1 Proving Results from the paper Nachum Dershowitz: Tripartite Unions

The paper starts with Theorems 1 and 2, and then proves Theorem 3 which is a considerable improvement of Theorems 1 or 2. We start with Theorem 3, which we call `wfp_tri`

It appears that all Dershowitz's results in the paper assume that A, B and C are well-founded.

As a preliminary, it should be noted that

- in Isabelle, a relation R is well-founded if there is not an infinite decreasing sequence

$$\ldots <_R x_n <_R x_{n-1} <_R \ldots <_R x_1 <_R x_0$$

  where $x <_R y$ means $(x, y) \in R$, and
- in Isabelle, the composition of relations R and S is defined by

$$R \bigcirc S = \{(x, z). \exists y. (x, y) \in S \& (y, z) \in R\}$$

```
rel_comp_def:
  "?r O ?s == {(x, z). EX y. (x, y) : ?s & (y, z) : ?r}"
```

Since *both* of these conventions are the opposite of those used by Dershowitz, which means that his theorems look the same as ours. If just one were different from his usage we would have to reverse the order of relation composition to make his theorems look like ours.

We use `dvk_cond` R A, the condition from Doornbos & von Karger [1], that $R \bigcirc A \subseteq (A \bigcirc (A \cup R)^*) \cup R$

```
dvk_cond_def':
  "dvk_cond ?s ?r == ?s O ?r <= (?r O (?r Un ?s)^*) Un ?s"
```

We next reproduce Dershowitz's Theorem 3, [2, Thm 3]

Theorem 1 (`wf_tri'`, Dershowitz, Theorem 3). *If A, B and C are well-founded, and the following hold:*

(a) $(B \cup C) \bigcirc A \subseteq (A \bigcirc (A \cup B \cup C)^*) \cup (B \cup C)$
(b) $C \bigcirc B \subseteq (A \bigcirc (A \cup B \cup C)^*) \cup (B \bigcirc B^*) \cup C$

then $A \cup B \cup C$ is well-founded.

```
wf_tri':
   "[| ?BC = ?B Un ?C; dvk_cond ?BC ?A;
    ?C O ?B <= (?A O (?A Un ?BC)^*) Un (?B O ?B^*) Un ?C;
    wf ?A; wf ?B; wf ?C |] ==> wf (?A Un ?BC)"
```

We separate Dershowitz's proof into a number of lemmas. Note how, generally, statements in the proof of the form "there exists an infinite chain" have to be translated into a lemma with hypotheses and conclusion that certain relations are well-founded, or that something is in the well-founded part or a relation.

The *well-founded part* (`wfp` in Isabelle) of a relation is the set whose elements are not the head of any infinite descending chain. So a relation is well-founded if and only if every member of the underlying set is in its well-founded part.

Following Dershowitz, we say an R-*immortal* element is the head of an infinite descending chain in R, and "*immortal*" means $A \cup R$-immortal, or $A \cup B \cup C$-immortal, as the case may be.

NEW Define R^- to be R, but excluding steps of the form (w, z) where there exists some y such that $(y, z) \in A$ and y is $A \cup R$-immortal.

Lemma 1 (`wfp_tri_lem_ch`)**.** *ORIGINAL If there is an infinite descending $A \cup R$-chain then there is an infinite descending $A \cup R$-chain where each step $(w, z) \in R$ in that chain has the property that there is no $(y, z) \in A$ such that y is the head of an infinite descending $A \cup R$-chain.*

CONTRAPOSITIVE If $A \cup R^-$ is well-founded then $A \cup R$ is well-founded.

Proof. You construct an infinite descending $A \cup R$-chain using A where possible and using R only where necessary.

The (forward) `image` r "s of a set s under a relation r is the containing those y such that $x \in s$ and $(x, y) \in r$.

```
Image_def: "?r `` ?s == {y. EX x:?s. (x, y) : ?r}"
```

```
wfp_tri_lem_ch:
   "?x : wfp (?A Un ?R Int {(y, z). z ~: ?A `` (- wfp (?A Un ?R))})
      ==> ?x : wfp (?A Un ?R)"
```

Lemma 2 (`wfp_tri_lem_dvk`)**.** *ORIGINAL If R and A satisfy the Doornbos & von Karger [1] condition* `dvk_cond`*, and A is well-founded, and there is an infinite descending $A \cup R$-chain, then there is an infinite descending*

R-chain whose members are not of the form z where $(y, z) \in A$ and y is immortal, ie is the head of an infinite descending $A \cup R$-chain.

CONTRAPOSITIVE If R and A satisfy the Doornbos & von Karger [1] condition `dvk_cond`, and A and R^- (defined before Lemma 1) are well-founded, then $A \cup R$ is well-founded.

We first give a more intuitive proof, then a proof which more closely approximates the Isabelle proof.

Proof. Consider an infinite descending $A \cup R$-chain. As A is well-founded, from any point in this chain there must be another R-step. Wherever possible replace a R-step $z >_R v$ followed by an A-step $v >_A u$ by an A-step (possibly followed by a number of A- or R-steps) in the given chain. (This relates to the part $R \bigcirc A \subseteq (A \bigcirc (A \cup R)^*) \cup \ldots$ of `dvk_cond`). Alternatively, if possible, replace the remainder of the chain from this point by any other infinite chain $z >_A y >_{A \cup R} \ldots$. Again, this will not always be possible since A is well-founded.

So, where this is not possible, we can replace a R-step followed by an A-step by a single R-step, which is possible using the part $R \bigcirc A \subseteq \ldots \cup R$ of `dvk_cond`.

Doing this repeatedly could absorb any number of A-steps, but, again, as A is well-founded there cannot be infinitely many such A-steps, so eventually we reach another R-step. Repeating this gives the required infinite R-chain, with the given property.

This next proof approximates more closely to the Isabelle proof.

Proof. Assume that A is well-founded. Define R^- to be R, but excluding steps of the form (w, z) where there exists some y such that $(y, z) \in A$ and y is immortal. Assume that R^- is well-founded.

Suppose that there is an infinite descending $A \cup R$-chain. Choose a head z of such a chain, choosing z to be A-minimal, and also to be R^--minimal among A-minimal immortal elements. As z is A-minimal, the first step of an infinite chain must be (say) $(y, z) \in R$, and also in fact $(y, z) \in R^-$. As A is well-founded, let y be A-minimal among possible choices for y. Then, by the R^--minimality of z, although y is immortal, it is not A-minimal among immortal members. So we have $(x, y) \in A$, where x is immortal. So as $R \bigcirc A \subseteq (A \bigcirc (A \cup R)^*) \cup R$, we could replace $z >_R y >_A x$ in the infinite chain by

- $(x, z) \in A \bigcirc (A \cup R)^*$, say $(x, y') \in (A \cup R)^*$ and $(y', z) \in A$ (where x, y' and z are immortal), but this would contradict the A-minimality of z (and our consequent inference that $(y, z) \notin A$), or

– $(x, z) \in R$, which would contradict our choice of y which was to be A-minimal, since x could have been chosen instead of y.

Thus, either way we get a contradiction, so $A \cup R$ is well-founded.

```
wfp_tri_lem_dvk:
   "[| dvk_cond ?R ?A; wf ?A;
         wf (?R Int {(y, z). z ~: ?A `` (- wfp (?A Un ?R))}) |]
      ==> ?x : wfp (?A Un ?R)"
```

Define C^- to be C, but excluding steps of the form (w, z) where there exists some y such that $(y, z) \in A$ and y is $X \cup B \cup C$-immortal.

For the purposes of Theorem 1 X will be A, but we will use the lemma with more general X when there are four or more relations.

Lemma 3 (`wf_tri_lem_BCm`). *If B and C^- (using the definition of C^- just above) are well-founded, and condition (b) of Theorem 1 is satisfied, then $B \cup C^-$ is well-founded.*

Proof. Assume that B and C^- are well-founded.

Suppose, contrary to the lemma, that $B \cup C^-$ is not well-founded. So there exists an $B \cup C^-$-immortal z. Choose z to be B-minimal such, and also to be C^--minimal among possible B-minimal choices.

As z is B-minimal, the first step of an infinite $B \cup C^-$-chain must be (say) $(y, z) \in C^-$. As B is well-founded, let y be B-minimal among possible choices for y. Then, by the C^--minimality of z, although y is $B \cup C^-$-immortal, it is not B-minimal among $B \cup C^-$-immortal members. So we have $(x, y) \in B$, where x is $B \cup C^-$-immortal. So as $C \bigcirc B \subseteq (A \bigcirc (X \cup B \cup C)^*) \cup (B \bigcirc B^*) \cup C$, we could replace $z >_C y >_B x$ in the infinite chain by

– $(x, z) \in A \bigcirc (X \cup B \cup C)^*$, say $(x, y') \in (X \cup B \cup C)^*$ and $(y', z) \in A$ — but x is $B \cup C^-$-immortal, and so is the head of an infinite descending $X \cup B \cup C$-chain, contradicting that $(y, z) \in C^-$,
– $(x, z) \in B \bigcirc B^*$, which would contradict our choice of z to be B-minimal
– $(x, z) \in C$ (and so $(x, z) \in C^-$) which would contradict our choice of y to be B-minimal, since x could have been chosen instead of y.

Thus, in each case we get a contradiction, so $B \cup C^-$ is well-founded.

```
wf_tri_lem_BCm:
  "[| ?BC = ?B Un ?C; ?C O ?B <= (?A O (?X Un ?BC)^*) Un (?B O ?B^*) Un ?C;
     wf ?B; wf (?C Int {(y, z). z ~: ?A `` (- wfp (?X Un ?BC))}) |] ==>
   wf (?B Un ?C Int {(y, z). z ~: ?A `` (- wfp (?X Un ?BC))})"
```

Proof. *(of Theorem 1)* By Lemma 2 it is enough to prove that $(B \cup C)^-$ is well-founded. By Lemma 3 we have that $B \cup C^-$ is well-founded, and clearly $(B \cup C)^- \subseteq B \cup C^-$.

Now we show how to extend this result to four (or more) relations.

Theorem 2 (`wf_four`). *If A, B, C and D are well-founded, and the following hold:*

(a) $(B \cup C \cup D) \bigcirc A \subseteq (A \bigcirc (A \cup B \cup C \cup D)^*) \cup (B \cup C \cup D)$
(b) $D \bigcirc C \subseteq (A \bigcirc (A \cup B \cup C \cup D)^*) \cup (C \bigcirc C^*) \cup D$
(c) $(C \cup D) \bigcirc B \subseteq (A \bigcirc (A \cup B \cup C \cup D)^*) \cup (B \bigcirc B^*) \cup C \cup D$

then $A \cup B \cup C \cup D$ is well-founded.

```
val wf_four =
   "[| ?uall = ?A Un ?B Un ?C Un ?D; dvk_cond (?B Un ?C Un ?D) ?A;
       ?D O ?C <= (?A O ?uall^*) Un (?C O ?C^*) Un ?D;
       ?C Un ?D O ?B <= (?A O ?uall^*) Un (?B O ?B^*) Un (?C Un ?D);
       wf ?A; wf ?B; wf ?C; wf ?D |] ==> wf ?uall"
```

Proof. We adapt the previous definition of R^- for a relation R: R^- is R, but excluding steps of the form (w, z) where there exists some y such that $(y, z) \in A$ and y is $A \cup B \cup C \cup D$-immortal.

As D is well-founded, *a fortiori* D^- is well-founded.

Therefore by Lemma 3 (setting A, X, B, C to $A, A \cup B, C, D$) and condition (b) $C \cup D^-$ is well-founded, and so *a fortiori* $(C \cup D)^-$ is well-founded.

Then, by Lemma 3 (setting A, X, B, C to $A, A, B, C \cup D$) and condition (c) $B \cup (C \cup D)^-$ is well-founded and so *a fortiori* $(B \cup C \cup D)^-$ is well-founded.

Then, by Lemma 2 $A \cup B \cup C \cup D$ is well-founded.

We now extend this result to an arbitrary number of relations. The proof is straightforward but we need to set up some definitions.

First the condition we call `tri_cond`, which is the condition satisfied by the list $[B, C, D]$ in the case of four relations. It is defined recursively and gives (for example) conditions b and c of Theorem 2.

```
tri_cond_Nil : "tri_cond ?Auall [] = True"
tri_cond_Cons : "tri_cond ?Auall (?B # ?Bs) =
   ((let uBs = foldr op Un ?Bs {}
     in uBs O ?B <= ?Auall Un (?B O ?B^*) Un uBs) & tri_cond ?Auall ?Bs)"
```

We then need a separate lemma which is proved by structural induction on the list, say $[B, C, D]$, of relations. For the general case we work with a list $B_1, B_2, \ldots, B_n$.

Define U^- to be U, but excluding steps of the form (w, z) where there exists some y such that $(y, z) \in A$ and y is $X \cup U$-immortal.

Lemma 4. *Suppose $B_1, B_2, \ldots, B_n$ are all well-founded, and let $U = B_1 \cup B_2 \cup \ldots \cup B_n$. Suppose the condition* ***tri_cond*** *$(A \bigcirc (X \cup U)[B_1, B_2, \ldots, B_n]$ holds. Then U^- is well-founded.*

```
tri_n_lem : "[| ?uBs = foldr op Un ?Bs {}; ?Auall = ?A O (?X Un ?uBs)^*;
      tri_cond ?Auall ?Bs; Ball (set ?Bs) wf |] ==>
      wf (?uBs Int {(y, z). z ~: ?A `` (- wfp (?X Un ?uBs))})"
```

Proof. The proof is by structural induction on the list $[B_1, B_2, \ldots, B_n]$, and each step is proved using Lemma 3. The value used for X varies throughout, so if its final value is X_f, then the lemma is proved successively for

$$\begin{array}{ll} [] & X = X_f \cup B_1 \cup B_2 \cup \ldots \cup B_n \\ [B_n] & X = X_f \cup B_1 \cup B_2 \cup \ldots \cup B_{n-1} \\ \vdots & \quad \vdots \\ [B_2, \ldots, B_n] & X = X_f \cup B_1 \\ [B_1, B_2, \ldots, B_n] & X = X_f \end{array}$$

Note that the value of $X \cup U$ (as used in the definition of U^- above) therefore remains unchanged, and that at each step we also use, in addition to Lemma 3, the fact that if $B \cup V^-$ is well-founded, then $(B \cup V)^-$ is well-founded.

Then we have the following theorem.

Theorem 3. *Suppose A and $B_1, B_2, \ldots, B_n$ are all well-founded, and let $U = B_1 \cup B_2 \cup \ldots \cup B_n$. Suppose the condition* ***tri_cond*** *$(A \bigcirc (A \cup U)[B_1, B_2, \ldots, B_n]$ holds, and that $U \bigcirc A \subseteq (A \bigcirc (A \cup U)^*) \cup U$ Then $A \cup U$ is well-founded.*

```
tri_n "[| ?uBs = foldr op Un ?Bs {}; ?Auall = ?A O (?A Un ?uBs)^*;
  dvk_cond ?uBs ?A; tri_cond ?Auall ?Bs; wf ?A; Ball (set ?Bs) wf |]
==> wf (?A Un ?uBs)"
```

Proof. By Lemma 4 we get that U^- is well-founded, where we use $X = A$ in the definition of U^-. Then Lemma 2 gives the result.

References

1. Henk Doornbos & Burghard Von Karger. On the Union of Well-Founded Relations. L. J. of the IGPL 6 (1998), 195-201.
2. Nachum Dershowitz. Tripartite Unions. preprint