Some properties of darcs patch theory

Ganesh Sittampalam *et al.*

November 7, 2005

Abstract

This is an attempt to derive some properties of darcs patch theory. We start by specifying the "axioms" that must be true of patches and commutation, and prove some theorems.

1 Notation

A, B etc are individual patches, that can't be expressed as a sequence of two smaller patches. They could be either primitive patches or mergers or conflictors or whatever. They could be inverted.

Sequential patch composition is written with juxtaposition. Not all patches can be sequentially composed, but use of the notation AB implicitly assumes that they can. [1]

Commutation is written $AB \leftrightarrow B'A'$. If $\nexists B'A'$ s.t. $AB \leftrightarrow B'A'$, then we write $AB \leftrightarrow \textbf{fail}$.

We write As to represent a (possibly empty) sequence of patches of arbitrary length The empty sequence is written as **id**.

$\leftrightarrow^{\uparrow}$ is a commutation between sequences of patches, defined as follows:

$$\begin{array}{rcrcl} AB \leftrightarrow B'A' & \Longrightarrow & AB & \leftrightarrow^{\uparrow} & B'A' \\ As \leftrightarrow^{\uparrow} Bs & \Longrightarrow & AsC & \leftrightarrow^{\uparrow} & BsC \\ As \leftrightarrow^{\uparrow} Bs & \Longrightarrow & CAs & \leftrightarrow^{\uparrow} & CBs \end{array}$$

We distinguish different derivations of $As \leftrightarrow^{\uparrow} Bs$ from each other, so any particular statement of $As \leftrightarrow^{\uparrow} Bs$ has precisely one set of antecedents in the above definition. [2]

We define $\leftrightarrow^*$, the reflexive transitive closure of $\leftrightarrow^{\uparrow}$, as follows:

$$\begin{array}{rcrcl} & & As & \leftrightarrow^* & As \\ As \leftrightarrow^{\uparrow} Bs & \Longrightarrow & As & \leftrightarrow^* & Bs \\ As \leftrightarrow^* Bs \wedge Bs \leftrightarrow^* Cs & \Longrightarrow & As & \leftrightarrow^* & Cs \end{array}$$

[1] It is likely that a mechanised proof about patch theory would have to make this precondition explicit.

[2] This is horrible. I need a better notation. But for now I just want to get this proof written down.

Again we distinguish different derivations.

The relation $\sim$ between individual patches is defined as follows.

$$\begin{array}{rcrcl} & & A & \sim & A \\ AB \leftrightarrow B'A' & \implies & A & \sim & A' \\ AB \leftrightarrow B'A' & \implies & B & \sim & B' \\ A \sim A' \wedge A' \sim A'' & \implies & A & \sim & A'' \end{array}$$

We *do not* attempt to distinguish different derivations of $\sim$; it is a simple relation.

We adopt a notational convention that if we mention A and A' together, then $A \sim A'$ (etc).[3]

2 Axioms

These are properties that we assume about individual patches and commutation. They are not quite axioms, since it would be possible to prove them about any particular implementation of patches and commutation, but for our current purposes they are.

Associativity of patch sequencing:

$$(AB)C = A(BC)$$

Since this property is required, we can omit parentheses (and it does make sense to talk about lists).

Uniqueness of commutation:

$$AB \leftrightarrow B'A \wedge AB \leftrightarrow B''A'' \implies A' = A'' \wedge B' = B''$$

Invertibility of commutation:

$$AB \leftrightarrow B'A' \implies B'A' \leftrightarrow AB$$

Note that this means that $\sim$ is an equivalence relation.

3-way permutivitiy of commutation:

If

$$ABC \leftrightarrow^{\uparrow} B'A'C \leftrightarrow^{\uparrow} B'C'A'' \leftrightarrow^{\uparrow} C''B''A'' \leftrightarrow^{\uparrow} C''A'''B'' \leftrightarrow^{\uparrow} A''''C'''B'' \leftrightarrow^{\uparrow} A''''B'''C''''$$

Then

$$\begin{array}{rcl} A & = & A'''' \\ B & = & B''' \\ C & = & C'''' \end{array}$$

Consistency of failure:

If $A \sim A'$, $B \sim B'$, then $AB \leftrightarrow \mathbf{fail} implies A'B' \leftrightarrow \mathbf{fail}$.

[3]This is another thing that would need to be made explicit in a mechanised proof

3 Theorems

We start by explicitly writing down some "obvious" properties and constructing some useful machinery.

Theorem 1. *If* $As \leftrightarrow^{\uparrow} Bs$*, then* $|As| = |Bs|$*.*
If $As \leftrightarrow^{*} Bs$*, then* $|As| = |Bs|$*.*

Proof. By induction on the structure of $\leftrightarrow^{\uparrow}$ and $\leftrightarrow^{*}$. □

We now define the concept of the *associated permutation* for $\leftrightarrow^{\uparrow}$ and $\leftrightarrow^{*}$, by induction on their structure.

Informally, if p is the associated permutation for $As \leftrightarrow^{*} Bs$, and A_i occurs at position i in As, then A_i ends up being commuted into position $p(i)$ in Bs.

If $AB \leftrightarrow B'A'$, then $AB \leftrightarrow^{\uparrow} B'A'$ has the associated permutation $(1\ 2)$.

If $As \leftrightarrow^{\uparrow} Bs$ has the associated permutation $(n\ n+1)$, then $AsC \leftrightarrow^{\uparrow} BsC$ has the associated permutation $(n\ n+1)$.

If $As \leftrightarrow^{\uparrow} Bs$ has the associated permutation $(n\ n+1)$, then $CAs \leftrightarrow^{\uparrow} CBs$ has the associated permutation $(n+1\ n+2)$.

Note that by induction, the associated permutation for $\leftrightarrow^{\uparrow}$ is always a single transposition, so this definition makes sense.

$As \leftrightarrow^{*} As$ has the associated permutation *id*.

If $As \leftrightarrow^{\uparrow} Bs$ has the associated permutation p, then so does $As \leftrightarrow^{*} Bs$.

If $As \leftrightarrow^{*} Bs$ has the associated permutation p and $Bs \leftrightarrow^{*} Cs$ has the associated permutation q, then $As \leftrightarrow^{*} Cs$ has the associated permutation $q \odot p$.

Note that the alphabet for the associated permutation of $As \leftrightarrow^{\uparrow} Bs$ or $As \leftrightarrow^{*} Bs$ is $1 \ldots |As|$.

Every such commutation has precisely one associated permutation (since it is defined by induction on the structure of the commutation and we only allow one derivation for each commutation).

Theorem 2. *If* $As = A_{p(1)} \ldots A_{p(n)} \leftrightarrow^{*} B_1 \ldots B_n = Bs$ *has the associated permutation* p*, then* $\forall i. 1 \leq i \leq n. A_i \sim B_i$*.* [4]

Proof. By induction on the structure of $\leftrightarrow^{\uparrow}$ and $\leftrightarrow^{*}$. □

Note that the indexing of the patches is somewhat counter-intuitive; nonetheless, it is correct. We expect the $A_{p(i)}$, which is the ith element of As, to commute into $B_{p(i)}$, the $p(i)$th element of Bs.

We now define the concept of a *canonical representation* of a permutation p. Such a representation is a sequence of transpositions.

If $p = id$, the canonical representation of p is the empty sequence.

Otherwise, pick the smallest i such that $p(i) \neq i$ (if no such i existed then $p = id$). Let $j = p^{-1}(i)$. The first element of the sequence is $(j-1\ j)$, and the remainder of the sequence is the canonical representation of $p' = p \odot (j-1\ j)$.

[4] It would be nice if the converse were true, i.e. $A_{p(1)} \ldots A_{p(n)} \leftrightarrow^{*} B_1 \ldots B_n$ has the associated permutation p if $\forall i. 1 \leq i \leq n. A_i \sim B_i$. However I think it would require some kind of stronger property, such as unique patch ids, to make it so.

Note that j cannot be 1, so this definition is well-formed. [If $j = 1$, then $i = p(1)$, so $i \neq 1$ (otherwise $i = p(i)$), so $p(1) \neq 1$, so i is not the smallest for which this property holds.]

Also, this procedure must terminate, so the canonical representation is finite. Either:

- $p' = \mathit{idperm}$ and we terminate
- $p'^{-1}(i) = i$. Then the new i we will pick for p' is strictly greater than the original i for p.
- Otherwise, the new i we will pick for p' is the same as that for p,[5] and $p'^{-1}(i) = p^{-1}(i) - 1$.

So either i increases (and is bounded by n) or it stays the same and $p^{-1}(i)$ decreases.

Theorem 3. *If $(j-1\ j)$ is the first element of the canonical representation of p, then $p(j-1) > p(j)$, and $p(j) < j$.*

Proof. Let $i = p(j)$. We know that $\forall k.k < i.p(k) = k$, and so $\forall k.k < i.k = p^{-1}(k)$. Also, $i \neq p(i)$.

Clearly, $p(j-1) \neq p(j)$.

Suppose $p(j-1) < p(j)$. Then $p(j-1) < i$, so $j-1 < i$, so $j < i+1$. If $j = i$, then $p(i) = j = i$, so $j < i$. But then $p(j) = j < i$, which is impossible.

So $p(j-1) > p(j)$.

Now suppose $j < p(j)$. Then $p(j) = j$, which is impossible. So $p(j) < j$. □

We now define the *canonical commutation path* for a permutation p. Such a path starts from $A'_{p(1)} \dots A'_{p(n)}$ and finishes at $A_1 \dots A_n$, where the alphabet of p is $1 \dots n$. The path is the same length as the canonical representation of p, and each $\leftrightarrow^{\uparrow}$ step in the path has the corresponding transposition in the canonical representation of p as its associated permutation.

Informally, one is constructed by first commuting A'_1 to the left of the sequence, then commuting A'_2 to the one-but-leftmost position, and so on.

It is not guaranteed that all of these commutes will succeed, so there might not be any canonical commutation path for any given p and sequence of patches.

By construction, any suffix of a canonical commutation path is also a canonical commutation path (for a different permutation, but the same ending patch sequence).

Theorem 4. *If $Bs \leftrightarrow^* As$ is a canonical commutation path for p, then p is the associated permutation of $Bs \leftrightarrow^* As$.*

Proof. Obvious, from the definition of the canonical representation of p and the construction of the canonical commutation path. □

[5] Need to make this into a theorem and move it below the following theorem so we can use that

Theorem 5. *If $Bs \leftrightarrow^* As$ is a canonical commutation path for p, and $Cs \leftrightarrow^* As$ is also a canonical commutation path for p, then $Bs = Cs$.*

If $As \leftrightarrow^* Bs$ is a canonical commutation path for p, and $As \leftrightarrow^* Cs$ is also a canonical commutation path for p, then $Bs = Cs$.

Proof. Since the commutation paths must have the same structure, this follows from the "Uniqueness of commutation" and "Invertibility of commutation" axioms. (More formally, by induction on the length of the canonical representation of p.) □

We therefore talk about "the" canonical commutation path for p starting with or ending with a particular patch sequence.

With all this machinery set up, we can move on to proving some useful properties.

Theorem 6. *Suppose that p is the associated permutation for $As' \leftrightarrow^* As$ Then there is a canonical commutation path for p that starts with As'.*

Proof. We use induction on the length of the canonical representation of p.

If $p = id$, then we are done.

Otherwise, Let $As' = A'_{p(1)} \dots A'_{p(n)}$, and $As = A_1 \dots A_n$.

Let (i-1 i) be the first element in the canonical representation of p, and let $j = p(i-1)$ and $k = p(i)$, so that A'_j and A'_k are the first patches in As' we try to commute. Recall that $j > k$.

If $A'_j A'_k \leftrightarrow A''_k A''_j$, then let $As'' = A'_{p(1)} \dots A'_{p(i-2)} A''_k A''_j A'_{p(i+1)} \dots A'_{p(n)}$, giving $As' \leftrightarrow^{\uparrow} As''$ as the first step on the canonical commutation path.

Then use the inverse of this commute together with $As' \leftrightarrow^* As$ to construct a new path $As'' \leftrightarrow^* As$, and apply the induction hypothesis to construct the canonical commutation path from $As'' \leftrightarrow^* As$.

Now suppose that $A'_j A'_k \leftrightarrow$ **fail**. But we know that $j > k$, so A_k occurs before A_j in As.

So somewhere in the path $As' \leftrightarrow^* As$, some patches A''_j and A''_k must swap position[6], *i.e.*$A''_j A''_k \leftrightarrow^* A'''_k A'''_j$. But this violates our "Consistency of failure" axiom. □

Theorem 7. *Suppose:*

- *$As \leftrightarrow^* Bs$ is a canonical commutation path for p*
- *$As' \leftrightarrow^{\uparrow} As$ with associated permutation $(i-1\ i)$*
- *$As' \leftrightarrow^* Bs'$ is a canonical commutation path for $p \odot (i-1\ i)$*
- *The canonical representation for $p \odot (i-1\ i)$ is one transposition longer than that for p*

Then $Bs = Bs'$.

[6]This claim really should be formalised

Proof. Write As as $A_{p(1)} \dots A_{p(n)}$ and As' as $A_{p(1)} \dots A_{p(i-2)} A'_{p(i-1)} A'_{p(i)} A_{p(i+1)} \dots A_{p(n)}$.

Write Bs as $B_1 \dots B_n$ and Bs' as $B'_1 \dots B'_n$.

Let $p' = p \odot (i-1\ i)$. Let q be the canonical representation of p and q' be the canonical representation of p'.

Intuitively, q' carries out the same sequence of commutations as q, except that at some point it also has to swap commuted versions of A'_i and A'_{i-1}, which is why it is one element longer. Also, A_{i-1} and A_i are in the correct order, so $p(i-1) < p(i)$. [7]

We use induction on the length of q'.

Consider the first transposition in q', $(j-1\ j)$.

Recall that $p'(j-1) > p'(j)$, and that $\forall k. k < p'(j). k = p^{-1}(k) \wedge k = p(k)$.

We now proceed by case analysis on the value of j.

If $j = i$, then the "swapping back" happens immediately. The first commutation in $As' \leftrightarrow^* Bs'$ must be $As' \leftrightarrow^\uparrow As$ (by "Uniqueness of commutation"), so $As \leftrightarrow^* Bs'$ must be a canonical commutation path for p (since suffixes of canonical commutation paths are also canonical). So $Bs = Bs'$.

Suppose $j = i-1$. Then $p'(j) = p'(i-1) = p(i)$, and $p'(j+1) = p'(i) = p(i-1)$. Since $p(i-1) < p(i)$, $p'(j+1) < p'(j)$. So $p'(j+1) = j+1$, so $j < j+1 < p'(j)$, so $p'(j) = j$, which is impossible.

Now suppose $j = i+1$. Then $p'(j) < p'(j-1)$ So $p(i+1) = p'(i+1) < p'(i) = p(i-1)$. Recall also that $p(i-1) < p(i)$. We also know that $p'(j) < j$. So $p(i+1) < i+1$.

Now, $forallk.k < p'(j).p'(k) = k$, so $forallk.k < p(i+1).p'(k) = k$, and since $p(i+1) < i+1$, $p'(k) = p(k)$.

Suppose $p(i+1) = i$. Then $i-1 < p(i+1)$ so $p(i-1) = i-1$. So $p'(i) = i-1$, and $p'(i+1) = i$. So $p''(i) = i$ and $p''(i+1) = i-1$, and $p''(i-1) = p'(i-1) = p(i)$.

Now, consider $p'' = p' \odot (j-1\ j) = p' \odot (i\ i+1)$. If $k < p''(i) = p'(i+1) = p(i+1)$, then $p''(k) = p(k) = k$. Also, $p''(i) = p'(i+1) = p(i+1) \neq i$. So the first transposition in the canonical representation of p'' is $(i-1\ i)$.

First transposition in p is $(i\ i+1)$ and second is $(i-1\ i)$. [8]

We have that

$$As' = A_{p(1)} \dots A_{p(i-2)} A'_{p(i)} A'_{p(i-1)} A_{p(i+1)} A_{p(i+2)} \dots A_{p(n)}$$

The first commutation gives us

$$A_{p(1)} \dots A_{p(i-2)} A'_{p(i)} A''_{p(i+1)} A''_{p(i-1)} A_{p(i+2)} \dots A_{p(n)}.$$

The next commutation gives us

$$A_{p(1)} \dots A_{p(i-2)} A'''_{p(i+1)} A''_{p(i)} A''_{p(i-1)} A_{p(i+2)} \dots A_{p(n)}.$$

Call this sequence As'''.

[7] Ought to formalise this paragraph too...

[8] More rabbits out of hats.

Now consider

$$As = A_{p(1)} \dots A_{p(i-2)} A_{p(i-1)} A_{p(i)} A_{p(i+1)} A_{p(i+2)} \dots A_{p(n)}$$

The first commutation gives us

$$A_{p(1)} \dots A_{p(i-2)} A_{p(i-1)} A''''_{p(i+1)} A'''_{p(i)} A_{p(i+2)} \dots A_{p(n)}.$$

The next commutation gives us

$$A_{p(1)} \dots A_{p(i-2)} A'''''_{p(i+1)} A'''_{p(i-1)} A'''_{p(i)} A_{p(i+2)} \dots A_{p(n)}.$$

Call this sequence As''.

Now, by "Consistency of failure", we can commute $A''_{p(i)} A''_{p(i-1)}$ in As'' to give $A''''_{p(i-1)} A''''_{p(i)}$.

Taking apart the structure of $\leftrightarrow^{\uparrow}$ and inverting some of the commutations, we can construct the commutation path

$$A'''''_{p(i+1)} A'''_{p(i-1)} A'''_{p(i)} \leftrightarrow A_{p(i-1)} A''''_{p(i+1)} A'''_{p(i)} \leftrightarrow A_{p(i-1)} A_{p(i)} A_{p(i+1)} \leftrightarrow A'_{p(i)} A'_{p(i-1)} A_{p(i+1)} \leftrightarrow A'_{p(i)} A''_{p(i+1)}$$

By the "Three-way permutivity of commute" axiom, the initial and final sequences must actually be equal. In other words, As'' and As''' are linked by a single commutation, and we have the canonical paths $As'' \leftrightarrow^* Bs$ and $As''' \leftrightarrow^* Bs'$

We now apply induction on the length of these canonical paths, since they are shorter than the original ones.

For $j > i+1$, the first commutation from As' gives $A_1 \dots A_{i-1} A'_{i+1} A'_i Ai + 2 \dots A_{j-1} A'_{j+1} A'_j A_{j+2} \dots A_n$, and the first commutation from As gives $A_1 \dots A_{i-1} A_i A_{i+1} Ai + 2 \dots A_{j-1} A'_{j+1} A'_j A_{j+2} \dots A_n$, and these two are also linked by a single commutation with shorter canonical paths, so we can apply induction.

A similar argument follows for $j < i - 1$. $\square$

These two results are key. From here, it is a series of short easy steps to proving an "N-way permutivity" result.

Corollary 1. *Suppose:*

- $As \leftrightarrow^* Bs$ *is a canonical commutation path for* p
- $As' \leftrightarrow^{\uparrow} As$ *with associated permutation* $(i\ \ i+1)$
- $As' \leftrightarrow^* Bs'$ *is a canonical commutation path for* $p \odot (i\ \ i+1)$

Then $Bs = Bs'$.

Proof. The canonical commutation path for $p \odot (i\ \ i+1)$ must be either one transposition shorter or one transposition longer than that for p. If it is one transposition longer, apply the previous theorem. If it is one transposition shorter, construct the inverse commutation $As \leftrightarrow^{\uparrow} As'$ and apply the previous theorem with As, Bs and As', Bs' reversed. $\square$

Theorem 8. *Suppose:*

- $As \leftrightarrow^* Bs$ *is a canonical commutation path for* p
- $As' \leftrightarrow^{\uparrow} As$ *with associated permutation* $(i\ \ i+1)$

Then there exists a canonical commutation path $As' \leftrightarrow^* Bs$ *for* $p \odot (i\ \ i+1)$*.*

Proof. We can construct $As' \leftrightarrow^* Bs$ with associated permutation $p \odot (i\ \ i+1)$ from $As' \leftrightarrow^{\uparrow} As$ and $As \leftrightarrow^* Bs$. So by an earlier theorem a canonical path $As' \leftrightarrow^* Bs'$ for this permutation must exist (for some Bs'). By the previous corollary, $Bs' = Bs$. □

Theorem 9. *Suppose:*

- $As \leftrightarrow^* Bs$ *is a canonical commutation path for* p
- $As \leftrightarrow^* As'$ *with associated permutation* q

Then there exists a canonical commutation path $As' \leftrightarrow^* Bs$ *for* $p \odot q^{-1}$*.*

Proof. Invert $As \leftrightarrow^* As'$ to give $As' \leftrightarrow^* As$, and then apply induction on the structure of $As' \leftrightarrow^* As$, along with the previous theorem. □

Corollary 2. *If* $As \leftrightarrow^* As'$ *has associated permutation* id*, then* $As = As'$*.*

Proof. Let $p = id$ and $q = id$. Then we can trivially construct a canonical commutation path for p, $As \leftrightarrow^* As$.

Applying the previous theorem, there must be a canonical commutation path $As' \leftrightarrow^* As$ for $id \odot id^{-1} = id$, so by an earlier theorem showing uniqueness of canonical commutation paths, $As' = As$. □