \), so the condition in line 34 is satisfied. Hence, \( F \in D^s \) holds, as required.

For the inductive step, assume that \( I^*_i-1 | o \) satisfies (26) for \( i > 0 \), and consider arbitrary \( F \in I^*_i | o \setminus I^*_i | n \). If \( F \in I^*_i-1 | o \), then \( F \in D^s \) holds by the induction assumption. Otherwise, there exist a rule \( r \in \Pi^s \) and its instance \( r' \in \text{inst}_s[I^*_i-1 | o] \) such that \( F \in h(r') \). Definition (3) ensures \( b^+(r') \subseteq I^*_i-1 | o \subseteq I^*_i | o \) and \( b^-(r') \cap I^*_i-1 | o = \emptyset \), and \( b^-(r') \subseteq O^s \) implies \( b^+(r') \cap I^*_i-1 | o = b^+(r') \cap I^*_i-1 | o = \emptyset \). Finally, \( F \not\in I^*_i | n \) implies \( r' \not\in \text{inst}_r[I^*_i | n] \), so by definition (3) we have one of the following two possibilities.

- \( b^+(r') \not\subseteq I^*_i | n \). Thus, a fact \( G \in b^+(r') \) exists such that \( G \in I^*_i-1 | o \setminus I^*_i | n \) holds. The induction assumption for (26) implies \( G \in D^s \), and \( G \not\in I^*_i | n \) implies \( G \not\in I^*_i | n \), so the induction assumption for (16) ensures \( G \not\in A^s \); hence, \( G \in D^s \setminus A^s \).
- \( b^-(r') \cap I^*_i-1 | n = b^-(r') \cap I^*_i | n = \emptyset \). Thus, a fact \( G \in b^-(r') \) exists such that \( G \in I^*_i-1 | n \setminus I^*_i-1 | o \) holds; but then, the right-hand inclusion of (13) implies \( G \not\in D^s \), and the induction assumption for (16) implies \( G \in A^s \); therefore, we have \( G \in A^s \setminus D^s = A^s \setminus D^s \).

Either way, the right-hand side of (11) or (12) is larger than zero. Hence, the count for \( F \) is decremented in \textsc{Overdelete} and \( F \) is added to \( N_D \). Then, in the same way as in the proof of the base case we have \( F \in D^s \), as required.

\begin{claim}
\textbf{The right-hand inclusion of property (14) holds.}
\end{claim}

\begin{proof}
Consider an arbitrary \( F \in R^s \). \( F \) can only be added to \( R^s \) in line 24, so we have \( F \in D^s \cap O^s \) and \( C_r[F] | d > 0 \); \( F \in D^s \cap O^s \) and \( C_r[F] | o > 0 \) holds by the induction assumption (13) ensures \( F \in I^*_o \cap O^s \); but then, properties (12), (10) and \( C_r[F] | o = \text{Occ}(F, \Pi^*_o[I^*_o | o \cap O^s]) \) jointly imply \( C_r[F] | d = \text{Occ}(F, \Pi^*_o[I^*_o \cap (D^s \setminus A^s), I^*_o \cup A^s]) \); now \( C_r[F] | o > 0 \) implies \( \text{Occ}(F, \Pi^*_o[I^*_o \cap (D^s \setminus A^s), I^*_o \cup A^s]) \subseteq \Pi^*_o[I^*_o | o \ cap A^s] \); due to stratification negative body atoms will only be matched against facts from lower strata, so we have \( \Pi^*_o[I^*_o | o \ cap A^s] = \Pi^*_o[I^*_o | o \ cap A^s] \); moreover, the left-hand inclusion of (13) implies \( I^*_o | o \ cap D^s \subseteq I^*_o | o \), which together with the induction assumption for property (16) implies \( I^*_o | o \ cap (D^s \setminus A^s) \subseteq (I^*_o | o \ cap D^s) \cup A^s \subseteq I^*_o | o \); furthermore, the induction assumption for property (16) ensures \( I^*_o | o \ cap (D^s \setminus A^s) \subseteq I^*_o | o \ cap A^s \); therefore we clearly have \( \Pi^*_o[I^*_o \ cap (D^s \setminus A^s), I^*_o \ cap A^s] \subseteq \Pi^*_o[I^*_o | o \ cap A^s] \). But then, \( \text{Occ}(F, \Pi^*_o[I^*_o \ cap (D^s \setminus A^s), I^*_o \ cap A^s]) > 0 \) implies \( \text{Occ}(F, \Pi^*_o[I^*_o | o \ cap A^s]) > 0 \), so we have \( F \in I^*_o | o \), as required.

\begin{claim}
\textbf{The left-hand inclusion of property (14) holds.}
\end{claim}

\begin{proof}
Consider arbitrary \( F \in O^s \cap D^s \cap \Pi^*_o[I^*_o \ cap (D^s \setminus A^s), I^*_o \ cap A^s] \), and we show that \( F \in R^s \) holds. \( F \in O^s \cap D^s \) implies \( C_r[F] | d = \text{Occ}(F, \Pi^*_o[I^*_o \ cap (D^s \setminus A^s), I^*_o \ cap A^s]) \) in the same way as in the proof of claim 7; but then, the fact that \( F \in \Pi^*_o[I^*_o \ cap (D^s \setminus A^s), I^*_o \ cap A^s] \) holds imply \( C_r[F] | d > 0 \), so line 24 of Algorithm 2 ensures that \( F \) is added to \( R^s \), as required.

\begin{claim}
\textbf{Property (15) holds.}
\end{claim}

\begin{proof}
Consider an arbitrary fact \( F \in I^*_o \) if \( F \not\in I^*_o \cap A^s \) holds, then the induction assumption ensures that we have \( F \not\in D^s \), if \( F \in I^*_o \) holds, then \( F \) is added to \( \Delta_A \) in line 46 of procedure \textsc{Insert} for stratum index \( s \), which ensures \( F \not\in (I^*_o \ cap D^s) \cup A^s \); but then, \( F \in I^*_o \) implies \( F \in D^s \), as required.

\begin{claim}
\textbf{The \( \subseteq \) direction of property (16) holds.}
\end{claim}

\begin{proof}
Consider an arbitrary fact \( F \in I^*_o \cap A^s \); if \( F \in I^*_o \ cap A^s \) holds, then the induction assumption ensures that we have \( F \in D^s \), if \( F \not\in I^*_o \ cap A^s \) holds, then \( F \) is added to \( \Delta_A \) in line 46 of procedure \textsc{Insert} for stratum index \( s \), which ensures \( F \not\in (I^*_o \ cap D^s) \cup A^s \); but then, \( F \in I^*_o \) implies \( F \in D^s \), as required.
Proof. We prove by induction on the construction of $A$ in INSERT that $(I_r\mid_n \setminus D^s) \cup A \subseteq I_r\mid_n$ holds. We first consider the base case. Set $A$ is equal to $A^{s-1}$ before the loop in lines 45–50; thus, property (16) is equivalent to $(I_r\mid_n \setminus D^s) \cup A^{s-1} \subseteq I_r\mid_n$; now $I_r\mid_n \setminus D^s \subseteq I_r\mid_n$ is implied by the left-hand inclusion of property (13), whereas $A^{s-1} \subseteq I_r\mid_n$ holds by the induction assumption.

For the inductive step, we assume that $(I_r\mid_n \setminus D^s) \cup A \subseteq I_r\mid_n$ holds, and we consider ways in which Algorithm 2 can add a fact $F$ to $A$. If $F \in E^s \cap O^s$, then $F \in I_r\mid_n$ clearly holds. Moreover, if $F \in E^r \setminus O^s$, then $F \in I_r\mid_n$ holds by (14). Otherwise, $F$ is derived in line 41, 43, or 49, so a rule $r \in \Pi^*$ and its instance $r^* = \text{inst}_r[(I_r\mid_n \setminus D^s) \cup A]$ exist such that $F \in L(r^*)$ holds. But then, definition (3) ensures $b^+(r^*) \subseteq (I_r\mid_n \setminus D^s) \cup A \subseteq I_r\mid_n$, and $b^+(r^*) \cap ((I_r\mid_n \setminus D^s) \cup A) = \emptyset$, which together with $b^-(r^*) \subseteq O^{s^*}$ and the induction assumption for (16) implies $b^-(r^*) \cap I_r\mid_n = b^-(r^*) \cap I_r\mid_n = \emptyset$. Consequently, we have $r^* \in \text{inst}_r[I_r\mid_n]$, so $F \in I_r\mid_n$ holds, as required. □

Claim 11. The $\supseteq$ direction of property (16) holds.

Proof. We show by induction that (27) holds for each $i$.

$$(I_r\mid_n \setminus D^s) \cup A^s \supseteq I_r\mid_n$$

(27)

For the base case, we have $I_r\mid_n = I_r\mid_n \setminus (E^s \cap O^s) = (I_r\mid_n \setminus D^s) \cup A^{s-1} \cup (E^s \cap O^s)$ by the induction assumption for (16). $I_r\mid_n \setminus D^s \subseteq I_r\mid_n \setminus D^s$ and $A^{s-1} \subseteq A^s$ clearly hold. Now consider arbitrary $F \in E^s \cap O^s$. If $F \in E^s$, then lines 41, 42, 46, and 48 ensure $F \in (I_r\mid_n \setminus D^s) \cup A^s$. If $F \in E^s \cap E^s = E^s \cap E^s$, then we clearly have $F \in I_r\mid_n$; but then, $C_r[F] = \text{Occ}(F, E^s \cup \Pi_r \cup \eta_r[I_r\mid_n])$ and property (11) imply $C_r[F] \geq 1$; thus, line 34 ensures $F \notin D^s$.

For the inductive step, assume that $I_r\mid_n$ satisfies (27) for $i > 0$, and consider arbitrary $F \in I_r\mid_n$. If $F \in I_r\mid_n$, then (27) holds by the induction assumption. Otherwise, by definition a rule $r$ and its instance $r^* = \text{inst}_r[I_r\mid_n]$ exist where $h(r^*) = F$.

Definition (3) and the induction assumption for (27) ensure $b^+(r^*) \subseteq I_r\mid_n \setminus (D^s) \cup A^s$. Moreover, definition (3) also ensures $b^-(r^*) \cap I_r\mid_n = \emptyset$, which together with the induction assumption that property (16) holds for $s-1$ and the definition of $I_r\mid_n$, implies $b^-(r^*) \cap ((I_r\mid_n \setminus D^s) \cup A^{s-1}) = \emptyset$; but then, $b^-(r^*) \subseteq O^{s^*}$ implies $b^-(r^*) \cap ((I_r\mid_n \setminus D^s) \cup A^{s-1}) = \emptyset$. Now we consider the following cases.

- $b^+(r^*) \cap (A^s \setminus A^{s-1}) \neq \emptyset$. Facts in $A^s \setminus A^{s-1}$ are added to $A$ via lines 46 and 48, so there is a point in the execution of the algorithm where $b^+(r^*) \cap (A^s \setminus A^{s-1}) \cap A^s \neq \emptyset$ holds in line 49 for the last time for $A^s$. Since $A^s \subseteq A^s$ holds at this point, we clearly have $b^+(r^*) \subseteq (I_r\mid_n \setminus D^s) \cup A^s$; moreover, $A \subseteq A^s$ and $b^-(r^*) \cap ((I_r\mid_n \setminus D^s) \cup A^s) = \emptyset$ ensure $b^-(r^*) \cap ((I_r\mid_n \setminus D^s) \cup A^s) = \emptyset$. But then, $r^* \in \text{inst}_r[(I_r\mid_n \setminus D^s) \cup A^s]$ holds; $F = h(r^*)$ will be added to $A^s$ in line 50; and lines 46 and 48 ensure $F \in (I_r\mid_n \setminus D^s) \cup A^s$.

- $b^+(r^*) \cap (A^s \setminus A^{s-1}) = \emptyset$, so $b^+(r^*) \subseteq (I_r\mid_n \setminus D^s) \cup A^{s-1}$ holds. We have the following two possibilities.

  - $b^+(r^*) \cap (A^s \setminus A^{s-1}) = \emptyset$, so $b^+(r^*) \subseteq (I_r\mid_n \setminus D^s) \cup A^{s-1}$ holds. But then, by the definition (3) of rule matching, we clearly have $r^* \in \text{inst}_r[(I_r\mid_n \setminus D^s) \cup A^{s-1}]$. But then, lines 41–44 ensure that $F = h(r^*)$ is added to $A^s$; and lines 46 and 48 ensure $F \in (I_r\mid_n \setminus D^s) \cup A^s$.

Claim 12. The following two properties hold.

$$
\begin{align*}
\Pi^s_{nr}[\Pi^s_{nr}[(I_r\mid_n \setminus D^s) \cup A^s]] &= \Pi^s_{nr}[\Pi^s_{nr}[(I_r\mid_n \setminus D^s) \cup A^s \setminus A^{s-1}]], \\
\Pi^s_{nr}[\Pi^s_{nr}[(I_r\mid_n \setminus D^s) \cup A^s \setminus D^{s-1} \setminus A^{s-1}]] &= \Pi^s_{nr}[\Pi^s_{nr}[(I_r\mid_n \setminus D^s) \cup A^s \setminus D^{s-1} \setminus A^{s-1}]]
\end{align*}
$$

(28)

(29)

Proof. By the definition of $\Pi^s_{nr}$ it is sufficient to show that for each rule $r \in \Pi^s$, properties (30) and (31) hold.

$$
\begin{align*}
\text{inst}_r[I_r\mid_n \setminus (D^s \setminus A^{s-1})] \cap \text{inst}_r[I_r\mid_n \setminus (D^s \setminus A^{s-1})] &= \emptyset, \\
\text{inst}_r[I_r\mid_n \setminus (D^s \setminus A^{s-1})] \cap \text{inst}_r[I_r\mid_n \setminus (D^s \setminus A^{s-1})] &= \emptyset
\end{align*}
$$

(30)

(31)

To prove (30), consider an arbitrary rule instance $r^* \in \text{inst}_r[I_r\mid_n \setminus (D^s \setminus A^{s-1})]$. By definition (3) we have $b^+(r^*) \cap (A^s \setminus A^{s-1}) \neq \emptyset$ or $b^-(r^*) \cap (D^s \setminus A^{s-1}) \neq \emptyset$; now we examine these two cases separately.
For the first case, let $F$ be an arbitrary fact in $b^+(r') \cap (A^s \setminus D^{s-1})$. Now if $F \in A^{s-1} \setminus D^{s-1}$ holds, then the induction assumption for (15) ensures $F \not\in I^*_{\bigcup\{I\}}$, which in turn implies $F \not\in I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})$; if $F \in A^s \setminus A^{s-1}$ holds, then in the same way as in the proof of claim 9 we have $F \not\in (I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1})$; either way, we have $b^+(r') \not\in I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})$, so $r' \not\in \text{inst}_{I^*_{\bigcup\{I\}}}((D^s \setminus A^{s-1}) \setminus (D^s \setminus A^{s-1})).$

For the second case, $b^-(r') \cap (D^{s-1} \setminus A^{s-1}) \neq \emptyset$ and the induction assumption for property (13) imply $b^-(r') \cap (I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \neq \emptyset$; which clearly implies $b^-(r') \cap (I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \neq \emptyset$; thus, by definition (3) we have $r' \not\in \text{inst}_{I^*_{\bigcup\{I\}}}((D^s \setminus A^{s-1}) \setminus (D^s \setminus A^{s-1}));$

this completes our proof for (30).

Next we prove the 2 direction of property (31). Consider an arbitrary rule instance $r'$ contained in the right-hand side of (31); if $r' \in \text{inst}_{I^*_{\bigcup\{I\}}}((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1})), then by definition (3) we clearly have $r' \in \text{inst}_{I^*_{\bigcup\{I\}}}((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1}));$

Moreover, $b^-(r') \cap (I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \neq \emptyset$; which clearly implies $b^-(r') \cap (I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \neq \emptyset$; thus, by definition (3) we have $r' \not\in \text{inst}_{I^*_{\bigcup\{I\}}}((D^s \setminus A^{s-1}) \setminus (D^s \setminus A^{s-1}));$

this completes our proof for (31).

Claim 13. Property (17) holds.

Proof. Due to claim 12 it is now sufficient to show that for each $F \in ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \cap I^*_{\bigcup\{I\}} \cap O^s$, the following property holds.

$$C_{\Pi} |F|_{\alpha} - C_{\Pi} |F|_{\beta} = \text{Occ}(F, (E^+ \cap O^s) \cap \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1}))$$

(32)

$\Pi_{\alpha}$ contains only nonrecursive rules, so it is sufficient to prove

$$C_{\Pi} |F|_{\alpha} - C_{\Pi} |F|_{\beta} = \text{Occ}(F, (E^+ \cap O^s) \cap \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1})),$$

(33)

which is ensured by line 41 and line 42 of the algorithm.

Claim 14. Property (18) holds.

Proof. $F \not\in I^*_{\bigcup\{I\}} \cap O^s$ ensures $C_{\Pi} |F|_{\alpha} = C_{\Pi} |F|_{\beta} = 0$. Moreover, $F \not\in \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1}))) \setminus (D^s \setminus A^{s-1})),$

then by property (28) and $F \not\in (E_{\alpha} \cap E^-) \cap O^s$ we clearly have $\text{Occ}(F, ((E_{\alpha} \cap E^-) \cap E^+) \cap \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s))) = 0$; moreover, line 41 ensures that the nonrecursive count for $F$ is not incremented in this case, so the left-hand side of (18) equals zero as well. Otherwise, each occurrence of $F$ in the multisets $(E^+ \cap O^s) \cap \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1}))$ results in incrementing the nonrecursive count of $F$ by one; together with $F \not\in (E_{\alpha} \cap E^-) \cap O^s$ and $F \not\in \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1})), this ensures the correctness of the property.

Claim 15. Property (19) holds.

Proof. Line 46 and line 48 ensure that $\Delta_A$ used in line 49 is different between iterations of the loop in lines 45–50, so the rl instances considered in line 49 are different between iterations. All these rule instances are in $\bigcup_{I \in \Pi} \text{inst}_{\alpha} (I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s))$, which is equal to $\bigcup_{I \in \Pi} \text{inst}_{\alpha} (I^*_{\bigcup\{I\}})$ by property (16). Therefore, the loop will terminate. Now let $T$ be the total number of iterations; moreover, for each $1 \leq i \leq T$, let $A_i^t$ be the value of $A$ at the beginning of the $i$th iteration of the loop, and let $C_{\Pi} |F|_i$ be the value of $C_{\Pi} |F|$ for each $F \in ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \cap I^*_{\bigcup\{I\}} \cap O^s$ at the same time point. We next prove by induction on $i$ that (34) holds for $1 \leq i \leq T$; then (34) for $i = T$ and property (29) ensure the correctness of the claim.

$$C_{\Pi} |F|_i - C_{\Pi} |F|_i = \text{Occ}(F, \Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \setminus (D^s \setminus A^{s-1})) \setminus (D^s \setminus A^{s-1}))$$

(34)

For the base case, we have $A_1^t = A^{s-1}$. Consider arbitrary $F \in ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \cap I^*_{\bigcup\{I\}} \cap O^s$. Lines 43 and 44 ensure that each occurrence of $F$ in $\Pi_{\alpha} ((I^*_{\bigcup\{I\}} \setminus (D^s \setminus A^s)) \setminus (D^s \setminus A^{s-1}))$ results in incrementing the corresponding recursive
Property count by one. But then, stratification ensures $\Pi_r^e \left((I^e|_o \setminus D^e) \cup A^{s-1} : A^{s-1} \setminus D^e, D^e \setminus A^{s-1}\right] = \Pi_r^e \left((I^e|_o \setminus D^e) \cup A^{s-1} : A^{s-1} \setminus D^e, D^e \setminus A^{s-1}\right]$, so (34) holds for $i = 1$, as required.

For the inductive step, assume that (34) holds for $i - 1$ where $1 < i \leq T$, and consider arbitrary $F \in ((I^e|_o \setminus D^e) \cup A^e) \cap I^e|_o \cap O^e$. Lines 46, 48, and 49 jointly imply (35).

$$C_r[F]_{|_o} - C_r[F]_{|_o}^{-1} = \text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right])$$

We now show that the following holds.

$$\text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right]) + \text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right]) = \text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right])$$

To this end, it is sufficient to show that for each $r \in \Pi_r^e$, property (37) holds.

$$\text{inst}_{r\cap \text{Occ}} \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right) \cup \text{inst}_{r\setminus \text{Occ}} \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right)$$

(37) holds as well, consider arbitrary $r \in \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right)$. If $b^+(r') \cap (A^e \setminus A^{e-1}_r) \neq \emptyset$, then we clearly have $r' \in \text{inst}_{\text{Occ}} \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus A^{e-1}_r \right)$. If $b^+(r') \cap (A^e \setminus A^{e-1}_r) = \emptyset$, then definition (3) ensures that we have $b^+(r') \subseteq \left( (I^e|_o \setminus D^e) \cup A^e \setminus A^{e-1}_r \right) = (I^e|_o \setminus D^e) \cup A^{e-1}_r$. There are two possibilities here: if $b^+(r') \cap (A^e \setminus D^{e-1}) \neq \emptyset$, then clearly $b^+(r') \cap (A^e \setminus A^{e-1}_r) = \emptyset$ holds as well; either way, we have $F \in \text{inst}_{\text{Occ}} \left( (I^e|_o \setminus D^e) \cup A^e \setminus A^{e-1}_r \right)$. Therefore, the $\supseteq$ direction of property (37) holds. But then, property (36) holds, which together with (35) and the induction assumption for (34) ensures that (34) holds for $i$ as well.

**Claim 16. Property (20) holds.**

**Proof.** $F \notin I^e|_o$ implies $C_r[F]_{|_o} = 0$, so we have $C_r[F]_{|_o} = \text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^e : A^e \setminus D^{s-1} \cup A^{s-1}_r \right])$ in the same way as in the proof for the previous claim. Moreover, $F \notin I^e|_o$ ensures $\text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^{s-1}_r \right]) = 0$. Therefore, by property (29) we have $C_r[F]_{|_o} = \text{Occ}(F, \Pi_r^e \left( (I^e|_o \setminus D^e) \cup A^{s-1}_r \right])$, as required. 

$$\square$$