Determining a permutation from its set of reductions

by John Ginsburg

ABSTRACT For any positive integer n, let S_n denote the set of all permutations of the set $\{1, 2, ..., n\}$. We think of a permutation just as an ordered list. For any p in S_n and for any $i \leq n$, let $p \downarrow i$ be the permutation on the set $\{1, 2, ..., n-1\}$ obtained from p as follows: delete i from p and then subtract 1 in place from each of the remaining entries of p which are larger than i. For any p in S_n we let $R(p) = \{q \in S_{n-1} : q = p \downarrow i \text{ for some } i \leq n\}$, the set of reductions of p. It is shown that, for $n > 4$, any p in S_n is determined by its set of reductions $R(p)$.

Key words and phrases: permutation, reduction, set of reductions, reconstruction

For any positive integer n, let S_n denote the set of all permutations of the set $\{1, 2, ..., n\}$. We think of a permutation just as an ordered list, and a permutation is displayed simply by listing its entries in order, sometimes with commas between them for clarity.

Let $n \geq 2$, and let $p \in S_n$. For any $i \leq n$, let $p \downarrow i$ be the permutation on the set $\{1, 2, ..., n-1\}$ obtained from p as follows: delete i from p and then subtract 1 in place from each of the remaining entries of p which are larger than i. Thus $p \downarrow i$ is an element of S_{n-1}, which we call the i'th *reduction* of p.

To illustrate, let $n = 5$ and let $p = 53412$. We then have
$p \downarrow 1 = 4231$, $p \downarrow 2 = 4231$, $p \downarrow 3 = 4312$, $p \downarrow 4 = 4312$, $p \downarrow 5 = 3412$.

This example shows that the reductions of a permutation are not necessarily all distinct.

For any p in S_n we let $R(p) = \{q \in S_{n-1} : q = p \downarrow i \text{ for some } i \leq n\}$. The set $R(p)$ is called *the set of reductions of p*.

For our example above, with $p = 53412$, we have $R(p) = \{4231, 4312, 3412\}$.

The main question we consider in this paper is the following:

Is a permutation determined by its set of reductions?

We will show that the answer is yes for $n > 4$, and we will describe a simple procedure for determining p from its set of reductions $R(p)$.

We note that this result fails for $n = 4$. If we let $p = 3142$ and $q = 2413$, then p and q are two different permutations with the same set of reductions $R(p) = R(q) = \{213, 231, 312, 132\}$.

Deleting one entry i, in all possible ways, from a permutation on $\{1, 2, ..., n\}$, to create various $n-1$-permutations, is of course a very commonly used idea. Recent papers in coding theory [7] and permutation graphs [4], [5] use these one-element deletions. By subtracting 1 from each of the entries which are larger than i, we are just creating a standardized version of the one-element deletion, so that it becomes an $n-1$-permutation on the "standard $n-1$-element set" $\{1, 2, ..., n-1\}$. The n reductions of a permutation on $\{1, 2, ..., n\}$ can be thus be thought of as being the n one-element deletions, up to isomorphism. This form of reduction is employed in [11], pages 85-86, in an inductive description of the Schensted correspondence.

The problem we are considering here can be viewed as a simple type of *reconstruction problem*, in which one attempts to reconstruct an object from its one-element deleted sub-objects. While this type of problem is perhaps most familiar for graphs(see [1]) and ordered sets(see [10]), a recent paper on reconstructing subsets of the plane [9] includes references to reconstructing codes, sets of real numbers, sequences and geometries. We refer the reader to [2], [6] and [8] for interesting recent work on reconstructing sequences from subsequences.

Before proceeding further, we emphasize that we are not considering here the *multiset* of reductions of a permutation p, in which each reduction would be included as many times as it occurs in the list $p \downarrow 1, p \downarrow 1, ..., p \downarrow n$.

In our proof that a permutation p is determined by its set of reductions $R(p)$, there are two basic steps: we show that the position of the entry n in p is determined by the set $R(p)$, and, letting $p-n$ denote the element of S_{n-1} obtained by deleting n from p, we show that the set of reductions of $p-n$ is also determined by $R(p)$. The result then follows by induction. We will establish these facts by means of a number of lemmas. In connection with part (vi) of Lemma 1 below, we note that, for any p in S_n and for any $i \le n$, $p \downarrow i$ is an element of S_{n-1} and so $(p \downarrow i) \downarrow j$ is defined for all $j \le n-1$. We will usually omit the brackets in referring to this iterated reduction, denoting it simply by $p \downarrow i \downarrow j$.

As basic notation for exhibiting a permutation $p \in S_n$ we will write $p(1), p(2), ..., p(n)$ or alternately $p_1 p_2 \cdots p_n$ to indicate the entries of p. In using such notation, we thus write $p(i) = k$ or $p^{-1}(k) = i$ to express the fact that the integer k occurs in the i'th position of p. We will also let p^{opp} denote the permutation obtained by listing the entries in the opposite order from which they are listed in p. Thus, for $p = 35124$ in S_5, we have $p^{opp} = 42153$.

Lemma 1. Let $n \geq 2$ and let $p \in S_n$.

(i) Let $1 \leq i \leq n$. Then we have $p^{opp} \downarrow i = (p \downarrow i)^{opp}$.

(ii) $p \downarrow n = p - n$.

(iii) Let $1 \leq i \leq n$ and suppose that i and $i+1$ occur consecutively in p. Then $p \downarrow i = p \downarrow (i+1)$.

(iv) Let i and j be positive integers such that $i, j \leq n$. Then $p \downarrow i = p \downarrow j$ if and only if the segment of p from i to j (including i and j) is either an increasing sequence of consecutive integers or a decreasing sequence of consecutive integers.

(v) Let $c = |\{k : p(k) \text{ and } p(k+1) \text{ are consecutive integers}\}|$. Then $|R(p)| = n - c$.

(vi) For any positive integers i and j with $i < j \leq n$, we have

$$p \downarrow j \downarrow i = p \downarrow i \downarrow (j-1).$$

Proof: (i) and (ii) are obvious. To verify (iii), note that, if i and $i+1$ occur consecutively in p, then both $p \downarrow i = p \downarrow (i+1)$ can be described as follows: replace the pair of entries $\{i, i+1\}$ by the single entry i and then subtract 1 from all other entries which are larger than i.

The implication from right to left in (iv) follows from (iii). For the converse, assume that $i < j$ and that $p \downarrow i = p \downarrow j$. By part (i), it is sufficient to consider the case when i is to the left of j in p. Suppose $i = p(k)$ and $j = p(l)$ where $k < l$. Note that the k'th entry of $p \downarrow j$ is i. Therefore the k'th entry of $p \downarrow i$ is i. But this latter entry is either $p(k+1)$ or $p(k+1)-1$, depending on whether or not $p(k+1)$ is larger than i. Since $p(k+1)$ is not i, we must have $i = p(k+1) - 1$, and we see that the entry immediately following i in p is $i+1$. Continuing in this way (or, equivalently, using induction on the number of entries of p between i and j), we see that the segment of p from i to j consists of an increasing sequence of consecutive integers.

To verify (v), consider the equivalence relation $\sim$ defined on the set $\{1, 2, ..., n\}$ by $i \sim j \leftrightarrow$ the segment of p from i to j is either an increasing sequence of consecutive integers or a decreasing sequence of consecutive integers. Suppose there are exactly t different equivalence classes $C_1, C_2, ..., C_t$. By (iv) we have $|R(p)| = t$. Let $S = \{k : p(k) \text{ and } p(k+1)$ are consecutive integers $\}$. For any r, the class C_r contains exactly $|C_r| - 1$ elements of S. Summing over r gives the size of S, namely $n - t$.

(vi) Suppose $i < j$. By part (i), it is sufficient to consider the case when i is to the left of j in p. In the following illustrations, we will let

x_1, x_2 and x_3 denote integers which are $> j$, and we will let y_1, y_2 and y_3 denote integers which are between i and j. When the operations $p \downarrow i$ and $p \downarrow j$ are applied, it is only integers which are larger than $> j$ and integers which are between i and j which are reduced. In illustrating the result of applying two operations successively below, we consider the three segments into which p is divided by i and j. In each segment, we illustrate only entries x for which $x > j$ and entries y for which $i < y < j$. Note that any of the three segments of p may contain none or one or both types of entries. Also note that, in each segment, any x's and y's which appear can be in any relative order. For our purposes, the order in which these entries appear is not important – it is how these entries change in place. All the other entries of p are left in place unchanged. We will use the symbol $\circ$ to indicate an empty spot from which an entry has been deleted. In the following illustration, we show p in the top row and then the result of first applying $\downarrow j$ and then $\downarrow i$.

$$\cdots x_1 \quad \cdots y_1 \quad \cdots i \quad \cdots x_2 \quad \cdots y_2 \quad \cdots j \quad \cdots x_3 \quad \cdots y_3 \quad \cdots$$

$$\downarrow j$$

$$\cdots x_1 - 1 \quad \cdots y_1 \quad \cdots i \quad \cdots x_2 - 1 \quad \cdots y_2 \quad \cdots \circ \quad \cdots x_3 - 1 \quad \cdots y_3 \quad \cdots$$

$$\downarrow i$$

$$\cdots x_1 - 2 \quad \cdots y_1 - 1 \quad \cdots \circ \quad \cdots x_2 - 2 \quad \cdots y_2 - 1 \quad \cdots \circ \quad \cdots x_3 - 2 \quad \cdots y_3 - 1 \quad \cdots$$

Similarly we next illustrate the result of first applying $\downarrow i$ to p and then $\downarrow (j-1)$. As we see, the result is the same.

$$\cdots x_1 \quad \cdots y_1 \quad \cdots i \quad \cdots x_2 \quad \cdots y_2 \quad \cdots j \quad \cdots x_3 \quad \cdots y_3 \quad \cdots$$

$$\downarrow i$$

$$\cdots x_1 - 1 \quad \cdots y_1 - 1 \quad \cdots \circ \quad \cdots x_2 - 1 \quad \cdots y_2 - 1 \quad \cdots j - 1 \quad \cdots x_3 - 1 \quad \cdots y_3 - 1 \quad \cdots$$

$$\downarrow j - 1$$

$$\cdots x_1 - 2 \quad \cdots y_1 - 1 \quad \cdots \circ \quad \cdots x_2 - 2 \quad \cdots y_2 - 1 \quad \cdots \circ \quad \cdots x_3 - 2 \quad \cdots y_3 - 1 \quad \cdots$$

Lemma 2. Let $n \geq 5$ and let p and q be elements of S_n such that $R(p) = R(q)$. Then the entry n occurs in the same position in p as it does in q.

Proof: Equivalently, we show that the position of n in p can be determined from the set $R(p)$. Let us first make some preliminary observations on the possible positions which the entry $n-1$ might occupy among the various members of $R(p)$. We will let $Z_p = \{q^{-1}(n-1) \, : \, q \in R(p)\}$. Obviously the set Z_p is determined by the set $R(p)$.

If $p^{-1}(n) = 1$ then $n-1$ is the first entry of $p \downarrow i$ for $i = 1, 2, ..., n-1$, and, in $p \downarrow n$, the position of $n-1$ is one smaller than its position in p. So in this case we either have $Z_p = \{1\}$ (when $n-1$ is the second entry of p), or $Z_p = \{1, j\}$ for some $j > 1$(when $n-1$ is not the second entry of p). Similarly, when n is the last entry of p, we either have $Z_p = \{n-1\}$ or $Z_p = \{j, n-1\}$ for some $j < n-1$.

Suppose n is neither the first nor last entry of p, but occurs in position r for some integer r such that $1 < r < n$. If i is any integer which lies to the left of n in p, then $n-1$ is in position $r-1$ in the reduction $p \downarrow i$. If i is any integer which lies to the right of n in p, then $n-1$ is in position r in the reduction $p \downarrow i$. The position of $n-1$ in $p \downarrow n$ is either the same as the position of $n-1$ in p (when $n-1$ is to the left of n in p), or one less than that position (when $n-1$ is to the right of n in p). So in this case, we either have $Z_p = \{r-1, r\}$ for some r with $1 < r < n$, or $Z_p = \{j, r-1, r\}$ for some r with $1 < r < n$ and for some j distinct from both r and $r-1$.

Thus for any p in S_n, Z_p must be one of the following sets: $\{1\}, \{n-1\}, \{1, n-1\}, \{1, j\}$ for some j with $1 < j < n-1$, $\{j, n-1\}$ for some j with $1 < j < n-1$, $\{r-1, r\}$ for some r such that $2 < r < n-1$, $\{j, r-1, r\}$ for some r with $1 < r < n$ and for some j distinct from both r and $r-1$. These possibilities are listed so as to be mutually exclusive. To show that $p^{-1}(n)$ is determined by the set $R(p)$, we proceed as follows: given the set $R(p)$, we find the corresponding set Z_p. It will be one of the 7 kinds of sets just listed. We will show that the position of n in p can be determined in each case.

The case when Z_p is a one-element set requires very little thought. If $Z_p = \{1\}$ then n must be the first entry of p - if n was in any other position, the above remarks show that Z_p would have to be one of the other 6 kinds of sets. Similarly, if $Z_p = \{n-1\}$ then n must be the last entry of p.

Next, suppose Z_p has two elements. We distinguish several possibilities here. If $Z_p = \{1, j\}$ for some j with $2 < j < n-1$, then n must be the first entry of p : n could not be the last entry in p because $n-1$ is not an element of Z_p and n could not occupy a position r with $1 < r < n$, since, as remarked above, in this eventuality the set Z_p would contain two consecutive integers.

If $Z_p = \{1, 2\}$ then n could not be in any position r in p with $r > 2$. This is clear for $r = n$, because $n-1$ is not an element of Z_p. If n were in position r for some r such that $2 < r < n$ then r would be an element of Z_p. This isn't possible, since $r > 2$. So n must be the first or second element of p. We have to show that one of these two positions is ruled out. Inspecting the elements of set $R(p)$, we determine in how many of these the entry $n-1$ is in the first position. Let s denote the number of elements of $R(p)$ in which the entry $n-1$ is in the first position. Note that $s \geq 1$.

If $s = 1$, then n must be in position 2 of p. To see this, we just need to show that it could not be in position 1 in p: if it were, then $n-1$ would be the first entry in every one of the reductions $p \downarrow i$, for $i < n$. Since $s = 1$, these reductions must all be equal to one another, which implies, by part (iii) of Lemma 1, that the last $n-1$ entries of p are either in consecutive increasing order or consecutive decreasing order. But $n-1$ could not be the last entry of p, because $n-1$ is not an element of Z_p, and $n-1$ could not be the second entry of p, because this would imply that $Z_p = \{1\}$.

Now suppose that $s > 1$. Now, let us show that n must be the first entry of p. To see this, we only need to show that n could not be the second entry of p. Suppose it was. Well, then $n-1$ could not be the first entry of p: if $p = n-1, n, p_3, \ldots$ then, for any $i \notin \{n-1, n\}$, $n-1$ is not the first entry of $p \downarrow i$, and so the only elements of $R(p)$ in which $n-1$ is the first entry are $p \downarrow n$ and $p \downarrow n-1$. But $p \downarrow n = p \downarrow n-1$, since n and $n-1$ are consecutive in p. So there is only one element of $R(p)$ with this property. This is contrary to $s > 1$. So the first entry of p would be some integer m with $m \neq n-1$. But then the only integer i for which $n-1$ is the first entry of $p \downarrow i$ is $i = m$, which is again contrary to $s > 1$.

By applying the preceding arguments to p^{opp} we see that the position of n in p is also determined when Z_p is $\{j, n-1\}$ for some j such that $1 < j < n-2$ and when $Z_p = \{n-2, n-1\}$.

Let us next consider the case when $Z_p = \{1, n-1\}$. In this case, n cannot occupy any position r in p for which $1 < r < n$, since the set Z_p does not contain two consecutive integers $r, r-1$. So n is either the first or last entry of p. This accounts for one element of the set Z_p. The second element of Z_p is the position of $n-1$ in $p \downarrow n = p - n$. So, in order to have $Z_p = \{1, n-1\}$, we must either have n first in p and $n-1$ last in p, or vice-versa. We need to show that one of these(and therefore the position of n in p) is determined by the set $R(p)$. Clearly $|R(p)| \geq 2$. If $|R(p)| > 2$ then either there are 2 elements of $R(p)$ in which $n-1$ is the first entry or 2 elements of $R(p)$ in which $n-1$ is the last entry. If it is the former, then n must be the first entry of p: the only other possibility is to have $n-1$ first and n last in p. But this would imply that the only element of the set $R(p)$ in which $n-1$ is the first entry is $p \downarrow n$, contrary to our assumption that two such elements exist. Similarly, if there are 2 elements of the set $R(p)$ in which $n-1$ is the last entry then n must be the last entry of p.

On the other hand, what if $|R(p)| = 2$? In this case, Lemma 1(v) implies that $n-2$ consecutive pairs of integers occur in the permutation. We know that $\{n-1, n\}$ is not one of these pairs, and so the integers $\{1, 2, ..., n-1\}$ must all be consecutive. So p must be either $n, 1, 2, 3, ..., n-1$ or $n-1, n-2, ..., 3, 2, 1, n$. We can easily determine which(and therefore the position of n) from the set $R(p)$: if $R(p)$ has an element in which the entry $n-2$ is last, then p must be $n, 1, 2, 3, ..., n-1$.

The last remaining possibility to consider when Z_p is a two-element set is when $Z_p = \{r-1, r\}$ for some r such that $2 < r < n-1$. In this case, n must be in position r in p. For any position other than r, it is clear that Z_p would be a set different from $\{r-1, r\}$.

Finally, we consider the case when Z_p is a three-element set. As we saw above, in this case we have $Z_p = \{j, r-1, r\}$ for some r with $1 < r < n$ and for some j distinct from both r and $r-1$. Here r is the position of n in p and j is either the position of $n-1$ in p (when $n-1$ is to the left of n in p), or one less than that position (when $n-1$ is to the right of n in p). So Z_p is a three-element set which contains two consecutive integers and a third integer which may or may not be consecutive with the other two. If Z_p does *not* consist of three consecutive integers, then the position of n in p is easily determined: it is the larger of the two consecutive integers in Z_p. So let us assume that $Z_p = \{i-1, i, i+1\}$ for some integer i. The position of n in p must either be i or $i+1$. We need to show that one of these is determined by the set $R(p)$. If the position of n is i, p would have the form

(1) $\cdots, x, n, y, n-1, \cdots$

If the position of n is $i+1$, p would have the form

(2) $\cdots, n-1, x, n, y, \cdots$

In both cases the displayed elements denote four distinct, consecutive elements of p.

In **(1)**, there are at most two elements in the set $R(p)$ in which $n-2$ is to the left of $n-1$, possibly $p \downarrow n$ and $p \downarrow n-1$. Similarly, in **(2)**, there are at most two elements in the set $R(p)$ in which $n-2$ is to the right of $n-1$. So, if we inspect the set $R(p)$ and find there are at least 3 elements in $R(p)$ in which $n-2$ is to the left of $n-1$, the position of n in p is determined to be $i+1$, the largest element of Z_p. And if we inspect the set $R(p)$ and find there are at least 3 elements in $R(p)$ in which $n-2$ is to the right of $n-1$, the position of n in p is determined to be i, the middle element of Z_p. If $|R(p)| > 4$, one of these two will apply by the pigeonhole principle. So we may assume that $|R(p)| \leq 4$. Now $|R(p)| \geq 3$, since $|Z_p| = 3$. Therefore either $|R(p)| = 3$ or $|R(p)| = 4$.

If $|R(p)| = 3$ then in **(1)** we must have $y = n-2$, since otherwise the four reductions $p \downarrow x, p \downarrow n, p \downarrow y, p \downarrow n-1$ would be four distinct elements of $R(p)$ by part (iii) of Lemma 1. Similarly, in **(2)**, we would have $x = n-2$. So we need to see that, in this case, the set $R(p)$ distinguishes between
(1′) $\cdots, x, n, n-2, n-1, \cdots$ and

(2′) $\cdots, n-1, n-2, n, y, \cdots$

In **(1′)**, in two of the three elements of $R(p)$ we have $n-1$ to the left of $n-2$ ($p \downarrow x$ and $p \downarrow n-2$), whereas in **(2′)**, in two of the three elements of $R(p)$ we have $n-1$ to the right of $n-2$ ($p \downarrow y$ and $p \downarrow n-2$). So $R(p)$ determines the position of n accordingly.

Finally, we consider the case when $|R(p)| = 4$. As noted above, if $R(p)$ has three elements having $n-1$ and $n-2$ in the same relative order, then the position of n can be determined. So we may as well suppose that $n-1$ is to the left of $n-2$ in two of the elements of $R(p)$, and to the right of $n-2$ in the other two elements of $R(p)$. This implies that **(1)** above could only occur with $y \neq n-2$. For, if y were equal to $n-2$, then $p \downarrow n$ would be the one and only element of $R(p)$ in which $n-1$ is to the right of $n-2$. Similarly, **(2)** above can occur only with $x \neq n-2$. Thus we have either
(1) $\cdots, x, n, y, n-1, \cdots$ with $y \neq n-2$, or

(2) $\cdots, n-1, x, n, y, \cdots$ with $x \neq n-2$.

Since $R(p)$ has exactly 4 elements, in both cases we have $R(p) = \{p \downarrow x, p \downarrow n, p \downarrow y, p \downarrow n-1\}$. Reading from left to right, the positions occupied by $n-1$ in each of these four elements of $R(p)$ are $i-1, i+1, i, i$ in **(1)** and $i, i-1, i+1, i$. Note that $n-1$ has the smallest position only once, and the largest position only once.

In **(1)** the two elements of $R(p)$ where $n-1$ is to the right of $n-2$ must be $p \downarrow n$ and $p \downarrow n-1$. Since $y \neq n-2$, this implies that $n-2$ must be to the left of n. Now, since $|R(p)| = 4$, Lemma 1(v) implies that p consists of 4 segments of consecutive integers. Since we know that n, y and $n-1$ are not adjacent to any integers consecutive to themselves, these individual integers constitute 3 of the segments. Thus the remaining integers are consecutive and y must be 1. It follows that there are two configurations possible for p in **(1)**:

(1a) $[2,3,\cdots,n-2,n,1,n-1]$ or **(1b)** $[n-2,n-3,\cdots,2,n,1,n-1]$

In a similar way we see there are two configurations possible for p in **(2)**:

(2a) $[n-1,1,n,2,3,\cdots,n-2]$ or **(2b)** $[n-1,1,n,n-2,n-3,\cdots,2]$.

We only need to show that $R(p)$ distinguishes **(1)** from **(2)**. To see this, note that, since $n > 4$, $n-1$ could never occur as the first entry in any of the elements of $R(p)$ if **(1a)** or **(1b)** applied, whereas it clearly does in both **(2a)** and **(2b)**. So in this case, we simply check whether 1 does or does not belong to Z_p. □

Lemma 3. Let $n \geq 3$ and let p and q be elements of S_n. Let $p' = p - n$ and let $q' = q - n$. If $R(p) = R(q)$ then $R(p') = R(q')$.

Proof: Using formula (vi) of Lemma 1 we have
$R(p') = \{t \in S_{n-2} : t = p' \downarrow i \text{ for some } i \leq n-1\}$
$= \{t \in S_{n-2} : t = (p \downarrow n) \downarrow i \text{ for some } i \leq n-1\}$
$= \{t \in S_{n-2} : t = (p \downarrow i) \downarrow n-1 \text{ for some } i \leq n-1\}$.
Since (again using formula (vi) in Lemma 1) $p \downarrow n \downarrow n-1 = p \downarrow n-1 \downarrow n-1$, we have
$R(p') = \{t \in S_{n-2} : t = (p \downarrow i) \downarrow n-1 \text{ for some } i \leq n\}$
$= \{t \in S_{n-2} : t = s \downarrow n-1 \text{ for some } s \in R(p)\}$
$= \{t \in S_{n-2} : t = s \downarrow n-1 \text{ for some } s \in R(q)\} = R(q')$. □

Lemma 4. Let p and q be elements of S_5 such that $R(p) = R(q)$. Then $p = q$.

Proof: One can, of course, execute a simple computer program to verify this statement, which we have done using GAP[3]. We can also argue directly. First of all, by Lemma 2, we can assume that 5 occurs in the same position in p and q. And secondly, by (i) of Lemma 1, we can assume that this common position is either first, second or third. Similar arguments can be made in all three cases. We will include the details for the first two of these cases and leave the third to the reader.

In the first case, we would have $p = 5p_2p_3p_4p_5$ and $q = 5q_2q_3q_4q_5$, and $R(p) = R(q)$. This implies that $p_2p_3p_4p_5 \in R(q)$ and so $p_2p_3p_4p_5 = q \downarrow i$ for some $i \leq 5$. If this occurs for $i = 5$ we are done. So we can suppose $i \neq 5$. This implies that $q \downarrow i$ begins with 4 and so $p_2 = 4$. Thus $p = 54p_3p_4p_5$.

So every element of $R(p)$ begins with 4. Since the same must be true for $R(q)$, we see that $q_2 = 4$, and so $q = 54q_3q_4q_5$. If $4p_3p_4p_5$ is equal to $q \downarrow i$ for $i = 4$ or $i = 5$, this would clearly imply that $p = q$, so we can suppose that $4p_3p_4p_5 = q \downarrow i$ for some $i \leq 3$. But, for any $i \leq 3$, the first two entries of $q \downarrow i$ are 43, and so this implies that $p_3 = 3$, and so $p = 543p_4p_5$. This implies that every element of $R(p)$ begins with 43. Since the same must be true of the elements in $R(q)$, we must also have $q_3 = 3$. Thus $q = 543q_4q_5$. Finally, since $R(54321) \neq R(54312)$, we infer that $p = q$.

In the second case, we would have $p = p_15p_3p_4p_5$ and $q = q_15q_3q_4q_5$, and $R(p) = R(q)$. As in the first case, we can assume that $p_1p_3p_4p_5 = q \downarrow i$ for some $i \neq 5$. For any such i, either the first or second element of $q \downarrow i$ is 4, so either $p_1 = 4$ or $p_3 = 4$. We consider two subcases:

(i) $p = 45p_3p_4p_5$, and (ii) $p = p_154p_4p_5$.

In subcase (i), every element of $R(p)$ begins with either 3 or 4, so the same holds for the elements of $R(q)$. Therefore we must have $q_1 = 4$, and so $q = 45q_3q_4q_5$. Now we have $4p_3p_4p_5 = q \downarrow i$ for some i. Since $q \downarrow i$ does not begin with 4 for $i < 4$, we must have $4p_3p_4p_5 = q \downarrow i$ for $i = 4$ or 5. This implies that $p = q$. In the second subcase, $p = p_154p_4p_5$. We cannot have $q_1 = 4$, because this would imply that every element of $R(q)$ begins with 4 or 3, which is clearly not the case for all elements of $R(p)$. Now $R(p)$ has an element which begins 43. Therefore $R(q)$ does too, and, since $q_1 \neq 4$, this implies that $q_3 = 4$. Thus $q = q_154q_4q_5$. Now we must have $p_14p_4p_5 = q \downarrow i$ for some i. If $i = 4$ or 5, this implies $p = q$ as desired. Clearly $p_14p_4p_5 \neq q \downarrow q_1$, and so either $p_14p_4p_5 = q \downarrow q_4$ or $p_14p_4p_5 = q \downarrow q_5$. Either way, we must have $p_4 = 3$. Thus $p = p_1543p_5$. This implies that, in every element of $R(p)$, 3 is either second or third. Therefore the same is true of the elements of $R(q)$. This implies that 3 cannot be the first or the last element of q, and so $q_4 = 3$. Thus $q = q_1543q_5$. And since $R(15432) \neq R(25431)$, we infer that $p = q$. □

Our theorem now follows directly from the preceding lemmas by induction on n.

Theorem. Let $n \geq 5$. Then any $p \in S_n$ is determined by its set of reductions $R(p)$. Equivalently, if p and q are elements of S_n and $R(p) = R(q)$, then $p = q$.

The proof of our theorem leads to a straightforward recursive procedure for reconstructing a permutation p from its set of reductions $R(p)$. At the bottom, we tabulate the 120 different sets $R(p)$ corresponding to the elements p in S_5. The GAP program [3] is very well-suited to this task.

For any $n > 5$, if we are given the set $R(p)$ for some $p \in S_n$, we first apply the method used in the proof of Lemma 2 to find the position of n in p. Then, as in the proof of Lemma 3, letting $q = p - n$, we find the set $R(q) = R(p - n) = \{t \in S_{n-2} : t = s \downarrow n - 1 \text{ for some } s \in R(p)\}$. From this set we reconstruct q. We then insert n into q so that it occupies the position it must occupy.

Example. Here is an illustration for $n = 7$. Suppose we are given that the set of reductions for p is $R = \{536412, 542631, 543612, 546312, 653412\}$. The set of positions of $n - 1 = 6$ in the reductions is then $Z_p = \{1, 3, 4\}$. Since the three elements in Z_p are not all consecutive, the proof of Lemma 2 shows that the position of 7 in p must be the larger of the consecutive pair in Z_p, namely 4. We now let q be $p - 7$. The set of reductions of q is the set $\{t \in S_5 : t = s \downarrow 6 \text{ for some } s \in R(p)\} = \{s - 6 : s \in R(p)\}$. So we simply delete 6 from each of the permutations belonging to R. We get the set $R' = \{54231, 53412, 54312\}$. To find the position of the entry 6 in q, we apply the method in the proof of Lemma 2 to the set R'. The set of positions of $6 - 1 = 5$ in the reductions belonging to R' is $Z_q = \{1\}$. Thus (as in the proof of Lemma 2) 6 must be the first entry of q. Now, let $r = q - 6$. The set of reductions of r is found simply by deleting 5 from each of the permutations belonging to R'. We get the set $R'' = \{3412, 4231, 4312\}$. From the example at the beginning of this paper, r is given by $r = 53412$. We insert 6 into r to form q so that 6 is the first entry. We get $q = 653412$. Finally, we insert 7 into q to find p, so that 7 is the fourth entry. We get $p = 6537412$. □

To conclude, we would like to suggest two possible directions for future work related to our theorem. In recent work on reconstructing an n-sequence s from its multiset of k-subsequences, significant progress has been made in finding a function $f(n)$, having as small an order as possible, so that s can be reconstructed from its k-subsequences as long as $k \geq f(n)$. We refer the reader to [2], [6] and [8]. Analogously, it would be interesting to know how many reductions of a permutation are needed to reconstruct it. Can we find a non-trivial function $f(n)$ so that, for n sufficiently large, if I is any subset of $\{1, 2, ..., n\}$ with $|I| \geq f(n)$, then any permutation p in S_n can be reconstructed from the set of reductions relative to I, that is, from the set $R^I(p) = \{q \in S_{n-1} : q = p \downarrow i \text{ for some } i \in I\}$? We have made no useful progress on this question.

Secondly, one can consider variations on the notion of "reduction". After one entry i of a permutation on $\{1, 2, ..., n\}$ is deleted from it, there are many natural ways to view the result as a permutation on $\{1, 2, ..., n - 1\}$.

Instead of reducing by 1, in place, all entries of p which are larger than i, we could instead, for $i \neq n$, replace the entry n by i. This gives another type of "reduction", and one can again consider the set of all such reductions over all $i \leq n$. Can p be reconstructed from this set of reductions? A more general inquiry may be useful. One might attempt to define a general notion of "reduction" along the following lines. Let P_{n-1} denote the set of all $n-1$-permutations of the n-element set $\{1, 2, ..., n\}$. For any $p \in S_n$ and $i \leq n$, let $p - i$ be the element of P_{n-1} obtained by deleting i from p. Then any function $F : P_{n-1} \longrightarrow S_{n-1}$ gives rise to a type of "reduction set" for p, namely the set $R_F(p) = \{F(p - i) : i = 1, 2, ..., n\}$. Is there a large, natural class of functions F for which p can always be reconstructed from $R_F(p)$?

References

1. J.A.Bondy and R.L.Hemminger, Graph reconstruction - a survey, Journ. Graph Theory 1, (1977), 227-268.

2. M.Dudik and L.Schulman, Reconstruction from subsequences, Journ. Comb. Theory A, 103, (2003), No. 2, 337-348.

3. GAP, The GAP Group, GAP – Groups, Algorithms and Programming, Version 4.2 ; Aachen, St. Andrews, 1999.

4. J.Ginsburg, A coloring problem on chordal rings, Ars Combinatoria 45(1997), 109-127.

5. J.Ginsburg and B.Sands, On the number of elements dominated by a subgroup, Ars Combinatoria 74(2005), 103-127.

6. I.Krasikov and Y.Roditty, On a reconstruction problem for sequences, Journ. Comb. Theory A, 77, (1997), No. 2, 344-348.

7. V.I.Levenshtein, On perfect codes in deletion and insertion metric, Discrete Math. Appl. Vol.2, No.3(1992), 241-258.

8. V.I.Levenshtein, Efficient reconstruction of sequences from their subsequences or supersequences, Journ. Comb. Theory A, 93,(2001), No. 2, 310-332.

9. L.Pebody, A.J. Radcliffe and A.D. Scott, Finite subsets of the plane are 18 reconstructible, SIAM Journal of Discrete Math. 16 (2003), No. 2, 262-275.

10. B.Sands, Reconstruction of Partially Ordered Sets, Order Vol. 1 (1985), 311-313.

11. D.Stanton and D.White, Constructive Combinatorics, Springer-Verlag New York Inc.,1986.

Department of Mathematics and Statistics
University of Winnipeg, Winnipeg, Canada, R3B2E9.
j.ginsburg@uwinnipeg.ca