Chapter 10. Inductive Foundation

The foundation for the inductive algorithms which handle large permutation groups is a chain of stabilisers. A chain of stabilisers is represented by a base and strong generating set. The information required to go from one stabiliser to the next is contained in a Schreier vector for the stabiliser.

This chapter defines the above concepts and presents algorithms for the fundamental operations which use a base and strong generating set.

Definitions

Let G be a permutation group acting on the points Ω. Let $\beta \in \Omega$ be any point. We define the *stabiliser of* β *in* G by

$$G_\beta = \{ g \in G \mid \beta^g = \beta \},$$

the set of elements in G which fix or stabilise the point β. This set is a *subgroup*.

For example, in the symmetries of the square acting on {1,2,3,4} the stabiliser of the point 2 is G_2 = {*elt*[1]=/1 2 3 4/, *elt*[7]=/3 2 1 4/=(1,3)}.

The index $|G:G_\beta|$ of the stabiliser is the size of the orbit β^G. For each point $\gamma \in \beta^G$, the set of elements

$$\{ g \in G \mid \beta^g = \gamma \}$$

is a (right) coset of the stabiliser G_β in G. If v is a Schreier vector of the orbit β^G, then *trace* (γ, v) is a representative of this coset. Thus,

$$\{ \mathit{trace}\,(\gamma, v) \mid \gamma \in \beta^G \}$$

is a *set of coset representatives* of G_β in G.

For example, in the symmetries of the square {*elt*[4]=(1,2,3,4), *elt*[8]=(1,4)(2,3)} is the set of elements that map the point 2 to the point 3. Hence, it is a coset of G_2. As a set of coset representatives we could take {*elt*[1], *elt*[2], *elt*[3], *elt*[4]} since this set contains precisely one element mapping the point 2 to each point in {1,2,3,4}, the orbit of 2 under G.

We have demonstrated the one-to-one correspondence between the cosets of the stabiliser G_β in G and the points of the orbit β^G. Note that

$$\{ g \in G \mid \beta^g = \gamma \} \;=\; G_\beta \times \mathit{trace}\,(\gamma, v).$$

Since G_β is a subgroup, we can iterate the process of defining stabilisers and consider a stabiliser in G_β. That is, a subgroup of G of the elements which stabilise two points. In the general case, we define the stabiliser

$$\begin{aligned} G_{\beta_1, \beta_2, \ldots, \beta_i} &= \text{stabiliser of } \beta_i \text{ in } G_{\beta_1, \beta_2, \ldots, \beta_{i-1}} \\ &= \left[G_{\beta_1, \beta_2, \ldots, \beta_{i-1}} \right]_{\beta_i} \\ &= \{ g \in G_{\beta_1, \beta_2, \ldots, \beta_{i-1}} \mid g \text{ fixes } \beta_i \} \\ &= \{ g \in G \mid g \text{ fixes each of } \beta_1, \beta_2, \ldots, \beta_i \}. \end{aligned}$$

Hence, there is a one-to-one correspondence between the points in the orbit of β_i under $G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}$ and the cosets of $G_{\beta_1, \beta_2, \ldots, \beta_i}$ in $G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}$. That is,

$$| G_{\beta_1, \beta_2, \ldots, \beta_{i-1}} : G_{\beta_1, \beta_2, \ldots, \beta_i} | = | \beta_i^{G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}} |.$$

If $v^{(i)}$ is a Schreier vector of the orbit then

$$\{ \; trace(\gamma, v^{(i)}) \mid \gamma \in \beta_i^{G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}} \; \}$$

is a set of coset representatives of $G_{\beta_1, \beta_2, \ldots, \beta_i}$ in $G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}$.

For example, in the symmetries of the square the stabiliser $G_{2,3}$ is the subgroup of G_2 which fixes 3. This is just the identity subgroup. The set of coset representatives of the identity subgroup in G_2 is $\{elt[1], elt[7]\}$. These elements map 3 to 3 and 1 respectively, and these two points are precisely the points in the orbit 3^{G_2}.

Eventually, we will stabilise so many points that the only element in the stabiliser is the identity element. This will give us a *chain of stabilisers*

$$\{identity\} = G_{\beta_1, \beta_2, \ldots, \beta_k} \leq G_{\beta_1, \beta_2, \ldots, \beta_{k-1}} \leq \cdots \leq G_{\beta_1} \leq G.$$

A sequence B of points $[\beta_1, \beta_2, \ldots, \beta_k]$ is called a *base* for G if the corresponding stabiliser chain does terminate with the identity subgroup. That is, the only element of the group G which fixes each of the points $\beta_1, \beta_2, \ldots, \beta_k$ is the identity.

For the example of the symmetries of the square we have shown that [2,3] is a base.

One useful property of a base is that an element g of the group G is uniquely determined by the sequence $\beta_1^g, \beta_2^g, \ldots, \beta_k^g$ (called the *base image* of g).

For example, the element $elt[6]$ of the symmetries of the square is the unique element which maps the base [2,3] to [1,4] respectively.

To "know" each of the stabilisers in the chain we at least need generators for each of them. A subset S of the group G is called a *strong generating set* of G relative to the base B if S contains generators for each stabiliser in the chain.

For example, the set $\{elt[2], elt[7]\}$ is a strong generating set of the symmetries of the square relative to the base [2,3].

Associated with a base and strong generating set are the various stabilisers, orbits, Schreier vectors, and sets of coset representatives. The notation we will use follows.

The stabilisers in the chain are denoted by

$$G^{(i)} = G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}$$

for $1 \le i \le k+1$. So, in particular, $G^{(1)} = G$ and $G^{(k+1)} = \{identity\}$.

The stabiliser $G^{(i)}$ is generated by

$$S^{(i)} = S \cap G^{(i)}$$

for $1 \le i \le k+1$.

The *basic orbit* of the stabiliser is

$$\Delta^{(i)} = \beta_i^{G^{(i)}}$$

for $1 \le i \le k$. The sizes of the orbits are called the *basic indices*, since $|\Delta^{(i)}|$ is the index of $G^{(i+1)}$ in $G^{(i)}$.

The Schreier vector of the basic orbit $\Delta^{(i)}$ with respect to the generators $S^{(i)}$ is denoted $v^{(i)}$.

A fixed set of coset representatives of $G^{(i+1)}$ in $G^{(i)}$ is denoted $U^{(i)}$ and is called a *basic transversal*. For example, the set

$$\{ \ trace(\gamma, v^{(i)}) \ | \ \gamma \in \Delta^{(i)} \ \}.$$

Examples

This section illustrates the concepts of base and strong generating set through examples. The examples range from the most elementary to large imprimitive groups. Indeed, we have tried to include as wide a range as possible so as not to reinforce some erroneous notion of a "typical" base and strong generating set.

The first group is the symmetries of the square. The group has degree 4 and is generated by

a=(1,2,3,4), and
b=(2,4).

It has order $8=2^3$. A base for the group is

[1, 2]

and a strong generating set relative to this base is

$s_1=a$, and
$s_2=b$.

The stabilisers are

$G=G^{(1)}=<a, b>$, and
$G_1=G^{(2)}=<b>$

and the coset representatives may be taken to be

$U^{(1)}=\{id, a, a^2, a^3\}$, and
$U^{(2)}=\{id, b\}$.

The Schreier vectors are

	1	2	3	4
$v^{(1)}$	0	a	a	a
$v^{(2)}$	0	0	0	b

The second group is the symmetries of the projective plane of order two. The group has degree 7 and is generated by

a=(1,2,4,5,7,3,6), and
b=(2,4)(3,5).

It has order $168=2^3 \times 3 \times 7$. A base for the group is

[1, 2, 4]

and a strong generating set relative to this base is

$s_1=a$,
$s_2=b$,
s_3=(4,5)(6,7), and
s_4 =(4,6)(5,7).

The stabilisers are

$G=G^{(1)}=<a, b>$,
$G_1=G^{(2)}=<b, s_3, s_4>$, and
$G_{1,2}=G^{(3)}=<s_3, s_4>$

and the coset representatives may be taken to be

$U^{(1)}=\{id, a, a^2, a^3, a^4, a^5, a^6\}$,
$U^{(2)}=\{id, b, b \times s_3, b \times s_4, b \times s_3 \times b, b \times s_3 \times s_4\}$, and
$U^{(3)}=\{id, s_3, s_4, s_3 \times s_4\}$.

The Schreier vectors are

	1	2	3	4	5	6	7
$v^{(1)}$	0	a	a	a	a	a	a
$v^{(2)}$	0	0	b	b	s_3	s_4	s_4
$v^{(3)}$	0	0	0	0	s_3	s_4	s_4

The third group was discovered by the French mathematician Mathieu. The group has degree 11. A base for the group is

[11, 10, 1, 2]

and a strong generating set relative to this base is

s_1=(1,2,3)(4,5,6)(7,8,9),
s_2=(2,4,3,7)(5,6,9,8),
s_3=(2,5,3,9)(4,8,7,6),
s_4=(1,10)(4,5)(6,8)(7,9), and
s_5=(1,11)(4,6)(5,9)(7,8).

It has order 7,920=$2^4 \times 3^2 \times 5 \times 11$.

The Schreier vectors are

	1	2	3	4	5	6	7	8	9	10	11
$v^{(1)}$	s_5	s_1	s_1	s_2	s_3	s_1	s_2	s_3	s_3	s_4	0
$v^{(2)}$	s_4	s_1	s_1	s_2	s_3	s_1	s_2	s_3	s_3	0	0
$v^{(3)}$	0	s_1	s_1	s_2	s_3	s_1	s_2	s_3	s_3	0	0
$v^{(4)}$	0	0	s_2	s_2	s_3	s_2	s_2	s_3	s_3	0	0

The fourth group has degree 21 and is generated by

a=(1,8,9)(2,11,15)(3,10,12)(4,14,19)(5,16,17)(6,21,20)(7,13,18),
b=(9,18,20)(12,19,17), and
c=(10,21,11)(13,16,14).

It has order 27,783=$3^4 \times 7^3$. A base for the group is

[1, 9, 8, 10, 2, 12]

and a strong generating set relative to this base is

s_1=a,
s_2=b,
s_3=c,
s_4=(8,13,21)(10,14,16),
s_5=(2,6,3)(4,5,7), and
s_6=(12,20,15)(17,19,18).

The Schreier vectors are

	1	2	3	4	5	6	7	8	9	10	11
$v^{(1)}$	0	a	s_5	a	a	s_5	a	a	a	s_4	c
$v^{(2)}$	0	0	0	0	0	0	0	0	0	0	0
$v^{(3)}$	0	0	0	0	0	0	0	0	0	s_4	c
$v^{(4)}$	0	0	0	0	0	0	0	0	0	0	c
$v^{(5)}$	0	0	s_5	0	0	s_5	0	0	0	0	0
$v^{(6)}$	0	0	0	0	0	0	0	0	0	0	0

12	13	14	15	16	17	18	19	20	21
b	s_4	c	s_6	c	s_6	b	s_6	b	s_4
b	0	0	s_6	0	s_6	b	s_6	b	0
0	s_4	c	0	c	0	0	0	0	s_4
0	0	0	0	0	0	0	0	0	c
0	0	0	0	0	0	0	0	0	0
0	0	0	s_6	0	0	0	0	s_6	0

The fifth group is the set of all operations of Rubik's cube. The group has degree 48 and is generated by

a=(1,3,8,6)(2,5,7,4)(9,48,15,12)(10,47,16,13)(11,46,17,14),
b=(6,15,35,26)(7,22,34,19)(8,30,33,11)(12,14,29,27)(13,21,28,20),
c=(1,12,33,41)(4,20,36,44)(6,27,38,46)(9,11,26,24)(10,19,25,18),
d=(1,24,40,17)(2,18,39,23)(3,9,38,32)(41,43,48,46)(42,45,47,44),
e=(3,43,35,14)(5,45,37,21)(8,48,40,29)(15,17,32,30)(16,23,31,22), and
f=(24,27,30,43)(25,28,31,42)(26,29,32,41)(33,35,40,38)(34,37,39,36).

The group has order

$$2^{27}3^{14}5^{3}7^{2}11 = 43\ 252\ 003\ 274\ 489\ 856\ 000.$$

A base for the group is

[1, 6, 3, 8, 21, 23, 26, 5, 29, 19, 7, 24, 25, 28, 31, 18, 4, 2]

and a strong generating set relative to this base is

$s_1=a$,
$s_2=b$,
$s_3=e$,
s_4=(5,37,28,21)(8,26,29,32)(14,33,35,40)(15,27,30,43)(16,31,34,22),
s_5=(5,45,13,37,21)(7,31,22,16,23)(26,27,33)(29,35,30),
s_6=(19,23,34)(20,45,28),
$s_7=f$,
s_8=(5,28,37)(16,34,31),
s_9=(2,28,47,34)(24,41,38)(25,39,31,36,42,37)(29,43,30,40,35,32),
s_{10}=(19,31,34)(20,37,28),
s_{11}=(7,31,34)(13,37,28),
s_{12}=(24,41,38)(32,43,40),
s_{13}=(24,40)(25,39,34,37)(28,31,36,42)(32,38)(41,43),
s_{14}=(25,28,31)(34,37,36),
s_{15}=(2,31,34)(28,47,37),
s_{16}=(2,31,39)(37,42,47),
s_{17}=(2,18,39)(42,47,44),
s_{18}=(2,10,39)(4,42,47), and
s_{19}=(2,47)(39,42).

The sixth group has degree 14 and is generated by

a=(1,2)(3,4)(5,6)(7,8)(9,10)(11,12), and
b=(1,13)(2,3,7,5)(6,9,11,8)(10,14).

The group is imprimitive. It has order $10{,}752 = 2^9 \times 3 \times 7$. A base for the group is

[1, 2, 3, 4, 7, 5]

and a strong generating set relative to this base is

$s_1=a$,
s_2=(2,7)(3,5)(6,11)(8,9),
s_3=(3,7,11,8)(4,14)(5,6)(12,13),
s_4=(3,13,11,14)(4,8)(5,6)(7,12),
s_5=(4,12)(13,14),
s_6=(7,8)(13,14), and
s_7=(5,6)(13,14).

The Schreier vectors are

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$v^{(1)}$	0	a	s_3	s_3	s_2	s_7	s_2	s_6	s_2	a	s_4	s_3	s_4	s_4
$v^{(2)}$	0	0	s_3	s_3	s_2	s_7	s_2	s_6	s_2	0	s_4	s_3	s_4	s_4
$v^{(3)}$	0	0	0	s_3	0	0	s_3	s_6	0	0	s_4	s_3	s_4	s_4
$v^{(4)}$	0	0	0	0	0	0	0	0	0	0	0	s_5	0	0
$v^{(5)}$	0	0	0	0	0	0	0	s_6	0	0	0	0	0	0
$v^{(6)}$	0	0	0	0	0	s_7	0	0	0	0	0	0	0	0

The seventh group has degree 16 and is generated by

a=(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16), and
b=(1,2,5,3)(4,7)(6,9)(8,11)(10,13,16,15)(12,14).

The group is imprimitive. It has order 21,504 = $2^{10} \times 3 \times 7$. A base for the group is

[1, 2, 3, 4]

and a strong generating set relative to this base is

s_1=a,
s_2=(3,14,10,6)(4,5,9,13)(7,11)(8,12),
s_3=(2,6,10,14,11,7,3)(4,8,12,13,15,9,5),
s_4=(4,12)(6,11)(7,14)(8,9), and
s_5=(4,8)(6,7)(9,12)(11,14).

The eighth group has degree 18 and is generated by

a=(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18), and
b=(1,2,5,3)(4,7)(6,9,12,11)(8,13,16,15)(10,14,18,17).

The group is imprimitive. It has order 508,032 = $2^7 \times 3^4 \times 7^2$. A base for the group is

[1, 2, 3, 4, 5, 6]

and a strong generating set relative to this base is

s_1=a,
s_2=(2,10)(3,6)(4,11)(5,17)(7,18)(8,14)(9,16)(12,13),
s_3=(3,15,7,10,6,18,13)(4,8)(5,9)(11,14)(16,17),
s_4=(4,16,5,8,14,11,17),
s_5=(5,14,8,16,11,17,9), and
s_6=(6,15,10,7,18,13,12).

The ninth group has degree 16 and is generated by

a=(1,15,7,5,12)(2,9,13,14,8)(3,6,10,11,4),
b=(1,7)(2,11)(3,12)(4,13)(5,10)(8,14), and
c=(1,16)(2,3)(4,5)(6,7)(8,9)(10,11)(12,13)(14,15).

The group is primitive. It has order 11,520=$2^8 \times 3^3 \times 5$. A base for the group is

[1, 2, 8, 3, 4]

and a strong generating set relative to this base is

s_1=a,
s_2=(2,4,6)(3,5,7)(8,9)(10,13,14,11,12,15),
s_3=(8,9)(10,11)(12,13)(14,15),
s_4=(3,12,14)(4,10,6,7,9,5)(8,11)(13,16,15),
s_5=(3,12,14)(4,9,6)(5,7,10)(13,16,15), and
s_6=(4,6)(5,7)(12,14)(13,15).

The tenth group has degree 31 and is generated by

a=(4,5)(6,8)(7,9)(10,12)(13,16)(15,19)(18,22)(20,24)
(23,27)(25,29)(26,30)(28,31), and
b=(1,2,3,4,6)(5,7,10,13,17)(8,11,14,18,23)
(9,12,15,20,25)(16,21,22,26,29)(19,24,28,31,27).

The group is primitive. It has order 9,999,360=$2^{10} \times 3^2 \times 5 \times 7 \times 31$. A base for the group is

[4, 2, 3, 1, 6]

and a strong generating set relative to this base is

s_1=*b*,
s_2=(2,13)(3,18)(5,25)(7,26)(9,31)(11,16)(12,27)(14,28)(15,22)
(17,20)(19,24)(21,30),
s_3=(1,8)(3,30,7,24)(9,28,17,22)(10,29)(11,16)(12,27)
(14,31,15,20)(18,19,26,21),
s_4=(1,29)(8,10)(9,20)(11,27)(12,16)(17,31)(19,24)(21,30),
s_5=(6,8)(7,9)(13,16)(15,19)(23,29)(25,27)(26,31)(28,30),
s_6=(6,29)(7,31)(8,23)(9,26)(13,27)(15,30)(16,25)(19,28),
s_7=(6,16)(7,19)(8,13)(9,15)(23,27)(25,29)(26,30)(28,31), and
s_8=(6,19)(7,16)(8,15)(9,13)(23,30)(25,31)(26,27)(28,29).

Representing Elements and Testing Membership

Let's look at some consequences of knowing a base and strong generating set (and the Schreier vectors).

Recall that the cosets of a subgroup partition a group. In our case, the subgroup is a stabiliser G_{β_1} of the group G. This partition means that each element of the group can be written as a product

$$h \times u$$

where u is a coset representative, and h is an element of the subgroup. Each product gives a distinct element of the group (provided we use a fixed set of coset representatives). In this case, it says that each element of the group G is uniquely represented as a product

$$h \times u_1$$

where $h \in G^{(2)}$ and $u_1 \in U^{(1)}$. Using induction, we see that each element of G is uniquely represented as a product

$$u_k \times u_{k-1} \times \cdots \times u_1 \tag{4.1}$$

where $u_i \in U^{(i)}$, for $1 \le i \le k$, the length of the base.

With the correspondence between the coset representatives and the orbits, we know that $|U^{(i)}| = |\Delta^{(i)}|$. Hence,

$$|G| = \prod_{i=1}^{k} |U^{(i)}| = \prod_{i=1}^{k} |\Delta^{(i)}|.$$

Not only do we get the order of the group, but (4.1) tells us how to get each and every element of the group. Note that the base image of the element in (4.1) is

$$\beta_1^{u_1}$$
$$\beta_2^{u_2 \times u_1}$$
$$\beta_3^{u_3 \times u_2 \times u_1}$$
$$\vdots$$
$$\beta_i^{u_i \times u_{i-1} \times \cdots \times u_1}$$
$$\vdots$$
$$\beta_k^{u_k \times u_{k-1} \times \cdots \times u_1}$$

since the element u_j fixes $\beta_1, \beta_2, \ldots, \beta_{j-1}$. This is a useful relationship between the unique representation of an element by its base image and the unique representation as a product (4.1) of coset representatives, especially when the coset representatives come from the Schreier vectors. We will use these representations of elements heavily in the next few algorithms. The algorithms solve some elementary but necessary tasks.

The first task is to test membership of an arbitrary permutation on Ω in the group G. Algorithm 1 attempts to find the coset representatives involved in the product (4.1). If the permutation is an element then the coset representatives will be found. If the permutation is not an element of the group then it will not be possible to find the coset representatives.

Algorithm 1 : Testing Membership

Input : a group G acting on $\Omega = \{1,2,\ldots,n\}$;
a permutation g of $\Omega = \{1,2,\ldots,n\}$;
a base and strong generating set for G;
sets $U^{(i)}, 1 \leq i \leq k$ of coset representatives for stabiliser chain;

Output : a boolean value *answer*, indicating whether $g \in G$;

```
function is_in_group( p : permutation; i : 1..k+1 ) : boolean;
(* return true if the permutation p is in the group G^(i) *)
begin
  if i = k+1 then
    result is p = id;
  else
    find u_i ∈ U^(i) such that β_i^(u_i) = β_i^p;
    if no such u_i exists then
      result is false;
    else
      result is is_in_group( p × u_i^-1, i+1 );
    end if;
  end if;
end;

begin
  answer := is_in_group( g, 1 );
end;
```

Algorithm 2 solves the same problem using the Schreier vectors to determine the coset representative.

Algorithm 2 : Testing Membership

Input : a group G acting on $\Omega = \{1,2,...,n\}$;
a permutation g of $\Omega = \{1,2,...,n\}$;
a base and strong generating set for G;
Schreier vectors $v^{(i)}, 1 \le i \le k$, for the stabiliser chain;

Output : a boolean value *answer*, indicating whether $g \in G$;

```
function is_in_group( p : permutation; i : 1..k+1 ) : boolean;
(* return true if the permutation p is in the group G^(i) *)
begin
  if i = k+1 then
    result is p = id;
  else
    if β_i^p ∈ Δ^(i) then
      result is is_in_group( p × trace ( β_i^p, v^(i) )^-1, i+1 );
    else
      result is false;
    end if;
  end if;
end;

begin
  answer := is_in_group( g, 1 );
end;
```

To analyse Algorithm 2, we note that the worst case cost of tracing $v^{(i)}$ is $2 \times |\Delta^{(i)}| \left\lceil |\Omega|+1 \right\rceil$ operations. We must also consider the $|\Omega|$ operations to test $p = id$; the operation to form the image of β_i under p; and the one operation to test membership of a point in $\Delta^{(i)}$. The total worst case cost is therefore

$$|\Omega| \times \left\lceil 1 + 2 \times k + 2 \times \sum_{i=1}^{k} |\Delta^{(i)}| \right\rceil + 2 \times k + 2 \times \sum_{i=1}^{k} |\Delta^{(i)}| \text{ operations.}$$

Algorithm 3 presents a non-recursive version of Algorithm 2. Similarly a non-recursive version of Algorithm 1 could be devised.

Algorithm 3 : Testing Membership

Input : a group G acting on $\Omega = \{1,2,...,n\}$;
a permutation g on $\Omega = \{1,2,...,n\}$;
a base and strong generating set for G;
Schreier vectors $v^{(i)}$, $1 \le i \le k$, for the stabiliser chain;

Output : a boolean value *answer*, indicating whether $g \in G$;

```
function is_in_group( p : permutation; i : 1..k+1 ) : boolean;
(* return true if the permutation p is in the group G^(i) *)
begin
  for j := i to k do
    if β_j^(p × u_i^-1 × u_(i+1)^-1 × ··· × u_(j-1)^-1) ∈ Δ^(j) then
      u_j := trace( β_j^(p × u_i^-1 × u_(i+1)^-1 × ··· × u_(j-1)^-1), v^(j) );
    else
      result is false;
    end if;
  end for;
  result is p = u_k × u_(k-1) × ··· × u_i;
end;

begin
  answer := is_in_group( g, 1 );
end;
```

We will consider some examples of testing membership. Let G be the symmetries of the projective plane of order two, as given earlier. Let p=(1,2,3,4,5,6,7). We wish to know whether $p \in G$? Using Algorithm 1, we find $u_1 = a$ is a coset representative that maps 1 to 2, which is the image of 2 under p. Therefore, we ask is $p \times {u_1}^{-1}$=(2,7,6,5,3) $\in G^{(2)}$? We find $u_2 = b \times s_3 \times s_4$ is a coset representative that maps 2 to 7, which is the image of 2 under $p \times {u_1}^{-1}$. Therefore, we ask is $p \times {u_1}^{-1} \times {u_2}^{-1}$=(3,4,7) $\in G^{(3)}$? We find $u_3 = s_3 \times s_4$ is a coset representative that maps 4 to 7, which is the image of 4 under $p \times {u_1}^{-1} \times {u_2}^{-1}$. Therefore, we ask is $p \times {u_1}^{-1} \times {u_2}^{-1} \times {u_3}^{-1}$ = (3,7)(5,6) $\in G^{(4)} = \{id\}$? The answer to this is clearly no, so $p \notin G$.

Let us consider the same group, but take p=(1,4,2,3,7,5,6). We will use Algorithm 2 to decide whether $p \in G$. We find that the image of 1 under p is 4, which is in $\Delta^{(1)}$, and that $trace(4, v^{(1)}) = a^2$. Therefore, we ask if $p \times trace(4, v^{(1)})^{-1}$ = (2,5,7)(3,4,6) $\in G^{(2)}$? We find that the image of 2 under $p \times trace(4, v^{(1)})^{-1}$ is 5, which is in $\Delta^{(2)}$, and that $trace(5, v^{(2)}) = b \times s_3$. Therefore, we ask if $p \times trace(4, v^{(1)})^{-1} \times trace(5, v^{(2)})^{-1}$ = (4,7)(5,6) $\in G^{(3)}$? We find that the image of 4 under $p \times trace(4, v^{(1)})^{-1} \times trace(5, v^{(2)})^{-1}$ is 7, which is in $\Delta^{(3)}$, and that $trace(7, v^{(3)}) = s_3 \times s_4$. Therefore, we ask if $p \times trace(4, v^{(1)})^{-1} \times trace(5, v^{(2)})^{-1} \times trace(7, v^{(3)})^{-1}$ = $id \in G^{(4)}$? The answer is clearly yes, so $p \in G$. Indeed, it tells us that $p = (s_3 \times s_4) \times (b \times s_3) \times (a^2)$.

The next task we wish to perform is to write an element of the group G as a product of strong generators. Again, we will attempt to write the element as a product of coset representatives. The Schreier vectors determine coset representatives as products of strong generators (and their inverses), so we will use the Schreier vectors. The procedure *trace* will be assumed to also return the element as a product of the strong generators. Since an element is determined by its base image, we will represent some elements in the algorithm by a base image $[\gamma_1, \gamma_2, ..., \gamma_k]$. The algorithm to perform the task is Algorithm 4.

Algorithm 4 : Element as Product of Strong Generators

Input : a group G acting on $\Omega = \{1,2,...,n\}$;
an element g of G;
a base and strong generating set for G;
Schreier vectors $v^{(i)}, 1 \le i \le k$, for the stabiliser chain;

Output : a symbolic product, *word*, expressing g in terms of the strong generators;
begin
$[\gamma_1, \gamma_2, ..., \gamma_k] := [\beta_1, \beta_2, ..., \beta_k]^g$;
word := ε; (*the empty word*)
for $i := 1$ **to** k **do**
$u_i := trace(\gamma_i, v^{(i)})$; (*$\gamma_i = \beta_i^{g \times u_1^{-1} \times u_2^{-1} \times \cdots \times u_{i-1}^{-1}}$*)
word := $u_i \times word$; (*regarding u_i as a word in $S^{(i)}$ *)
$[\gamma_1, \gamma_2, ..., \gamma_k] := [\gamma_1, \gamma_2, ..., \gamma_k]^{u_i^{-1}}$;
end for;
end;

We will now consider an example of Algorithm 4. Let G be the sixth group in our examples. We know that

$$g = a \times b = (1,3,4,7,6,2,13)(5,9,14,10,11,12,8)$$

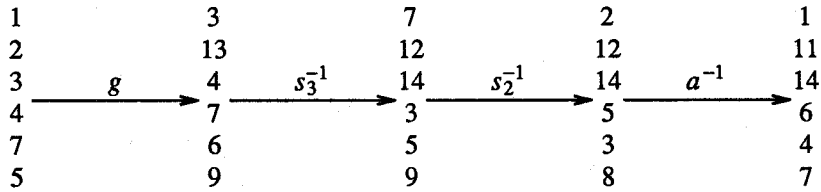
is an element of the group. Using Algorithm 4, we will express this element as a product of the strong generators. The base image of g is Figure 1.

Figure 1

1		3
2		13
3	g	4
4	$\longrightarrow$	7
7		6
5		9

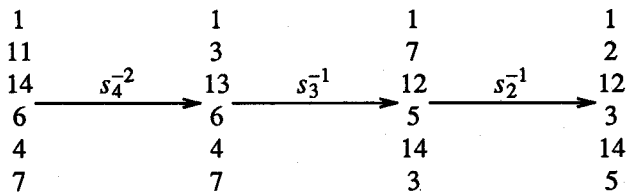
The element $trace(3, v^{(1)})$ is $a \times s_2 \times s_3$. The resulting base image $[\gamma_1, \gamma_2, ..., \gamma_k]$ is Figure 2.

Figure 2



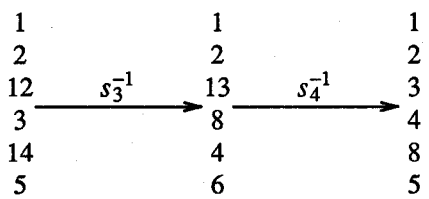
The element *trace* (11, $v^{(2)}$) is $s_2 \times s_3 \times s_4 \times s_4$. The resulting base image $[\gamma_1, \gamma_2, ..., \gamma_k]$ is Figure 3.

Figure 3



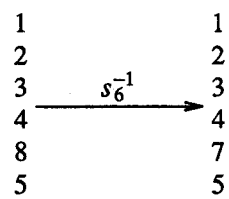
The element *trace* (12, $v^{(3)}$) is $s_4 \times s_3$. The resulting base image $[\gamma_1, \gamma_2, ..., \gamma_k]$ is Figure 4.

Figure 4



Therefore, *trace* (4, $v^{(4)}$) is the identity, leaving the base image unchanged. The element *trace* (8, $v^{(5)}$) is s_6, giving the base image in Figure 5.

Figure 5



Therefore, $trace(5, v^{(6)})$ is the identity, leaving the base image unchanged. Hence, the result is

$$g = (s_6) \times (s_4 \times s_3) \times (s_2 \times s_3 \times s_4^2) \times (a \times s_2 \times s_3).$$

Note, that the above example suggests an improvement in Algorithm 4. At no stage did we need the complete element $trace(\gamma_i, v^{(i)})$. We simply needed the coset representative as a word, and we needed its action on a certain sequence of points. This action could be calculated from the strong generators (and their inverses) as we determine the word. Thus, a major improvement to Algorithm 4 would be to modify *trace* to return a word, and the image of a sequence of points (rather than an element).

Note also that $\gamma_1, \gamma_2, ..., \gamma_{i-1}$ are fixed by $trace(\gamma_i, v^{(i)})$, since these are the base points. This fact could also be used to improve Algorithm 4.

The last task we wish to consider here is to determine the element with a given base image. Since the base image uniquely determines the element, this is a reasonable request. Again, we will use the Schreier vectors to determine the coset representatives. The algorithm is given as Algorithm 5.

Algorithm 5 : Element from a Base Image

Input : a group G acting on $\Omega = \{1,2,...,n\}$;
the base image $[\gamma_1, \gamma_2, ..., \gamma_k[$ of an element g of G;
a base and strong generating set for G;
Schreier vectors $v^{(i)}, 1 \le i \le k$, for the stabiliser chain;

Output : the element $g = u_k \times u_{k-1} \times \cdots \times u_1$;

begin
  $g := id$;
  for $i := 1$ **to** k **do**
    $u_i := trace(\gamma_i, v^{(i)})$;
    $g := u_i \times g$;
    $[\gamma_1, \gamma_2, ..., \gamma_k] := [\gamma_1, \gamma_2, ..., \gamma_k]^{u_i^{-1}}$;
  end for;
end;

Enumerating All Elements

In this section we present some straightforward algorithms for enumerating all the elements of a permutation group. We will consider two representations of an element - as a complete permutation, and as a base image. Both rely on essentially enumerating all the products of coset representatives.

Algorithm 6 sketches a non-recursive approach to enumerating all the elements as permutations. Later we will present a more precise recursive version.

Algorithm 6 : Enumerating All Elements

Input : a permutation group G;
a base and strong generating set for G;
the sets $U^{(i)}$, $1 \leq i \leq k$, of coset representatives of the stabiliser chain;

Output : the elements of the group G (without repetition);

begin

for each $u_1 \in U^{(1)}$ **do**
for each $u_2 \in U^{(2)}$ **do**
.
.
.
for each $u_k \in U^{(k)}$ **do**

$g := u_k \times u_{k-1} \times \cdots \times u_1$; (*next element of G*)

end for;
.
.
.
end for;
end for;

end;

Provided the identity is the "first" coset representative in each $U^{(i)}$, then Algorithm 6 enumerates the elements of $G^{(k)}$, then the elements of $G^{(k-1)} - G^{(k)}$, and so on until at last it enumerates the elements of $G^{(1)} - G^{(2)}$.

The next algorithm enumerates the base images of the elements. It is important to note that in the base image of $u_k \times u_{k-1} \times \cdots \times u_1$, the i-th point γ_i of the image is

$$\beta_i^{u_i \times u_{i-1} \times \cdots \times u_1}$$

The point $\beta_i^{u_i}$ runs over $\Delta^{(i)}$ as u_i varies, so the image point γ_i runs over

$$\left[\Delta^{(i)} \right]^{u_{i-1} \times u_{i-2} \times \cdots \times u_1}$$

With this explanation, we are ready to present Algorithm 7.

Algorithm 7 : Enumerating All Base Images

Input : a permutation group G;
a base and strong generating set for G;
the Schreier vectors $v^{(i)}$, $1 \leq i \leq k$, of the stabiliser chain;

Output : the base images of the elements of the group G (without repetition);

begin

for each $\gamma_1 \in \Delta^{(1)}$ **do**

$u_1 := trace(\gamma_1, v^{(1)})$;

for each $\gamma_2 \in \left[\Delta^{(2)}\right]^{u_1}$ **do**

$u_2 := trace(\gamma_2, v^{(2)})$;

.
.
.

for each $\gamma_k \in \left[\Delta^{(k)}\right]^{u_{k-1} \times u_{k-2} \times \cdots \times u_1}$ **do**

$image := [\gamma_1, \gamma_2, ..., \gamma_k]$; (*next base image*)

end for;

.
.
.

end for;

end for;

end;

These algorithms are perhaps more clearly presented recursively. This is done in Algorithm 8, which enumerates the base images, but is easily modified to enumerate the complete permutations.

Algorithm 8 : Enumerating All Base Images

Input : a permutation group G;
a base and strong generating set for G;
the Schreier vectors $v^{(i)}$, $1 \leq i \leq k$, of the stabiliser chain;

Output : the base images of the elements of the group G (without repetition);

```
procedure base_image( i : 1..k+1;
                      [ γ1, γ2, ..., γi−1 ] : sequence of points;
                      ui−1 × ui−2 × ··· × u1 : element          );
(*
  Enumerate all the base images which begin with [ γ1, γ2, ..., γi−1 ],
  where ui−1 × ui−2 × ··· × u1 is an element mapping
  the initial segment of the base to the given sequence.
*)
begin

  if i = k+1 then
    image := [ γ1, γ2, ..., γi−1 ];  (*next base image*)
  else
    g := ui−1 × ui−2 × ··· × u1;

    for each γi ∈ ⌊ Δ(i) ⌋^g do

      ui := trace( γi^(g^−1), v(i) );
      base_image( i+1, [ γ1, γ2, ..., γi ], ui × g );

    end for;

  end if;

end;

begin
  base_image( 1, empty sequence, id );
end;
```

Summary

This chapter has introduced the stabiliser chain, the inductive foundation of the powerful algorithms for handling large permutation groups. The representation of elements by their base image, and as a product of coset representatives is central to the power of these algorithms. They are applied here to the performance of the tasks of testing membership, writing elements as products of the strong generators, and the enumeration of all the elements of a group.

We have presented several examples. It is hoped the reader will use them in the study of these and later algorithms.

Exercises

(1/Easy) Give a base and strong generating set for the symmetric group of degree 4.

(2/Moderate) Let $G=\langle s \rangle$ be a cyclic group. Let $B = [\beta_1, \beta_2, ..., \beta_k]$ be a base for G. Devise an algorithm that determines a strong generating set of G relative to B.

(3/Difficult) Construct (perhaps using the definition of stabiliser and automorphism) a base and strong generating set of the automorphism group of Petersen's graph.

(4/Easy) Construct Schreier vectors for some, or all, of the examples for which they are not given.

(5/Moderate) Modify *trace* to return both a word in the strong generators for the coset representative, and the image under the coset representative of a sequence of points. The sequence of points is a parameter. Do not return an element.

Do the same for the inverse of the coset representative.

(6/Moderate) Modify Algorithm 5 so that, given a sequence $[\gamma_1, \gamma_2, ..., \gamma_{i-1}]$ of points, it determines whether or not there is an element of the group whose base image begins with $[\gamma_1, \gamma_2, ..., \gamma_{i-1}]$.

Bibliographical Remarks

The concept of a stabiliser, and the one-to-one correspondence between the cosets of a stabiliser and the orbit of the point being stabilised are old. They are discussed in H. Wielandt, **Finite Permutation Groups**, Academic Press, New York, 1964.

The use of a stabiliser chain and the sets $U^{(i)}$ of coset representatives to represent a permutation group are presented in C. C. Sims, *"Computational methods in the study of permutation groups"*, **Computational Problems in Abstract Algebra**, (Proceedings of a conference, Oxford, 1967), John Leech (editor), Pergamon, Oxford, 1970, 169-183. This paper also notes the unique representation of an element as a product of coset representatives, even though the base is assumed to be $[1,2,...,|\Omega|-1]$. The representation is used to test membership similarly to Algorithm 1.

The terms *base* and *strong generating set* are due to C. C. Sims, *"Determining the conjugacy classes of a permutation group"*, **Computers in Algebra and Number Theory** (Proceedings of the Symposium on Applied Mathematics, New York, 1970), G. Birkhoff and M. Hall, Jr (editors), SIAM-AMS Proceedings, volume 4, American Mathematics Society, Providence, Rhode Island, 1971, 191-195; and C. C. Sims, *"Computation with permutation groups"*, (Proceedings of the Second Symposium on Symbolic and Algebraic Manipulation, Los Angeles, 1971), S. R. Petrick (editor), Association of Computing Machinery, New York, 1971, 23-28. In these papers, a base is not necessarily $[1,2,...,|\Omega|-1]$; the representation of an element by its base image is noted; and the representation of an element as a product of coset representatives is generalized to its present form.

The use of Schreier vectors in testing membership comes from the Oxford lectures of Sims in January and February 1973.