Abstract

We look into the problem of unifying multisets containing (first-order) terms and multiple multiset variables. The variables are labelled, meaning that a unifier that places a term in a multiset variable \( M_i \) is different from another that places a term in a multiset variable \( M_j \), for \( i \neq j \). We describe a sound, complete, and terminating algorithm for computing the set of all possible unifiers, and analyse its complexity. We also prove an input pre-processing step that avoids the computation of less general unifiers.

1 Introduction

Multiset is an important data-structure that is used to specify various object systems. Our motivation stems mostly from proof theory, where logical entailment is encoded as sequents \( \Gamma \vdash \Delta \), where both \( \Gamma \) and \( \Delta \) are typically considered as multisets. When reasoning about such objects, one might need to use an implementation of sets/multisets based on lists, since most reasoning tools (i.e., logical frameworks, proof assistants, and logic programming languages) do not have built-in support for these data structures [2, 3, 6, 7]. Adding this kind of support requires, among other things, a unification algorithm.

Multiset unification was studied in [1, 4], where the authors propose solutions for the problem of unifying multisets with at most one multiset variable. We extend those results for multisets with multiple multiset variables. In our setting, each multiset variable is labelled, meaning that assigning a term to either a multiset \( M_i \) or \( M_j \), where \( i \neq j \), should be considered different solutions. We describe a terminating algorithm and analyse its complexity. Moreover, we prove that a simple modification of our algorithm avoids the computation of less general unifiers.

1.1 Preliminaries

A multiset \( \mathcal{M} \) with multiple labelled multiset variables is denoted by \( \{ | t_1, \ldots, t_n | M_1, \ldots, M_k | \} \). Each \( t_i \) is a term ranging over a first-order language \( \mathcal{L} = (\Sigma, V) \), where \( \Sigma \) is a set of constants.
and function symbols, and \(\mathcal{V}\) is a denumerable set of term variables. Each \(M_i\) is a multiset variable ranging over a denumerable set of multiset variables. When \(n\) and \(k\) are not relevant, we abbreviate \(t_1, ..., t_n\) as \(T\) and \(M_1, ..., M_k\) as \(M\). When \(k = 0\), we write the multiset as \(\{t_1, ..., t_n\}\). Henceforth, we refer to multisets with multiple labelled multiset variables as mmsets for brevity.

**Definition 1** (Substitution). An mmset substitution \(\sigma\) is a finite mapping of term variables to terms, and of multiset variables to mmsets. The application of a substitution \(\sigma\) to an mmset \(\{t_1, ..., t_n\}|M_1, ..., M_k\|\) is defined as:

\[
\{t_1, ..., t_n| M_1, ..., M_k\}|\sigma = \{t_1| \sigma, ..., t_n| \sigma\} \uplus M_1| \sigma \uplus ... \uplus M_k| \sigma
\]

where each \(t_i| \sigma\) is the usual first-order substitution and \(\uplus\) is left-associative and defined as:

\[
\{t_1, ..., t_n| M_1, ..., M_k\|\uplus \{s_1, ..., s_m|N_1, ..., N_l\} = \{t_1, ..., t_n, s_1, ..., s_m| M_1, ..., M_k, N_1, ..., N_l\}\]

**Definition 2** (Equality). Mmsets \(M = \{t_1, ..., t_n| M_1, ..., M_k\}\) and \(N = \{s_1, ..., s_m| N_1, ..., N_l\}\) are considered equal modulo a constraint theory \(T\), written \(M =_{T} N\) iff: \(n = m\) and \(t_1, ..., t_n\) is a permutation of \(s_1, ..., s_m\); and \(T \vdash M_1 \uplus ... \uplus M_k \equiv N_1 \uplus ... \uplus N_l\).

## 2 Mmsets Unification

The mmset unification problem of mmsets \(M_1\) and \(M_2\) consists of finding a substitution \(\sigma\) and constraint theory \(T_\sigma\) such that \(M_1| \sigma =_{T_\sigma} M_2| \sigma\). The theory \(T_\sigma\) consists of an equality over unions of multiset variables, and it is computed a posteriori for each unifier \(\sigma\).

### 2.1 Algorithm

In what follows, we use \(\sigma\) to denote a single substitution, \(\Sigma\)s to denote sets of substitutions, \(\times\) for the Cartesian product of two sets (or lists), and \(\setminus\) for multiset difference. The pseudo code for all algorithms are listed in Appendix A, and an implementation in SML can be found at https://github.com/meta-logic/mmset-unif.

The main function for mmset unification is implemented by Algorithm 1. In the most general case (lines 11 to 17), the unifiers of \(\{T|\overline{M}\}\) and \(\{\overline{\pi}\}|\overline{N}\) are computed by choosing a subset of terms (of the same size) from \(T\) and \(\pi\) to be unified, and distributing the rest among the multiset variables \(\overline{M}\) and \(\overline{N}\). The number of terms chosen to be unified can vary from 0 to the minimum length of \(T\) and \(\pi\). Two other cases are considered separately for efficiency purposes. The first one is when there are no multiset variables (line 1). Here a unification is only possible if \(|T| = |\overline{\pi}|\). The second case is when one of the mmsets does not have multiset variables (lines 4 and 7). If \(\overline{M}\) is empty, then all terms in \(\overline{\pi}\) must be unified with a term from \(T\). The remaining terms in \(\overline{\pi}\) can be allocated in \(\overline{N}\).

Function \texttt{ unify}(Algorithm 2) chooses \(c\) terms from the multisets \(T\) and \(\pi\) to be unified, and distributes the rest of the terms among the multiset variables. The function \texttt{choose}(\(F_i\), \(c\)) returns a set of tuples \((F_i, c_i)\), where \(F_i\) is the multiset with the chosen \(c\) elements (thus \(|F_i| = c\)), and \(F_i = F_i \setminus F_i\). Unifiers for the chosen terms are computed by \texttt{ unify terms} and stored in \(\Sigma T\). Substitutions for each context variable, containing the remaining terms, are computed by \texttt{ unify distribute} and stored in \(\Sigma M\). The final set of unifiers consists of the composition \(\sigma M| \sigma\) for each \((\sigma M, |\sigma|) \in \Sigma M \times \Sigma\). Note that, since the image of \(\sigma M\) may contain terms, the composition needs to be in this order.
Function \texttt{unify\_terms} (Algorithm 3) finds all unifiers of two multisets of terms (without multiset variables) of equal length. This is done by testing all possible pairings of the two multisets, obtained by pairing some order of the first multiset with all possible permutations of the second one. For each pairing, the function \texttt{unify\_lists} computes the most general unifier.

Function \texttt{unify\_distribute} (Algorithm 4) computes unifiers for the mmsets \( \{t|\overline{M}\} \) and \( \{\overline{s}|\overline{N}\} \) considering that all \( t \) occurs in \( \overline{N} \) and all \( \overline{s} \) occurs in \( \overline{M} \). Let \( \Sigma_N \) denote the substitutions that distribute \( t \) into \( \overline{N} \), and \( \Sigma_M \) the substitutions that distribute \( \overline{s} \) into \( \overline{M} \). The resulting substitutions are \( \sigma_M \cup \sigma_N \) for each \( (\sigma_M, \sigma_N) \in \Sigma_M \times \Sigma_N \). A simple union can be used in the case, as the image of \( \sigma_M \) is disjoint from the domain of \( \sigma_N \) (see below).

Function \texttt{distribute} (Algorithm 5) is used by \texttt{unify\_distribute} and that is where the aforementioned \( \Sigma_N \) and \( \Sigma_M \) are computed. It computes substitutions for the multiset variables \( N_1, ..., N_l \) such that all terms \( t_1, ..., t_n \) occur in one of the multisets. This is done by calculating all ordered \( l \)-partitions of the multiset \( \{t_1, ..., t_n\} \). For example, the ordered 2-partitions of the multiset \( \{a, b, c\} \) are:

\[
\begin{align*}
\{\{a, b\}, \{c\}\} & \quad \{\{a\}, \{b, c\}\} & \quad \{\{a\}, \{b\}, \{c\}\} \\
\{\{\}, \{a, b, c\}\} & \quad \{\{a\}, \{b\}, \{c\}\} & \quad \{\{a\}, \{b\}, \{c\}\}
\end{align*}
\]

Each computed substitution corresponds to an \( l \)-ordered partition. If there are no terms \( (n = 0) \), then there is only the trivial partition of \( l \) empty multisets. In this case, the algorithm returns a list with one substitution, which maps every multiset variable \( N_i \) to the mmset with no terms. If there are no multiset variables \( (l = 0) \), then there are no partitions, and thus no possible substitutions. The exceptional case is when there are no terms nor multiset variables \( (l = n = 0) \). In this case, the solution is the set containing only the empty substitution \( \{\}\).

The last parameter of \texttt{distribute} indicates whether the multiset variables should contain exactly the terms \( t_1, ..., t_n \). If set to true, then there is no more space for other terms, and \( N_i \) is mapped to an mmset with the appropriate terms and no multiset variables. Otherwise it is mapped to an mmset with a set of terms and a fresh multiset variable. If there are no terms to place in the multiset variable, it is mapped to itself (to avoid unnecessary renamings). This is needed to compute the constraint theory, after which such identity substitutions can be eliminated.

Constraint theory For a unifier \( \sigma \), the constraint theory \( T_\sigma \) is defined as:

\[
\bigcup \{M'_i \mid M_i \mapsto \{ts|M'_i\} \in \overline{\sigma} \} \equiv \bigcup \{N'_i \mid N_i \mapsto \{ts|N'_i\} \in \overline{\sigma} \}
\]

Soundness and completeness of the algorithm are straightforward, since it exhaustively checks all possibilities for unifying multisets.

\textbf{Theorem 1.} Soundness If \( \text{unify}(M, N) \mapsto \{\sigma_1, ..., \sigma_n\} \) then \( \forall \sigma_i. M \sigma_i = T_\sigma \times N \sigma_i \)

\textbf{Theorem 2.} Completeness If \( \exists \sigma. M \sigma = T_\sigma \times N \sigma \) then \( \text{unify}(M, N) \mapsto \{\sigma_1, ..., \sigma_n\} \) and \( \exists \sigma_i \) such that \( \sigma = \sigma_i \sigma' \).

Note that the use of a substitution \( \sigma' \) is needed even if the set of computed unifiers is not the minimal one.
2.2 Complexity

The most expensive part of the unification algorithm is the one between lines 11 and 17 in Algorithm 1, so we concentrate our complexity analysis to that case. For each $i$ from 0 to the minimum number of terms, unify$_{LC}$ is called. This function has two nested loops over the sets $T_c$ and $S_c$ (Alg. 2, lines 4, 5), which contain all possible ways of choosing $i$ elements from $n$ and $m$, respectively. Thus $|T_c| = \binom{n}{i}$ and $|S_c| = \binom{m}{i}$. In the inner part of the loops, unify$_{terms}$ is called, which finds all possible unifiers for two multisets of size $i$. Since all possible pairings of elements must be tried, and for each order of $i^2$, the function (Alg. 3) has complexity $i^2!$. The function unify$_{distribute}$ (Alg. 4) computes all possible ways of partitioning $n-i$ elements into $l$ parts, and $m-i$ elements into $k$ parts, and returns the Cartesian product of these sets. Therefore, its complexity is $l^{m-i} k^{m-i}$.

Putting those together, we get to the cost for the unification of mmsets $\{t_1, ..., t_n|M_1, ..., M_k\}$ and $\{s_1, ..., s_m|N_1, ..., N_l\}$:

$$\sum_{i=0}^{\min(n, m)} \binom{n}{i} \binom{m}{i} i^2! l^{m-i} k^{m-i}$$

After some arithmetic manipulation, we can conclude that, on the worst case, unify runs in $O(n! m! l^n k^m)$. For the special case where the multisets have only one multiset variable: $l = k = 1$, and the unification algorithm runs in $O(n! m!)$.

2.3 Removing Less General Unifiers

The algorithm described in Section 2.1 does not compute the set of minimal unifiers. For example, given multiset $\{a, a|M\}$ and $\{a|N\}$, unify computes three unifiers with constraint: $\{N \mapsto \{a|N'\}\}$, where $M \equiv N'$, twice (once for each occurrence of $a$), and $\{M \mapsto \{a|M'\}; N \mapsto \{a|N'\}\}$, where $M' \equiv N'$. These are the same unifiers obtained by the non-deterministic algorithm from [5].

In order to reduce the number of less general unifiers, we can remove every pair of equal terms $t_i$ and $s_j$ from the mmsets (i.e., $t_i$ and $s_j$ unify with the empty substitution). The rationale behind this is that, every other unifier that is obtained by unifying these terms with something else, or placing them in a multiset variable, can be recovered from the set of unifiers obtained when this pair is not in the mmset.

We start by showing that it is safe to eliminate pairs of equal terms from the problem of unifying multisets without multiset variables.

**Theorem 3.** Let $\mathcal{T}$ and $\mathcal{S}$ be two multisets of terms such that $t_a \in \mathcal{T}$ and $s_b \in \mathcal{S}$ are equal, for some $a$ and $b$. Let $\Sigma_{all} = \text{unify}_{\text{terms}}(\mathcal{T}, \mathcal{S})$, and $\Sigma = \text{unify}_{\text{terms}}(\mathcal{T} \setminus \{t_a\}, \mathcal{S} \setminus \{s_b\})$. Then for every $\sigma \in \Sigma_{all}$, there exists $\mu \in \Sigma$ s.t. $\sigma = \mu \sigma'$ for some substitution $\sigma'$.

The proof for this theorem can be found in Appendix B. The overall idea is as follows. $\sigma$ was obtained by some pairing of terms in $\mathcal{T}$ and $\mathcal{S}$. We choose $\mu$ as the unifier that used a pairing that is as close as possible as the one used for $\sigma$. Those pairings differ only for the terms involving $t_a$ and $s_b$. Suppose $t_a$ is paired with $s_x$ and $s_b$ is paired with $t_y$. Using the most general unifiers of $t_y$ and $s_z$, we can conclude the existence of $\sigma'$ such that $\sigma = \mu \sigma'$.

**Theorem 4.** Let $\{t|M\}$ and $\{s|N\}$ be two mmsets such that $t_a \in \mathcal{T}$ is equal to $s_b \in \mathcal{S}$ for some $a$ and $b$. Moreover, let $\Sigma_{all} = \text{unify}(\{t|M\}, \{s|N\})$, and $\Sigma = \text{unify}(\{t \setminus \{t_a\}|M\}, \{s \setminus \{s_b\}|N\})$. Then for every $\sigma \in \Sigma_{all}$ there exists $\mu \in \Sigma$ such that $\sigma = \mu \sigma'$ for some $\sigma'$.
The proof for this theorem can be found in Appendix B. We proceed by a case analysis on whether $t_a$ and $s_b$ were chosen to be unified, or to be placed in a multiset variable. There are four cases. The case in which both are chosen to be unified is solved using Theorem 3. For the case in which both are placed in a multiset variable, we can construct $\sigma'$. The other two (dual) cases are the more involved ones. They use a combination of the two strategies of the first cases.

This modification is implemented in the algorithm available online, and extensive testing has shown that all less general unifiers are eliminated. In particular, only the unifier $\{N \mapsto \{a|N'\}\}$, where $M \equiv N'$ is computed for mmsets $\{a,a|M\}$ and $\{a|N\}$.

3 Conclusion

We have developed a sound and complete algorithm for finding unifiers of multisets with multiple multiset variables. The algorithm is deterministic and terminating. It is implemented in SML, and we also provide the pseudo code for reproducibility. The same algorithm can be used for the particular case where there is only one multiset variable.

The complexity of the unification procedure is analysed, and its cost is high. This is inherent to the problem, since it is of combinatorial nature. It may be possible to improve this result by using the right data-structures and heuristics, but for our purposes, since the numbers are quite small, it runs fast enough.

We have also tried to eliminate all sources of redundancy, so that the set of computed unifiers is as close as possible to the minimal one. In particular, we have shown that a simple pre-processing of the input problem will produce fewer unifiers, and all those that are no longer produced can be recovered. We conjecture that this optimization leads to the computation of the minimal set of unifiers, but we leave this investigation as future work.

References

A Algorithms

Algorithm 1 unify(\{t_1, ..., t_n|M_1, ..., M_k\}, \{s_1, ..., s_m|N_1, ..., N_l\})
1: if \(k = 0 \land l = 0\) then
2: if \(n = m\) then return unify_terms([t_1, ..., t_n], [s_1, ..., s_m])
3: else return []
4: else if \(k = 0\) then
5: if \(m \leq n\) then return unify_c(m, \{t_1, ..., t_n|M_1, ..., M_k\}, \{s_1, ..., s_m|N_1, ..., N_l\})
6: else return []
7: else if \(l = 0\) then
8: if \(n \leq m\) then return unify_c(n, \{t_1, ..., t_n|M_1, ..., M_k\}, \{s_1, ..., s_m|N_1, ..., N_l\})
9: else return []
10: else
11: \(c \leftarrow \min(n, m)\)
12: \(\Sigma \leftarrow []\)
13: for \(i = 0\) to \(c\) do
14: \(\Sigma' \leftarrow \text{unify}_c(i, \{t_1, ..., t_n|M_1, ..., M_k\}, \{s_1, ..., s_m|N_1, ..., N_l\})\)
15: \(\Sigma \leftarrow \Sigma \cup \Sigma'\)
16: end for
17: return \(\Sigma\)
18: end if

Algorithm 2 unify_c(c, \{t_1, ..., t_n|M_1, ..., M_k\}, \{s_1, ..., s_m|N_1, ..., N_l\})
1: \(\Sigma \leftarrow []\)
2: \(T_c \leftarrow \text{choose}(\{t_1, ..., t_n\}, c)\)
3: \(S_c \leftarrow \text{choose}(\{s_1, ..., s_m\}, c)\)
4: for (\{t'_1, ..., t'_n\}, \{t''_1, ..., t''_n\}) \(\in T_c\) do
5: for (\{s'_1, ..., s'_m\}, \{s''_1, ..., s''_m\}) \(\in S_c\) do
6: \(\Sigma' \leftarrow \text{unify_terms}(\{t'_1, ..., t'_n\}, [s'_1, ..., s'_m])\)
7: if \(\Sigma' \neq []\) then
8: \(\Sigma_M \leftarrow \text{unify_distribute}(\{t'_1, ..., t'_n\}, \{M_1, ..., M_k\}, \{s''_1, ..., s''_m\}, \{N_1, ..., N_l\})\)
9: \(\Sigma' \leftarrow \text{map}(\lambda(\sigma_t, \sigma_M, \sigma_M \sigma_t) | that is the result of unifying the same permutations \(P_t\) and \(P_s\), and \(t_y\) with \(s_x\). We show how \(\sigma_i\) can be reconstructed from \(\mu_j\). Since the order in which terms are unified does not matter, we assume that \(\sigma_i\) and \(\mu_j\) are obtained as follows:

Proof for Theorem 3. We know that \(\Sigma_{all}\) contains at most \(n!\) unifiers, one for each way of pairing elements of \(\bar{t}\) with elements of \(\bar{s}\). Analogously, \(\Sigma\) contains at most \((n - 1)!\) unifiers. Let: \(\Sigma_{all} = \{\sigma_1, ..., \sigma_n\}\) and \(\Sigma = \{\mu_1, ..., \mu_{(n-1)!}\}\). Then each \(\sigma_i\) can be obtained from some \(\mu_j\).

If \(\sigma_i\) is a unifier resulting from pairing \(t_a\) with \(s_b\), then there exists \(\mu_j = \sigma_i\) and we are done.

Let \(\sigma_i\) be a unifier resulting from pairing \(t_a\) with some \(s_x\), \(s_b\) with some \(t_y\), and some permutation \(P_t\) of \(\{t_a, t_y\}\) with some permutation \(P_s\) of \(\{s_b, s_x\}\). There exists a unifier \(\mu_j \in \Sigma\) that is the result of unifying the same permutations \(P_t\) and \(P_s\), and \(t_y\) with \(s_x\). We show how \(\sigma_i\) can be reconstructed from \(\mu_j\). Since the order in which terms are unified does not matter, we assume that \(\sigma_i\) and \(\mu_j\) are obtained as follows:
### Algorithm 3 unify_terms([t₁, ..., tₙ], [s₁, ..., sₙ])

1. \( \Sigma \leftarrow [] \)
2. \( P_s \leftarrow \text{permutations}([s₁, ..., sₙ]) \)
3. \( P \leftarrow [[t₁, ..., tₙ]] \times P_s \)
4. for \((T, S) \in P\) do
5. \( \sigma \leftarrow \text{unify_lists}(T, S) \)
6. if \( \sigma \neq \text{None} \) then \( \Sigma \leftarrow \{ \sigma \} \cup \Sigma \)
7. end for

### Algorithm 4 unify_distribute(([t₁, ..., tₙ], [M₁, ..., Mₖ]), ([s₁, ..., sₘ], [N₁, ..., Nᵢ]))

1. \( \Sigma_N \leftarrow \text{distribute}([t₁, ..., tₙ], [N₁, ..., Nᵢ], k = 0) \) \{List of substitutions for \( Nᵢ \} \)
2. \( \Sigma_M \leftarrow \text{distribute}([s₁, ..., sₘ], [M₁, ..., Mₖ], l = 0) \) \{List of substitutions for \( Mᵢ \} \)
3. \( \Sigma \leftarrow \text{map}(\lambda(\sigma_M, \sigma_N).\sigma_M \cup \sigma_N)(\Sigma_M \times \Sigma_N) \)
4. return \( \Sigma \)

### Algorithm 5 distribute([t₁, ..., tₙ], [M₁, ..., Mₖ], exact)

1. if \( n = 0 \land k = 0 \) then
2. return \([\{\} ]\)
3. end if
4. \( \Sigma \leftarrow [] \)
5. \( P_t \leftarrow \text{ordered_partitions}([t₁, ..., tₙ], k) \)
6. for \( p \in P_t \) do
7. \( \sigma \leftarrow \{\} \)
8. for \( i = 1 \) to \( k \) do
9. \( ts \leftarrow p[i] \)
10. if \( \text{exact} \) then \( \sigma \leftarrow \sigma \{ Mᵢ \mapsto \{ts|·\} \} \)
11. if \( \neg\text{exact} \land ts = \emptyset \) then \( \sigma \leftarrow \sigma \{ Mᵢ \mapsto \{·|Mᵢ\} \} \)
12. if \( \neg\text{exact} \land ts \neq \emptyset \) then \( \sigma \leftarrow \sigma \{ Mᵢ \mapsto \{ts|Mᵢ\} \} \)
13. end for
14. \( \Sigma \leftarrow \{ \sigma \} \cup \Sigma \)
15. end for
16. return \( \Sigma \)

1. Computation of \( \sigma_i \):
   (a) \( \text{mg}u \sigma_{ax} \) of \( t_a \) and \( s_x \)
   (b) \( \text{mg}u \sigma_{by} \) of \( t_y \sigma_{ax} \) and \( s_b \sigma_{ax} \)
   (c) \( \text{mg}u \sigma_{P_a} \) of \( P_a \sigma_{ax} \sigma_{by} \) and \( P_a \sigma_{ax} \sigma_{by} \)

2. Computation of \( \mu_j \):
   (a) \( \text{mg}u \sigma_{xy} \) of \( t_y \) and \( s_x \)
   (b) \( \text{mg}u \sigma_{P_y} \) of \( P_y \sigma_{xy} \) and \( P_y \sigma_{xy} \)

Therefore \( \sigma_i = \sigma_{ax} \sigma_{by} \sigma_{P_y} \) and \( \mu_j = \sigma_{xy} \sigma_{P_y} \). We know that:

\[
\begin{align*}
    t_a \sigma_{ax} &= s_x \sigma_{ax} & \text{from 1a} \\
    t_y \sigma_{ax} \sigma_{by} &= s_b \sigma_{ax} \sigma_{by} & \text{from 1b} \\
    t_y \sigma_{ax} \sigma_{by} &= t_a \sigma_{ax} \sigma_{by} & \text{because } t_a = s_b \\
    t_y \sigma_{ax} \sigma_{by} &= s_x \sigma_{ax} \sigma_{by} & \text{from 3 and 1}
\end{align*}
\]

Thus, \( \sigma_{ax} \sigma_{by} \) is a unifier of \( t_y \) and \( s_x \). But from 2a we have that \( \sigma_{xy} \) is the most general
unifiers of these terms, which means that there exists a $\sigma'$ such that

$$\sigma_{ax}\sigma_{by} = \sigma_{xy}\sigma'$$

From 5 and 1c, we know that $P_{t}\sigma_{xy}\sigma' P_{i} = P_{s}\sigma_{xy}\sigma' P_{i}$, meaning that $\sigma' P_{i}$ is a unifier of $P_{t}\sigma_{xy}$ and $P_{s}\sigma_{xy}$. But from 2b, $\sigma_{xy}$ is the most general unifier of these two lists, therefore, there exists $\sigma''$ such that

$$\sigma' P_{i} = \sigma_{xy}\sigma''$$

Using 5, 6, and associativity of substitution composition:

$$\sigma_{t} = \sigma_{ax}\sigma_{by}\sigma_{i} = \sigma_{xy}\sigma_{i}\sigma'' = \mu_{j}\sigma''$$

**Proof for Theorem 4.** We case on how $t_{a}$ and $s_{b}$ were used to compute $\sigma$. Let $\overrightarrow{t_{c}}$ and $\overrightarrow{s_{c}}$ denote the terms and order chosen from $\overrightarrow{t}$ and $\overrightarrow{s}$, respectively, to be unified. Let $\overrightarrow{t_{r}}$ and $\overrightarrow{s_{r}}$ denote the rest of the terms in $\overrightarrow{t}$ and $\overrightarrow{s}$, that will be distributed to $\overrightarrow{N}$ and $\overrightarrow{M}$, respectively.

We know that $\sigma = \sigma_{M}\sigma_{i}$ (Alg. 2, line 9), where $\sigma_{t}$ is the unifier of $\overrightarrow{t_{c}}$ and $\overrightarrow{s_{c}}$, and $\sigma_{M}$ is obtained from partitions denoted as $\pi_{t}(\overrightarrow{t_{r}})$ and $\pi_{s}(\overrightarrow{s_{r}})$.

1. $t_{a} \in \overrightarrow{t_{c}}$ and $s_{b} \in \overrightarrow{s_{c}}$

   Take $\mu = \mu_{M}\mu_{t}$ such that $\mu_{M} = \sigma_{M}$ is obtained from the same partitions $\pi_{t}(\overrightarrow{t_{r}})$ and $\pi_{s}(\overrightarrow{s_{r}})$, and $\mu_{t}$ is such that $\sigma_{t} = \mu_{t}\sigma'$ for some $\sigma'$. The existence of such $\mu_{t}$ is guaranteed by Theorem 3. Therefore, $\sigma = \sigma_{M}\sigma_{t} = \sigma_{M}\mu_{t}\sigma' = \mu\sigma'$.

2. $t_{a} \in \overrightarrow{t_{r}}$ and $s_{b} \in \overrightarrow{s_{r}}$

   Let $\overrightarrow{t_{pa}}, t_{a}$ be the part from $\pi_{t}(\overrightarrow{t_{r}})$ with $t_{a}$, and $\overrightarrow{s_{pa}}, s_{b}$ the part from $\pi_{s}(\overrightarrow{s_{r}})$ with $s_{b}$.

   Take $\mu = \mu_{M}\mu_{t}$ such that $\mu_{t} = \sigma_{t}$ is the unifier of $\overrightarrow{t_{c}}$ and $\overrightarrow{s_{c}}$, and $\mu_{M}$ is obtained from partitions $\pi_{t}(\overrightarrow{t_{r}})$ where $\overrightarrow{t_{pa}}, t_{a}$ is replaced by $\overrightarrow{t_{pa}}$ and analogously for $\pi_{s}(\overrightarrow{s_{r}})$. Thus the mappings in $\sigma_{M}$ and $\mu_{M}$ are the same, except for two multiset variables $N_{a}$ and $M_{b}$:

$$\left\{ M_{b} \mapsto \overrightarrow{s_{pa}}; s_{b}, M'_{b} ; \quad N_{a} \mapsto \overrightarrow{t_{pa}}, t_{a}, N'_{a} \right\} \subset \sigma_{M}$$

$$\left\{ M_{b} \mapsto \overrightarrow{s_{pa}}; M'_{b} ; \quad N_{a} \mapsto \overrightarrow{t_{pa}}, N'_{a} \right\} \subset \mu_{M}$$

Since $M'_{b}$ and $N'_{a}$ are fresh multiset variable names:

$$\sigma_{M} = \mu_{M}\left\{ M'_{b} \mapsto s_{b}, M'_{b} ; \quad N'_{a} \mapsto t_{a}, N'_{a} \right\}$$

And since $\sigma_{t} = \mu_{t}$:

$$\sigma_{M}\sigma_{t} = \mu_{M}\mu_{t}\left\{ M'_{b} \mapsto s_{b}, M'_{b} ; \quad N'_{a} \mapsto t_{a}, N'_{a} \right\}\mu_{t}$$

The image of $\mu_{t}$ does not contain $M'_{b}$ nor $N'_{a}$, therefore:

$$\sigma_{M}\sigma_{t} = \mu_{M}\mu_{t}\left\{ M'_{b} \mapsto s_{b}, M'_{b} ; \quad N'_{a} \mapsto t_{a}, N'_{a} \right\}\mu_{t}$$

Thus:

$$\sigma = \mu\left\{ M'_{b} \mapsto s_{b}, M'_{b} ; \quad N'_{a} \mapsto t_{a}, N'_{a} \right\}\mu_{t}$$
3. $t_a \in \overline{t_c}$ and $s_b \in \overline{s_r}$

Let $s_k$ be the term from $\overline{s_c}$ that is paired with $t_a$ and $s_p, s_b$ be the part from $\pi_s(\overline{s_r})$ containing $s_b$. Assume that $t_a$ is unified with $s_k$ with mgu $\sigma_{ak}$, and that $(\overline{t_c}\setminus \{t_a\})\sigma_{ak}$ unifies with $(\overline{s_c}\setminus \{s_k\})\sigma_{ak}$ with mgu $\sigma_c$. Thus $\sigma_t = \sigma_{ak}\sigma_c$. Let $M_b$ be the variable to which partition $s_p, s_b$ is assigned. Thus:

$$\{M_b \mapsto \overline{s_p}, s_b, M'_b\} \subset \sigma_M$$  \hspace{1cm} \text{(1)}
$$\{M_b \mapsto \overline{s_p}\sigma_{ak}, s_b\sigma_{ak}, M'_b\} \subset \sigma_M\sigma_{ak}$$  \hspace{1cm} \text{(2)}
$$\{M_b \mapsto \overline{s_p}\sigma_{ak}, t_a\sigma_{ak}, M'_b\} \subset \sigma_M\sigma_{ak}$$  \hspace{1cm} \text{(3)}
$$\{M_b \mapsto \overline{s_p}\sigma_{ak}, s_k\sigma_{ak}, M'_b\} \subset \sigma_M\sigma_{ak}$$  \hspace{1cm} \text{(4)}

Take $\mu = \mu_M\mu_t$ such that the terms $\overline{t_c}\setminus \{t_a\}$ and $\overline{s_c}\setminus \{s_k\}$ are unified with mgu $\mu_t$, and $\mu_M$ is computed using partition $\pi_t(\overline{t_c})$ and $\pi_s(\overline{s_r})$ where part $s_p, s_b$ is replaced by $\overline{s_p}, s_k$. Therefore,

$$\{M_b \mapsto \overline{s_p}, s_k, M'_b\} \subset \mu_M$$  \hspace{1cm} \text{(5)}

Because $\mu_t$ is the mgu of the two lists, we have that: $\sigma_t = \sigma_{ak}\sigma_c = \mu_t\sigma'_t$ for some $\sigma'_t$. And from 4 and 5 we can also conclude: $\sigma_M\sigma_{ak} = \mu_M\sigma_{ak}$. Using these equalities:

$$\sigma = \sigma_M\sigma_t = \sigma_M\sigma_{ak}\sigma_c = \mu_M\sigma_{ak}\sigma_c = \mu_M\mu_t\sigma'_t = \mu\sigma'_t.$$  

4. $t_a \in \overline{t_r}$ and $s_b \in \overline{s_c}$ Analogous to the previous case.