London Mathematical Society ISSN 1461–1570

AN ALGORITHM FOR RECOGNISING THE EXTERIOR SQUARE OF A MULTISET

CATHERINE GREENHILL

Abstract

The exterior square of a multiset is a natural combinatorial construction which is related to the exterior square of a vector space. We consider multisets of elements of an abelian group. Two properties are defined which a multiset may satisfy: recognisability and involution-recognisability. A polynomial-time algorithm is described which takes an input multiset and returns either (a) a multiset which is either recognisable or involution-recognisable and whose exterior square equals the input multiset, or (b) the message that no such multiset exists. The proportion of multisets which are neither recognisable nor involution-recognisable is shown to be small when the abelian group is finite but large. Some further comments are made about the motivating case of multisets of eigenvalues of matrices.

1. *Introduction*

The exterior square of a vector space is a well-known and important construction, with applications in various areas of mathematics. In this paper the exterior square of a multiset is defined. This definition arises in a natural way, as it describes the relationship between the eigenvalues of a matrix X and the eigenvalues of the matrix representing the action of X on the exterior square of the underlying vector space. This relationship is fully determined by the nonzero eigenvalues, which belong to the multiplicative group of the splitting field of the characteristic polynomial of X. Therefore, the appropriate generalisation is to multisets of elements of an abelian group. For most of the paper we consider the problem in full generality.

Two properties are defined which a multiset may possess: the properties of recognisability and involution-recognisability. An algorithm is developed which can determine whether a given multiset is the exterior square of a recognisable or involution-recognisable multiset. This strategy is adapted from that used by Peter Neumann and Cheryl Praeger in their work on the tensor products of multisets [**6**].

The worst-case complexity of the algorithm is analysed, under the assumption that the elements of the abelian group can be linearly ordered. Let m, n be positive integers such that $m \geqslant 2$ and $n = m(m-1)/2$. Suppose that the input multisets have n elements. The basic operation is taken to be one multiplication, inversion or comparison of elements of the abelian group. Denote by $C_{(2)}$ the cost of finding square roots in the abelian group. Then the worst-case complexity of the algorithm is

$$O\left(n^2 m\, C_{(2)} + n^3 m \log(n)\right).$$

Received 20 July 1999, revised 14 February 2000; *published 27 March 2000*.
2000 Mathematics Subject Classification 05E99

Heuristic arguments are outlined which suggests that the improved bound

$$O\left(n\,C_{(2)} + n^2 \log(n)\right)$$

is more appropriate for the majority of inputs.

The algorithm cannot recognise the exterior square of a multiset which is neither recognisable nor involution-recognisable. In Section 6 we show that the proportion of multisets which are neither recognisable nor involution-recognisable is small when the abelian group is finite but large. The theoretical results and heuristic arguments are illustrated by the results of practical tests, which are presented in Section 7.

Finally, in Section 8 we consider the special case which motivated the general definition of the exterior square of a multiset; namely, multisets of eigenvalues of matrices. We show how the multiset algorithm can be used to recognise the exterior square of certain matrices over finite fields (up to conjugation). This might help us to solve the open problem of efficiently recognising the special linear group in its exterior square action.

2. *Notation and preliminary results*

First we review the definition of a multiset. Let Θ be any set. The set of all multisets of size r with elements in Θ is denoted by $\Theta^{\{r\}}$ and is defined by

$$\Theta^{\{r\}} = \Theta^r / \mathrm{Sym}(r),$$

where the symmetric group $\mathrm{Sym}(r)$ acts on Θ^r by permuting entries. If $(\omega_1, \ldots, \omega_r) \in \Theta^r$ then denote its image in $\Theta^{\{r\}}$ by $\{\omega_1, \ldots, \omega_r\}$. By convention, if $\omega \in \Theta^{\{r\}}$ then we write $\omega = \{\omega_1, \ldots, \omega_r\}$. Suppose that $\omega \in \Theta^{\{r\}}$ and $g \in \Theta$. Let $\mathrm{mult}(g;\ \omega)$ denote the *multiplicity* of g in ω, defined by

$$\mathrm{mult}(g; \omega) = |\,\{i : g = \omega_i\}\,|.$$

Write $g \in \omega$ if $\mathrm{mult}(g; \omega) \geqslant 1$. Say that ω is *multiplicity-free* if $\mathrm{mult}(g; \omega) \leqslant 1$ for all $g \in \Theta$. The multiset union, multiset intersection and multiset difference operations can all be defined in terms of multiplicities, as follows. Let

$$\begin{aligned}
\mathrm{mult}(g; \omega \cup \omega') &= \mathrm{mult}(g; \omega) + \mathrm{mult}(g; \omega'),\\
\mathrm{mult}(g; \omega \cap \omega') &= \min\{\mathrm{mult}(g; \omega), \mathrm{mult}(g; \omega')\},\\
\mathrm{mult}(g; \omega \setminus \omega') &= \max\{0, \mathrm{mult}(g; \omega) - \mathrm{mult}(g; \omega')\}
\end{aligned}$$

for all $g \in \Theta$ and all $\omega, \omega' \in \Theta^{\{r\}}$. Let k be a positive integer and $\omega \in \Theta^{\{r\}}$. Define the multiset $k\omega \in \Theta^{\{kr\}}$ as follows:

$$\mathrm{mult}(g; k\omega) = k\,\mathrm{mult}(g; \omega).$$

We might wish to define a multiset using some property $\mathcal{P}$ defined on Θ. Given $\omega \in \Theta^{\{r\}}$, write

$$\omega' = \{g \in \omega : \mathcal{P}(g)\}$$

to denote the multiset defined by

$$\mathrm{mult}(g; \omega') = \begin{cases} 0 & \text{if } g \notin \omega \text{ or not } \mathcal{P}(g),\\ \mathrm{mult}(g; \omega) & \text{otherwise.}\end{cases}$$

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

Finally, if Θ is a finite set then

$$|\Theta^{\{r\}}| = \binom{|\Theta| + r - 1}{r} \tag{1}$$

for $r \geqslant 1$.

2.1. *The exterior square of a multiset*

Suppose that A is a set which supports a commutative multiplication operation. Let a be an element of $A^{\{m\}}$. The *exterior square* of a, denoted by $a^{\wedge 2}$, is the multiset

$$\{a_i a_j : 1 \leqslant i < j \leqslant m\}.$$

For the remainder of this paper let $n = m(m-1)/2$. Let b be an element of $A^{\{n\}}$. Then a is said to be an *exterior square root* of b if $b = a^{\wedge 2}$. To justify the use of the term 'exterior square' in this context, we show how this definition relates to the best-known exterior square construction, the exterior square of a vector space. Let X be an $m \times m$ matrix over a field F, and let α be the multiset of eigenvalues of X. It is not difficult to prove that $\alpha^{\wedge 2}$ is the multiset of eigenvalues of the matrix which represents the action of X on the exterior square of the underlying vector space. Note that $\alpha \in K^{\{m\}}$ and $\alpha^{\wedge 2} \in K^{\{n\}}$, where K is the splitting field of the characteristic polynomial of X over F. Clearly, $\alpha^{\wedge 2}$ is determined by the multiset of nonzero elements in α. For this reason, we consider multisets of abelian group elements. For the remainder of the paper let A be an abelian group.

Suppose that we were given a multiset $b \in A^{\{n\}}$ and told that b has an exterior square root. Suppose that we were also given a map

$$\psi : \{\{i, j\} : 1 \leqslant i < j \leqslant m\} \to \{1, \ldots n\}$$

such that $a_i a_j = b_{\psi(\{i,j\})}$ for $1 \leqslant i < j \leqslant m$. Then, writing the abelian group A additively, we have n linear equations in m unknowns $a_1, \ldots, a_m$. We can solve the system to find the entries of a using elementary linear algebra over the integers. Here, multiplying an equation by a positive integer r corresponds to raising each side of the equation to the rth power, and multiplying an equation by -1 corresponds to inverting each side of the equation. Dividing an equation by a positive integer r corresponds to taking rth roots of both sides of the equation in A, and so is allowed only when both sides have an rth root in A. Of course, when given an element of $A^{\{n\}}$ we do not in general have access to the helpful map ψ, and simply testing all possible maps does not lead to an efficient algorithm as there are $n!$ of them. (Note that this approach does provide an algorithm, albeit a highly inefficient one, which applies when the algorithm described in this paper does not: namely, for finding exterior square roots which are neither recognisable nor involution-recognisable.)

It is easy to construct exterior square roots of elements of $A^{\{1\}}$ and $A^{\{3\}}$. Let 1_A denote the identity element of A. Then an exterior square root of $\{b_1\}$ is given by $\{1_A,\ b_1\}$ for all $b_1 \in A$. Let b be an element of $A^{\{3\}}$. If b has an exterior square root a then, without loss of generality,

$$b_1 = a_1 a_2,\ \ b_2 = a_1 a_3,\ \ b_3 = a_2 a_3.$$

Therefore $b_1 b_2 {b_3}^{-1} = {a_1}^2$. Given $b \in A^{\{3\}}$, if $b_1 b_2 {b_3}^{-1}$ has no square root then b has no exterior square root. Otherwise, let w be a square root of $b_1 b_2 {b_3}^{-1}$. Then the multiset $\{w,\ w^{-1}b_1,\ w^{-1}b_2\}$ is an exterior square root of b. For the remainder of the paper assume that $m \geqslant 4$.

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

2.2. *Preliminaries*

To close this section, we make a few more definitions and establish some preliminary results. If $a \in A^{\{r\}}$ and $\tau \in A$, define the multiset $\tau a \in A^{\{r\}}$ as follows:

$$\mathrm{mult}(g; \tau a) = \mathrm{mult}(\tau^{-1} g; a)$$

for all $g \in A$. Observe that if τ is any element of A such that $\tau^2 = 1$ then

$$(\tau a)^{\wedge 2} = a^{\wedge 2} \tag{2}$$

for all $a \in A^{\{m\}}$. For $a \in A^{\{m\}}$ let aa^{-1} denote the multiset

$$\{a_i\, a_j{}^{-1} : 1 \leqslant i \neq j \leqslant m\} \tag{3}$$

with $m(m-1)$ elements, and let $a^{\wedge 2}a^{-\wedge 2}$ denote the multiset

$$\{a_i a_j (a_k a_l)^{-1} : 1 \leqslant i < j \leqslant m,\ 1 \leqslant k < l \leqslant m;\ i, j, k, l \text{ distinct}\} \tag{4}$$

with $6\binom{m}{4}$ elements. Note that the multiset $a^{\wedge 2}a^{-\wedge 2}$ contains only those elements $a_i a_j (a_k a_l)^{-1}$ where i, j, k, l are distinct. Therefore the multisets $a^{\wedge 2}a^{-\wedge 2}$ and bb^{-1} are not equal, where $b = a^{\wedge 2}$. This point is clarified by the following result. The proof is elementary.

Lemma 2.1. *Suppose that $a \in A^{\{m\}}$ and let $b = a^{\wedge 2}$. Then the multiset equality*

$$bb^{-1} = (m-2)aa^{-1} \cup a^{\wedge 2}a^{-\wedge 2}$$

holds. In particular, bb^{-1} contains no more than

$$m(m-1) + 6\binom{m}{4} = \frac{m(m-1)}{4}(m^2 - 5m + 10)$$

distinct elements.

Given $a \in A^{\{m\}}$ let a^* denote the multiset defined by

$$a^* = aa^{-1} \cup a^{\wedge 2}a^{-\wedge 2}. \tag{5}$$

If $b = a^{\wedge 2}$ for some $a \in A^{\{m\}}$ then the set of distinct elements in bb^{-1} is equal to the set of distinct elements in a^*.

In the next two sections, two properties are defined which an element of $A^{\{m\}}$ may possess, the *recognisable* property and the *involution-recognisable* property. If $b = a^{\wedge 2}$ and a is recognisable or involution-recognisable then an exterior square root of b can be constructed, using procedures developed below. These procedures are then combined to produce an algorithm which can determine whether a given multiset has a recognisable or involution-recognisable exterior square root.

The algorithm fails to find an exterior square of any multiset whenever the input has an exterior square root, but no exterior square root which is recognisable or involution-recognisable. In Section 6 the proportion of multisets which are neither recognisable nor involution-recognisable is shown to be small when the abelian group is finite but large.

3. *Recognisable multisets*

A multiset $a \in A^{\{m\}}$ is said to be *recognisable* if there exists $g \in aa^{-1}$ such that g has multiplicity 1 in a^*. The proof of the next result is easy, and is omitted here.

Lemma 3.1. *If $a \in A^{\{m\}}$ and a is recognisable then a is multiplicity-free.*

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

The next two results will be used to construct a procedure which searches for recognisable exterior square roots of multisets.

Lemma 3.2. *Suppose that $a \in A^{\{m\}}$ is recognisable, and let $b = a^{\wedge 2}$. Then there exists $g \in aa^{-1}$ such that* $\mathrm{mult}(g;\ bb^{-1}) = m - 2$. *Let $S(g)$ be the multiset of size $m - 2$ defined by*

$$S(g) = \{u \in b : \text{there exists } v \in b \text{ such that } uv^{-1} = g\}. \tag{6}$$

Then $S(g)$ is multiplicity-free.

Proof. By Lemma 2.1 there exists $g \in aa^{-1}$ with multiplicity $m - 2$ in bb^{-1}. Without loss of generality let $g = a_1 a_2{}^{-1}$. Then $S(g) = \{a_1 a_k : 3 \leqslant k \leqslant m\}$. Since a is multiplicity-free (by Lemma 3.1), it follows that $S(g)$ is multiplicity-free. □

By searching through elements of the multiset b which do not lie in $S(g)$ or in $g^{-1}S(g)$ an exterior square root of b may be constructed. This is a consequence of the following result.

Lemma 3.3. *Let $a \in A^{\{m\}}$ be a recognisable multiset, and let $b = a^{\wedge 2}$. Let $g = a_1 a_2{}^{-1}$ and suppose that g has multiplicity $m - 2$ in bb^{-1}. Let $S(g)$ be as defined in equation (6). For at least one element z of $b \setminus (S(g) \cup g^{-1}S(g))$ the product gz has a square root w such that $w = \tau a_1$ for some $\tau \in A$, $\tau^2 = 1$. Furthermore, the multiset*

$$\{w,\ g^{-1}w\} \cup w^{-1}S(g)$$

is an exterior square root of b.

Proof. The multiset $b \setminus (S(g) \cup g^{-1}S(g))$ is given by

$$b \setminus (S(g) \cup g^{-1}S(g)) = \{a_1 a_2\} \cup \{a_k a_l : 3 \leqslant k < l \leqslant m\}.$$

When $z = a_1 a_2$ the product gz equals ${a_1}^2$, which certainly has a square root in A. Let w be any square root of gz. Then $w = \tau a_1$ for some $\tau \in A$ such that $\tau^2 = 1$. The multiset

$$\{w,\ g^{-1}w\} \cup w^{-1}S(g)$$

equals τa, which is an exterior square root of b by equation (2). □

Lemmas 3.2 and 3.3 give rise to a procedure for finding recognisable exterior square roots of multisets, as shown in Figure 1. Let $L_1(b)$ be the set defined by

$$L_1(b) = \{g \in bb^{-1} : \mathrm{mult}(g; bb^{-1}) = m - 2\}.$$

The input to the procedure is a multiset $b \in A^{\{n\}}$, together with an element $g \in L_1(b)$. We try to form a recognisable exterior square root a of b, using the quotient g. An analysis of the complexity of this procedure is presented in Section 5.1.

Lemma 3.4. *Procedure* REC *is correct.*

Proof. Let $b \in A^{\{n\}}$ be input to Procedure REC, together with the quotient $g \in L_1(b)$. Then g is an element of bb^{-1} with multiplicity $m-2$. Suppose first that b has a recognisable exterior square root a such that $g \in aa^{-1}$. Then Lemmas 3.2 and 3.3 guarantee that an exterior square root of b will be output. If b has no exterior square root then the procedure will certainly return the message *'false'*. Suppose that the output of Procedure REC, with input (b, g), is a multiset $a \in A^{\{m\}}$. Then $b = a^{\wedge 2}$, so it remains to prove that a is

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

PROCEDURE REC. *Given an element b of $A^{\{n\}}$ and a quotient $g \in L_1(b)$, this procedure outputs a recognisable exterior square root a of b such that $a \in A^{\{m\}}$ and $g \in aa^{-1}$, if one exists, and outputs the message 'false' otherwise.*

```
Begin
  let S(g) be the multiset defined in equation (6);
  if S(g) is multiplicity-free then
    for z in b \ (S(g) ∪ g^{-1}S(g)) do
      if gz has a square root w in A then
        a := {w, g^{-1}w} ∪ w^{-1}S(g);
        if a^{∧2} = b then
          return a;
        endif;
      endif;
    endfor;
  endif;
  return the message 'false';
End.
```

Figure 1: Procedure REC

recognisable and that $g \in aa^{-1}$. Now $\mathrm{mult}(g;\ bb^{-1}) = m - 2$ and $g \in a^*$. Let z be the element of $b \setminus (S(g) \cup g^{-1}S(g))$ which was involved in the construction of the multiset a. Then, without loss of generality, $gz = {a_1}^2$ and $g^{-1}a_1 = a_2$. Hence $g = a_1 {a_2}^{-1} \in aa^{-1}$, as required. Moreover, using Lemma 2.1, the multiplicity of g in a^* is 1. Therefore a is recognisable. □

4. *Involution-recognisable multisets*

A multiset $a \in A^{\{m\}}$ is said to be *involution-recognisable* if there exists an element g of aa^{-1} such that $g^2 = 1$ and $\mathrm{mult}(g;\ a^*) = 2$.

Suppose that A is an elementary abelian 2-group. Then no element of $A^{\{m\}}$ is recognisable. This is one reason for defining the involution-recognisability property. Another reason is that without this property, the calculations of Section 6 would be much more complicated. The proof of the next result is easy, and is omitted here.

Lemma 4.1. *Let a be an element of $A^{\{m\}}$ which is involution-recognisable. Let g be an element of aa^{-1} such that $g = g^{-1}$ and* $\mathrm{mult}(g;\ a^*) = 2$. *Then a contains at least $m - 1$ distinct entries, and a is multiplicity-free unless $g = 1$.*

The following series of lemmas demonstrates how one can construct an exterior square root of b from the multiset bb^{-1} if b has an involution-recognisable exterior square root. The proof of the next result is similar to that of Lemma 3.2.

Lemma 4.2. *Suppose that $a \in A^{\{m\}}$ is involution-recognisable, and let $b = a^{\wedge 2}$. There exists $g \in aa^{-1}$ such that $g^2 = 1$ and* $\mathrm{mult}(g;\ bb^{-1}) = 2(m-2)$. *Let $T(g)$ be the multiset of size $2(m-2)$ defined by*

$$T(g) = \{u \in b : \text{there exists } v \in b \text{ such that } uv^{-1} = g\}. \tag{7}$$

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

If $g \neq 1$ then $T(g)$ is multiplicity-free. If $g = 1$ then $T(g) = 2S(g)$ where $S(g)$ is a multiplicity-free multiset of size $m - 2$.

The next two results are proved by modifying the argument of Lemma 3.3. The first can be used to construct an exterior square root of b when $g = 1$.

Lemma 4.3. *Suppose that $a \in A^{\{m\}}$ is involution-recognisable, and let $b = a^{\wedge 2}$. Let $g = a_1 a_2^{-1}$ and suppose that $g = 1$ and that $\mathrm{mult}(g;\ bb^{-1}) = 2(m-2)$. Let $T(g)$ be the multiset defined in equation (7), and let $S(g)$ be the set of size $m-2$ such that $T(g) = 2S(g)$. For at least one $z \in b \setminus T(g)$ the product gz has a square root w in A such that the multiset*

$$\{w,\ w\} \cup w^{-1}S(g)$$

is an exterior square root of b.

When $g \neq 1$ the situation is slightly more complicated. The next result can be used to find an element w of A such that $w = \tau a_1$ for some $\tau \in A$, where $\tau^2 = 1$.

Lemma 4.4. *Let $a \in A^{\{m\}}$ be an involution-recognisable multiset, and let $b = a^{\wedge 2}$. Let $g = a_1 a_2^{-1}$, and suppose that $g^2 = 1$, $g \neq 1$ and g has multiplicity $2(m-2)$ in bb^{-1}. Let $T(g)$ be the multiset defined in equation (7). For at least one element z of $b \setminus T(g)$ the product gz has a square root w in A such that $w = \tau a_1$ for some $\tau \in A$, $\tau^2 = 1$.*

In the proof of Lemma 3.3 an exterior square root of b was constructed using the element w and the set $S(g)$ of size $m-2$. In the involution-recognisable case, no such set exists unless $g = 1$. When $g \neq 1$ let $S'(g)$ be the set of unordered pairs $\{b_i,\ b_j\}$ of elements of b such that $b_i\, b_j{}^{-1} = b_j\, b_i{}^{-1} = g$. If $g = a_1\, a_2{}^{-1}$ then the set $S'(g)$ is given by

$$S'(g) = \{\{a_1 a_k,\ a_2 a_k\} : 3 \leqslant k \leqslant m\}.$$

The next result shows how the set $S'(g)$ can be used to construct an exterior square root of b.

Lemma 4.5. *Suppose that $a \in A^{\{m\}}$, and that a is involution-recognisable. Let $b = a^{\wedge 2}$. Let $g = a_1\, a_2{}^{-1}$, and suppose that $g^2 = 1$, $g \neq 1$, $\mathrm{mult}(g;\ bb^{-1}) = 2(m-2)$. Let $S'(g)$ be the set of unordered pairs $\{b_i,\ b_j\}$ of elements of b such that $b_i\, b_j{}^{-1} = b_j\, b_i{}^{-1} = g$. Suppose that we have an element $w \in A$ such that $w = \tau a_1$ for some $\tau \in A$, where $\tau^2 = 1$. Then an exterior square root $\tilde{a}$ of b can be constructed.*

Proof. The elements $\tilde{a}_k$ of a multiset $\tilde{a}$ will be defined inductively, in such a way that $\tilde{a}^{\wedge 2} = b$. Let $\tilde{a}_1 = w$ and let $\tilde{a}_2 = gw$. Then $\tilde{a}_1 = \tau a_1$ and $\tilde{a}_2 = \tau a_2$. Let us fix a labelling on the elements of $S'(g)$ so that $S'(g) = \{s_1, \ldots, s_{m-2}\}$ where, without loss of generality, $s_{k-2} = \{a_1 a_k,\ a_2 a_k\}$ for $3 \leqslant k \leqslant m$. Let $\tilde{a}_3$ be assigned the value $w^{-1}x_3$ where x_3 is chosen at random from s_1. Then $\tilde{a}_3$ is one of τa_3, $\tau g a_3$. In either case, the multiset equality

$$\{\tilde{a}_1,\ \tilde{a}_2,\ \tilde{a}_3\}^{\wedge 2} = \{a_1,\ a_2,\ a_3\}^{\wedge 2}$$

holds. For the inductive step, assume that $4 \leqslant k \leqslant m$ and that the values of $\tilde{a}_1, \ldots, \tilde{a}_{k-1}$ have been assigned in such a way that

$$\{\tilde{a}_1, \ldots, \tilde{a}_{k-1}\}^{\wedge 2} = \{a_1, \ldots, a_{k-1}\}^{\wedge 2}.$$

Let $\tilde{a}_k$ be assigned the value $w^{-1}x_k$ where x_k is either element of s_{k-2}, chosen at random. Then $\tilde{a}_k$ is one of τa_k, $\tau g a_k$. Suppose that the chosen values are $\tilde{a}_3 = \tau a_3$ and $\tilde{a}_k = \tau g a_k$. Then $\tilde{a}_3 \tilde{a}_k = g a_3 a_k$. We claim that

$$g a_3 a_k \notin b \setminus \{\tilde{a}_1, \ldots, \tilde{a}_{k-1}\}^{\wedge 2}. \tag{8}$$

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

Since $g \neq 1$ it follows that $ga_3a_k \neq a_3a_k$. Suppose for a contradiction that $ga_3a_k = a_ia_j$ for some i, j satisfying $1 \leqslant i < j \leqslant m,\ j \geqslant k,\ (i, j) \neq (3, k)$. Then $g = a_i\, a_j\, (a_3\, a_k)^{-1}$ and $\mathrm{mult}(g;\ a^*) > 2$, contradicting the choice of g. The situation described by equation (8) also arises when $\tilde{a}_3 = \tau g a_3$ and $\tilde{a}_k = \tau a_k$. In either case, replace $\tilde{a}_k$ by $g\tilde{a}_k$. Then

$$\{\tilde{a}_1, \ldots, \tilde{a}_k\}^{\wedge 2} = \{a_1, \ldots, a_k\}^{\wedge 2}\,.$$

This inductive process stops when all the values of the multiset $\tilde{a}$ have been assigned. Then $\tilde{a}$ is an exterior square root of b, by construction. □

In fact, the multiset $\tilde{a}$ constructed above is one of τa or $\tau g a$, both of which are exterior square roots of b, by equation (2). Let us assume that CONSTRUCT is a function which implements the method of Lemma 4.5. Let $L_2(b)$ be the set defined by

$$L_2(b) = \{g \in bb^{-1} : \mathrm{mult}(g; bb^{-1}) = 2(m-2) \text{ and } g^2 = 1\}.$$

Then CONSTRUCT takes as input a multiset b, an element g of $L_2(b)$, the set $S'(g)$ of $m-2$ unordered pairs of elements of b whose quotient equals g and an element w of A. Let the function return the message *'failed'* if the method of Lemma 4.5 fails; otherwise, let it return an exterior square root of b. Lemmas 4.2 – 4.5 lead directly to Procedure INV (see Figure 2), which calls the function CONSTRUCT. The input is a multiset b and an element $g \in L_2(b)$. We try to construct an exterior square root of b using the quotient g. An analysis of the complexity of this procedure is presented in Section 5.1.

The following lemma can be proved in much the same way as Lemma 3.4.

Lemma 4.6. *Procedure* INV *is correct.*

5. *An exterior square root algorithm for multisets*

Procedure REC and Procedure INV can be combined to give an algorithm for finding exterior square roots which are recognisable or involution-recognisable (see Figure 3). The output of the algorithm is either an exterior square root of the input, or one of the following messages: *'no exterior square root'*, or *'no recognisable or involution-recognisable exterior square root'*.

The following theorem proves that Algorithm MULT is correct, using Lemmas 3.4 and 4.6.

Theorem 5.1. *Algorithm* MULT *is correct.*

Proof. Clearly, the output of Algorithm MULT is correct when b has no exterior square root. On the other hand, if b does have an exterior square root, then bb^{-1} contains at most $m(m-1)(m^2-5m+10)/4$ distinct elements, by Lemma 2.1. Now suppose that b has a recognisable exterior square root a. Then there exists $g \in aa^{-1}$ such that $\mathrm{mult}(g, a^*) = 1$. Hence $g \in L_1(b)$ and the output of Procedure REC upon input of (b, g) is an exterior square root of b, by Lemma 3.4. This exterior square root of b will be output by Algorithm MULT, and this output is correct. A similar argument shows that the output of Algorithm MULT is correct if b has an involution-recognisable exterior square root. Finally, suppose that b has an exterior square root, but not one which is recognisable or involution-recognisable. Now any multiset output by Procedure REC (INV) is recognisable by Lemma 3.4, and involution-recognisable by Lemma 4.6. Therefore the output of Algorithm MULT upon input of b is the message *'no recognisable or involution-recognisable exterior square root'*, and this output is correct. □

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

PROCEDURE INV. *Given an element b of $A^{\{n\}}$ and a quotient $g \in L_2(b)$, this procedure outputs an involution-recognisable exterior square root a of b such that $a \in A^{\{m\}}$ and $g \in aa^{-1}$, if one exists, and outputs the message 'false' otherwise.*

```
Begin
  let T(g) be the multiset defined in equation (7);
  if g ≠ 1 then
    if T(g) is multiplicity-free then
      let S'(g) be the list of pairs of elements of b whose quotient is g;
      for z in b \ T(g) do
        if gz has a square root w in A then
          a := CONSTRUCT(b, g, S'(g), w);
          if a is a multiset then
            return a;
          endif;
        endif;
      endfor;
    endif;
  else        (* g = 1 *)
    if T(g) = 2S(g) for some multiplicity-free multiset S(g) then
      for z in b \ T(g) do
        if gz has a square root w then
          a := {w, w} ∪ w^{-1}S(g);
          if a^{∧2} = b then
            return a;
          endif;
        endif;
      endfor;
    endif;
  endif;
  return the message 'false';
End.
```

Figure 2: Procedure INV

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

ALGORITHM MULT. *Given an element b of $A^{\{n\}}$, the algorithm outputs either an exterior square root $a \in A^{\{m\}}$ of b or one of the following messages: 'no exterior square root' or 'no recognisable or involution-recognisable exterior square root'.*

```
Begin
  form bb^{-1};
  if bb^{-1} contains more than m(m − 1)(m^2 − 5m + 10)/4 distinct elements then
    return the message 'no exterior square root';
  endif;
  let L_1(b) be the list of all elements in bb^{-1} with multiplicity m − 2;
  for g ∈ L_1(b) do
    perform Procedure REC with input (b, g);
    if the result is a multiset a then
      return a;
    endif;
  endfor;
  let L_2(b) be the list of all elements in bb^{-1} with order dividing 2 and
                                                    multiplicity 2(m − 2);
  for g ∈ L_2(b) do
    perform Procedure INV with input (b, g);
    if the result is a multiset a then
      return a;
    endif;
  endfor;
  return the message
          'no recognisable or involution-recognisable exterior square root';
End.
```

Figure 3: Algorithm MULT

Despite the fact that the output of Algorithm MULT is always correct, there is a sense in which it fails on certain inputs. Suppose that $b \in A^{\{n\}}$ has an exterior square root, but not one which is recognisable or involution-recognisable. Then Algorithm MULT cannot differentiate this multiset from one which has no exterior square root (unless bb^{-1} contains too many distinct elements in the latter case). The likelihood of this 'failure' is related to the proportion of elements in $A^{\{m\}}$ which are neither recognisable nor involution-recognisable. An upper bound for this proportion is developed in Section 6.

5.1. *Complexity analysis*

We will now analyse the complexity of Algorithm MULT. As the basic operation we take the cost of multiplying two elements of the abelian group A, which we assume is equal to the cost of comparing or inverting elements of A. Let $C_{(2)}$ denote the cost of finding square roots of elements of A, or of determining that a given element of A has no square root. The value of $C_{(2)}$ depends upon algorithms which exist for the abelian group A. We assume that there exists a linear ordering on the elements of A. This speeds up the multiset calculations,

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

as a multiset a in $A^{\{r\}}$ may be represented as some kind of ordered structure. We assume (see, for example, [4]) that it costs $O(r\log(r))$ operations to form an ordered structure representing an element of $A^{\{r\}}$. While doing so we can simultaneously check whether the multiset is multiplicity-free. The cost of comparing two elements of $A^{\{r\}}$, where one is represented by an ordered structure, is also assumed to equal $O(r\log(r))$. The cost of forming the multiset difference $a \setminus a'$ is assumed to be $O(s\log(r))$, where $a \in A^{\{r\}}$ is represented by an ordered structure, $a' \in A^{\{s\}}$ and $s \leqslant r$. Finally, it costs $O(r)$ to scan the ordered structure representing an element of $A^{\{r\}}$; for example, to list all elements with a given multiplicity. In this paper all logarithms are to base two.

We begin by estimating the complexity of Procedure REC. Recall the set $S(g)$ defined in equation (6).

Lemma 5.1. *Let $C(\mathrm{REC}, n, A)$ denote the cost of performing Procedure* REC *with input (b, g), where $b \in A^{\{n\}}$ and $g \in L_1(b)$. Assume that an ordered structure representing the multiset b is available. Then*

$$C(\mathrm{REC}, n, A) = O\left(n\,C_{(2)} + n^2\log(n)\right). \tag{9}$$

Proof. Consider the complexity of the steps performed by Procedure REC. Before entering the inner loop we check that $S(g)$ is multiplicity-free, and form the multiset difference $b \setminus (S(g) \cup g^{-1}S(g))$. This costs $O(m\log(m))$ operations. Then we loop over the $(n-2(m-2))$ elements z of $b \setminus (S(g) \cup g^{-1}S(g))$, performing the following calculations. The product gz is computed, and a square root w of gz is sought. This costs $O(C_{(2)})$. It costs $O(n\log(n))$ operations to form the multiset a and test whether $a^{\wedge 2} = b$. These costs dominate the costs performed outside the inner loop, and the inner loop is performed $O(n)$ times. Thus the complexity is either $O(n\,C_{(2)})$ or $O(n^2\log(n))$, whichever is the larger. □

Let $C(\mathrm{INV}, n, A)$ denote the complexity of performing Procedure INV with input (b, g), where $b \in A^{\{n\}}$ and $g \in L_2(b)$. Then it is not difficult to show that

$$C(\mathrm{INV}, n, A) = O\left(n\,C_{(2)} + n^2\log(n)\right), \tag{10}$$

since the calculations performed by Procedures REC and INV are very similar. We now use these results to analyse the complexity of Algorithm MULT.

Theorem 5.2. *Let $C(\mathrm{MULT}, n, A)$ denote the cost of performing Algorithm* MULT *with input an element of $A^{\{n\}}$. Then*

$$C(\mathrm{MULT}, n, A) = O\left(n^2 m\,C_{(2)} + n^3 m\log(n)\right). \tag{11}$$

Proof. Algorithm MULT has three components. The first component involves forming bb^{-1} and the lists $L_1(b)$ and $L_2(b)$, the second component consists of performing Procedure REC with input $(b,\ g)$ for (possibly) all elements $g \in L_1(b)$, and the third component consists of performing Procedure INV with input $(b,\ g)$ for (possibly) all elements $g \in L_2(b)$. The most expensive part of the first component involves forming an ordered structure to hold the multiset bb^{-1}. Hence the complexity of the first component is $O(n^2\log(n))$. We now consider the cost of the remaining components. For any element b of $A^{\{n\}}$ the equation

$$(m-2)|L_1(b)| + 2(m-2)|L_2(b)| \leqslant n(n-1)$$

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

holds. Therefore the cost of the last two components of Algorithm MULT is at most

$$\frac{n(m+1)}{4} \max\ (2C(\mathrm{REC}, n, A), C(\mathrm{INV}, n, A))$$

operations. Using equations (9) and (10), it follows that the complexity of the last two components of Algorithm MULT is $O(n^2 m\, C_{(2)})$ or $O(n^3 m \log(n))$, whichever is the greater. This dominates the complexity of the first component, proving the theorem. □

We believe that, in most cases, this complexity estimate is much too high. In the next subsection, heuristic arguments will be outlined which suggest that, for most multisets $b \in A^{\{n\}}$, at most one element of $L_1(b) \cup L_2(b)$ is processed by Algorithm MULT upon input of b.

5.2. *Heuristic arguments*

First, consider the number of elements of $L_1(b)$ processed by Algorithm MULT upon input of $b \in A^{\{n\}}$. If $b = a^{\wedge 2}$ for some $a \in A^{\{m\}}$, but b has no recognisable exterior square root, then $g \notin aa^{-1}$ for all $g \in L_1(b)$. On the other hand, if a is recognisable, then the number of elements of $L_1(b)$ processed is at most

$$|L_1(b) \setminus aa^{-1}| + 1,$$

where here, the operation '\' denotes *set* difference, not multiset difference. Using Lemma 2.1, it follows that $g \in L_1(b) \setminus aa^{-1}$ if and only if $g \in a^{\wedge 2}a^{-\wedge 2}$ but $g \notin aa^{-1}$, and the multiplicity of g in $a^{\wedge 2}a^{-\wedge 2}$ is $m-2$. If A is a large, finite abelian group then the proportion of elements in $A^{\{6\binom{m}{4}\}}$ which contain an element of multiplicity $m-2$ is small. Assume that the events

$$\{c \in A^{\{6\binom{m}{4}\}} : \mathrm{mult}(g; c) = m-2 \text{ for some } g \in A\}$$

and

$$\{c \in A^{\{6\binom{m}{4}\}} : c = a^{\wedge 2}a^{-\wedge 2} \text{ for some } a \in A^{\{m\}}\}$$

are independent. It follows that $L_1(a^{\wedge 2}) \setminus aa^{-1} = \emptyset$ for most multisets $a \in A^{\{m\}}$.

A recognisable multiset a is said to be *clearly recognisable* if

$$\mathrm{mult}(g;\ a^{\wedge 2}a^{-\wedge 2}) \neq m-2 \text{ for all } g \in a^{\wedge 2}a^{-\wedge 2}.$$

The above result, if true, would imply that most recognisable multisets are clearly recognisable. Suppose that $b = a^{\wedge 2}$ where a is a clearly recognisable multiset in $A^{\{m\}}$. Then every element of $L_1(b)$ is a member of aa^{-1}. Therefore, by Lemma 3.4, an exterior square root of b will be constructed when Procedure REC is performed with input (b, g), where g is *any* element of $L_1(b)$.

Similarly, suppose that $b \in A^{\{n\}}$ and b has no exterior square root in $A^{\{m\}}$. If A is finite but large then the proportion of elements of $A^{\{n(n-1)\}}$ which contain an element with multiplicity $m-2$ is small. Assume that the events

$$\{c \in A^{\{n(n-1)\}} : \mathrm{mult}(g; c) = m-2 \text{ for some } g \in A\}$$

and

$$\{c \in A^{\{n(n-1)\}} : c = bb^{-1} \text{ for some } b \in A^{\{n\}} \setminus \{a^{\wedge 2} : a \in A^{\{m\}}\}\}$$

are independent. It follows that $L_1(b) = \emptyset$ for most multisets $b \in A^{\{n\}}$ with no exterior square root. These heuristic arguments can be made more precise, and can be adapted to

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

the case of involution-recognisable multisets. In particular, the arguments imply that most involution-recognisable multisets are clearly involution-recognisable, where an involution-recognisable multiset a is said to be *clearly involution-recognisable* if

$$\mathrm{mult}(g;\ a^{\wedge 2}a^{-\wedge 2}) \neq 2(m-2) \text{ for all } g \in a^{\wedge 2}a^{-\wedge 2}.$$

Combining these heuristic arguments suggests that, for most elements $b \in A^{\{n\}}$, at most *one* element of $L_1(b) \cup L_2(b)$ will be processed by Algorithm MULT. Recall that the complexity of the first component of Algorithm MULT is $O(n^2 \log(n))$. Therefore, when at most one element of $L_1(b) \cup L_2(b)$ is processed by Algorithm MULT, the complexity of the algorithm is

$$O(n\, C_{(2)} + n^2 \log(n)).$$

These heuristic arguments suggest that this complexity estimate is more realistic than equation (11) in most cases.

6. *Counting multisets which are neither recognisable nor involution-recognisable*

We have seen that Algorithm MULT cannot detect that a multiset has an exterior square root unless the exterior square root is recognisable or involution-recognisable. In this section we obtain an upper bound for the proportion of multisets which are neither recognisable nor involution-recognisable, when A is a finite abelian group. Let $Z[\mathrm{nnor}, m, A]$ denote the set of all elements of $A^{\{m\}}$ which are neither recognisable nor involution-recognisable.

It is convenient to consider multiplicity-free multisets separately. Let $A^{\{m\}}_{\mathrm{free}}$ denote the set of all multiplicity-free multisets in $A^{\{m\}}$ and let

$$A^{\{m\}}_{\mathrm{mult}} = A^{\{m\}} \setminus A^{\{m\}}_{\mathrm{free}}.$$

This allows us to write

$$Z[\mathrm{nnor}, m, A] = Z[\mathrm{mult\&nnor}, m, A] \cup Z[\mathrm{free\&nnor}, m, A]$$

where

$$\begin{aligned} Z[\mathrm{mult\&nnor}, m, A] &= Z[\mathrm{nnor}, m, A] \cap A^{\{m\}}_{\mathrm{mult}}, \\ Z[\mathrm{free\&nnor}, m, A] &= Z[\mathrm{nnor}, m, A] \cap A^{\{m\}}_{\mathrm{free}}. \end{aligned}$$

By Lemma 3.1, a multiset with multiplicities is not recognisable. Similarly, using Lemma 4.1 we know that almost all involution-recognisable multisets are multiplicity-free. Hence $|A^{\{m\}}_{\mathrm{mult}}||A^{\{m\}}|^{-1}$ is a good upper bound for $|Z[\mathrm{mult\&nnor}]||A^{\{m\}}|^{-1}$. An upper bound for the former quantity is stated below (the proof is easy, and is omitted here).

Theorem 6.1. *Let Θ be any finite set. If $m \geqslant 2$ then*

$$\frac{|\Theta^{\{m\}}_{\mathrm{mult}}|}{|\Theta^{\{m\}}|} < \frac{m(m-1)}{|\Theta|}.$$

It remains to calculate an upper bound for $|Z[\mathrm{free\&nnor}, m, A]||A^{\{m\}}|^{-1}$. Some further notation is required. Fix a linear ordering on the elements of A. Assume throughout the remainder of this section that elements of multisets in $A^{\{m\}}_{\mathrm{free}}$ are labelled in ascending order

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

with respect to this ordering. Recall the multiset a^* defined in Section 2, equation (5). Given $a \in A_{\text{free}}^{\{m\}}$, define the multisets $\Gamma_{i,j}(a)$ for $1 \leqslant i < j \leqslant m$ as follows:

$$\Gamma_{i,j}(a) = \{a_i\, a_k{}^{-1},\ a_k\, a_j{}^{-1} : 1 \leqslant k \leqslant m,\ k \notin \{i,\ j\}\} \cup \{a_i a_k (a_j a_l)^{-1} : 1 \leqslant k \neq l \leqslant m,\ k, l \notin \{i,\ j\}\}.$$

Define the multisets $\Omega_{i,j}(a)$ for $1 \leqslant i < j \leqslant m$ by

$$\Omega_{i,j}(a) = a^* \setminus \left(\Gamma_{i,j}(a) \cup \{a_i\, a_j{}^{-1},\ a_j\, a_i{}^{-1}\}\right).$$

The multisets $\Omega_{i,j}(a)$ are used to produce equations which are satisfied by the elements of a, as shown in the next lemma.

Lemma 6.1. *Let a be an element of Z[free&nnor, m, A] with the elements of a labelled in ascending order. Let $\Omega_{i,j}(a)$ be the submultiset of a^* defined above for $1 \leqslant i < j \leqslant m$. Then there exists an element $e_{i,j}$ of $\Omega_{i,j}(a)$ such that the elements of a satisfy the equation*

$$a_i\, a_j{}^{-1} = e_{i,j}$$

for $1 \leqslant i < j \leqslant m$.

Proof. Since a is not recognisable, it follows that $\text{mult}(a_i\, a_j{}^{-1};\ a^*) > 1$ for $1 \leqslant i < j \leqslant m$. Suppose that $a_i\, a_j{}^{-1} = a_j\, a_i{}^{-1}$. Then, since a is not involution-recognisable, it follows that $\text{mult}(a_i\, a_j{}^{-1};\ a^*) > 2$ for this value of (i, j). Therefore there exists an element of $a^* \setminus \{a_i\, a_j{}^{-1},\ a_j\, a_i{}^{-1}\}$ which equals $a_i\, a_j{}^{-1}$, for $1 \leqslant i < j \leqslant m$. If $e_{i,j}$ is an element of $\Gamma_{i,j}(a)$ then the equation $a_i\, a_j{}^{-1} = e_{i,j}$ contradicts the fact that a is multiplicity-free, and so cannot be satisfied by the elements of a. □

Suppose that $e_{i,j}$ is an element of $\Omega_{i,j}(a)$ which satisfies $a_i a_j{}^{-1} = e_{i,j}$, where $1 \leqslant i < j \leqslant m$. Let $E_{i,j}$ denote the equation obtained from the equation $a_i a_j{}^{-1} = e_{i,j}$ by multiplying this equation by a_j and by any element of a whose inverse appears in $e_{i,j}$. Call $E_{i,j}$ the *equation extension* of $e_{i,j}$. The elements of a can be considered as variables in the equations $E_{i,j}$. Note that any variable which appears in $E_{i,j}$ appears to the first or second power. An action of the symmetric group $\text{Sym}(m)$ can be defined upon expressions or equations involving the variables $a_1, \ldots, a_m$, as follows. An element σ of $\text{Sym}(m)$ acts on an expression or equation involving the variables $a_1, \ldots, a_m$ by replacing a_k by $a_{k\sigma}$ for $1 \leqslant k \leqslant m$. It is easy to prove the following lemma.

Lemma 6.2. *Let a be an element of Z[free&nnor, m, A], and let $e_{i,j}$ be an element of $\Omega_{i,j}(a)$ such that the elements of a satisfy the equation $a_i a_j{}^{-1} = e_{i,j}$, where $1 \leqslant i < j \leqslant m$. Let $E_{i,j}$ be the equation extension of $e_{i,j}$. Denote by $E_1, \ldots, E_5$ the following equations:*

$$E_1 : a_1\, a_2 = a_3\, a_4,$$
$$E_2 : a_1{}^2 = a_2\, a_3,$$
$$E_3 : a_1{}^2\, a_2 = a_3{}^2\, a_4,$$
$$E_4 : a_1{}^2\, a_2 = a_3\, a_4\, a_5,$$
$$E_5 : a_1\, a_2\, a_3 = a_4\, a_5\, a_6.$$

Then $E_{i,j}$ is equivalent under the action of $\text{Sym}(m)$ to exactly one of $E_1, \ldots, E_5$.

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

We can now prove the following theorem.

Theorem 6.2. *Suppose that* $m \geqslant 4$ *and that* $2(m-1) < |A|$. *Then*

$$|Z[\text{free\&nnor}, m, A]||A^{\{m\}}|^{-1} < \begin{cases} 54\,|A|^{-1} & \text{if} \quad m = 4, \\ 250\,|A|^{-1} & \text{if} \quad m = 5, \\ 830\,|A|^{-1} & \text{if} \quad m = 6, \\ m^6\,(9|A|)^{-1} & \text{if} \quad m \geqslant 7. \end{cases}$$

Proof. Let a be a given element of $Z[\text{free\&nnor}, m, A]$, and let $e_{1,2}$ be an element of $\Omega_{1,2}(a)$ such that the elements a_1, a_2 of a satisfy the equation $a_1\,{a_2}^{-1} = e_{1,2}$. Let $E_{1,2}$ be the equation extension of $e_{1,2}$. Then, by Lemma 6.2, the equation $E_{1,2}$ is equivalent to exactly one of equations $E_1, \ldots, E_5$ under the action of $\mathrm{Sym}(m)$. Let $\psi : A^m \to A^{\{m\}}$ be the natural map which sends the m-tuple $(a_1, \ldots, a_m)$ to the multiset $\{a_1, \ldots, a_m\}$. Let us say that an m-tuple is multiplicity-free if it contains no repeated entries. Denote by W_r the set of all multiplicity-free m-tuples $(a_1, \ldots, a_m)$ in A^m such that the entries of a satisfy the equation E_r, for $1 \leqslant r \leqslant 5$. If $E_{1,2}$ is equivalent to E_r then a is an element of $\psi(W_r)$. Therefore

$$Z[\text{free\&nnor}, m, A] \subseteq \psi(W_1) \cup \cdots \cup \psi(W_5).$$

Now W_4 is empty if $m = 4$ and W_5 is empty if $m < 6$. Otherwise

$$|W_r| \leqslant |A|(|A|-1)\cdots(|A|-m+2) \tag{12}$$

for $1 \leqslant r \leqslant 5$, as the equation E_r allows the value of one element of an m-tuple in W_r to be expressed uniquely in terms of the values of the remaining $m-1$ elements. Let ν_r denote the order of the stabiliser of the equation E_r under the action of $\mathrm{Sym}(m)$. Then every element of $\psi(W_r)$ has at least ν_r preimages in W_r. Therefore

$$|\psi(W_r)| \leqslant \frac{|W_r|}{\nu_r}$$

for $1 \leqslant r \leqslant 5$. Now $\nu_1 = 8(m-4)!$, $\nu_2 = 2(m-3)!$, $\nu_3 = 2(m-4)!$, $\nu_4 = 6(m-5)!$ if $m \geqslant 5$ and $\nu_5 = 72(m-6)!$ if $m \geqslant 6$. Suppose that $m \geqslant 7$. Then

$$\begin{aligned} |Z[\text{free\&nnor}, m, A]| &\leqslant |\psi(W_1)| + \cdots + |\psi(W_5)| \\ &\leqslant |A|\cdots(|A|-m+2)\left({\nu_1}^{-1} + \cdots + {\nu_5}^{-1}\right) \\ &= \frac{m!({\nu_1}^{-1} + \cdots + {\nu_5}^{-1})}{(|A|-m+1)}\binom{|A|}{m}. \end{aligned}$$

Therefore, using the values of $\nu_1, \ldots, \nu_5$ calculated above,

$$\begin{aligned} |Z[\text{free\&nnor}, m, A]||A^{\{m\}}|^{-1} &< \frac{m!({\nu_1}^{-1} + \cdots + {\nu_5}^{-1})}{(|A|-m+1)} \\ &< \frac{2m!({\nu_1}^{-1} + \cdots + {\nu_5}^{-1})}{|A|} \\ &< \frac{m^6 + 12m^5 + 45m^4 + 36m^3}{36|A|} \\ &< \frac{m^6}{9|A|}, \end{aligned}$$

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

since $2(m-1) < |A|$ and $m \geqslant 7$. The estimates for the small values of m can be proved similarly. □

Suppose that we had wanted to calculate the proportion of multisets in $A^{\{m\}}$ which are not recognisable, using this method. Let a be an element of $A^{\{m\}}$ which is not recognisable. It is possible that $e_{1,2}$ has the value $a_2 a_1{}^{-1}$. In this case the equation extension $E_{1,2}$ of $e_{1,2}$ has the form $a_1{}^2 = a_2{}^2$, which does not allow us to solve for one element of a uniquely in terms of the other $m-1$ elements. This is why the definition of the involution-recognisable property makes the calculations of this section much easier. Note that only the equation $E_{1,2}$ was considered in the proof of Theorem 6.2. It is possible to extend these methods to obtain a bound which is inversely proportional to $|A|^2$ by considering both equations $E_{1,2}$ and $E_{3,4}$. In fact one can prove that

$$|Z[\text{free\&nnor}, m, A]||A^{\{m\}}|^{-1} \leqslant \frac{m^{12}}{64|A|^2}$$

when $m \geqslant 12$.

Suppose that b is an element of $A^{\{n\}}$ which has an exterior square root which is neither recognisable nor involution-recognisable. If $|A|$ is larger than m^6 then Theorems 6.1 and 6.2 imply that such multisets are rare. Therefore, on most inputs, Algorithm MULT will find an exterior square root if one exists.

7. *Testing*

The author has implemented Algorithm MULT in the programming language GAP, version 3.4 (see [7]). The test runs were performed on an Silicon Graphics R4000 Indigo. As GAP version 3.4 is not compilable, it does not run particularly fast. For this reason, we have restricted our testing to multisets of size $n \leqslant 120$ (in fact, we have used $n \in \{10, 45, 105\}$). However, for compilable programming languages on faster machines, $n \leqslant 1000$ should be achievable.

Tests were performed to illustrate two sections of this paper. The heuristic arguments of Section 5.2 are illustrated by the tests presented in Section 7.1 and Table 1. These tests focus on how many times Procedures REC and INV are called by Algorithm MULT; the heuristic arguments suggest that there is at most one call per input multiset. Then the results of Section 6 are illustrated by the tests described in Section 7.2 and Table 2. These tests are designed to show that a high proportion of multisets are recognisable or involution-recognisable.

7.1. *Testing the number of times Procedures* REC *and* INV *are performed*

We tested the number of times that Procedures REC and INV are called upon input of multisets chosen in two different ways. This gives two types of test. The first chooses 100 multisets from $A^{\{n\}}$ uniformly at random, and inputs them to Algorithm MULT. For the second type of test, 100 multisets are chosen from $A^{\{m\}}$ uniformly at random. In either case, we note the *total* number of times Procedures REC and INV are performed over the 100 runs, and the *average* CPU time, in seconds, used by Algorithm MULT over these 100 tests (as recorded using the GAP function `Profile`). The tests were performed using two different abelian groups. The first abelian group, denoted by CY, is the cyclic group of order N, where $N = 11^6 - 1 = 1771560$ (specifically, CY is the *additive* abelian group of

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

Table 1: Results of test runs for multisets of various size over two abelian groups

m	n	A	type	Procedure REC	Procedure INV	av. time
5	10	CY	I	0	0	0.079
5	10	CY	II	100	0	0.140
10	45	CY	I	0	0	3.652
10	45	CY	II	100	0	6.627
15	105	CY	I	0	0	26.769
15	105	CY	II	100	0	63.957
5	10	EA	I	0	0	0.236
5	10	EA	II	0	146	0.305
10	45	EA	I	0	0	7.142
10	45	EA	II	0	100	8.016
15	105	EA	I	0	0	48.441
15	105	EA	II	0	100	55.815

integers modulo N). The second abelian group, denoted by EA, is the elementary abelian 2-group of order $2^{20} = 1048576$. The results of these tests are presented in Table 1.

We see that Procedures REC and INV were not called in any Type I test. In all but one of the tests of Type II, exactly one call to Procedure REC was made per multiset over the abelian group CY, and one call per multiset to Procedure INV over the abelian group EA. This illustrates the heuristic arguments of Section 5.2. The exception was the test where 100 multisets were chosen from $\mathrm{EA}^{\{5\}}$, and their exterior square was presented to Algorithm MULT. Here Procedure INV was performed 146 times, over the 100 tests. This is many more times than the heuristic arguments would suggest. However, $\omega = \omega^{-1}$ for every element $\omega \in \mathrm{EA}$. Suppose that $a \in \mathrm{EA}^{\{5\}}$. If the five elements $a_i a_j a_k a_l$ are distinct, $1 \leqslant i < j < k < l \leqslant 5$, then $a^{\wedge 2} a^{-\wedge 2}$ consists of these five distinct elements, each with multiplicity six. Now $m = 5$ and so $2(m-2) = 6$. If the ten elements $a_i a_j$ are distinct, $1 \leqslant i < j \leqslant 5$, then $L_2(b)$ consists of the 10 distinct elements of aa^{-1} and the five distinct elements of $a^{\wedge 2} a^{-\wedge 2}$. The expected number of elements of $L_2(b)$ to be processed up to and including the first element of aa^{-1} is

$$10 \sum_{j=1}^{6} \binom{5}{j-1} \binom{15}{j}^{-1} = \frac{16}{11}.$$

Hence over 100 trials the expected number of times that Procedure INV is performed is $1600/11$, which is very close to our value of 146. This gives an illustration of a situation where the heuristic arguments of Section 5.2 are not applicable. However, such situations are very rare: even when working with elementary abelian 2-groups, the phenomenon described above only occurs when $m = 5$.

7.2. *Testing the proportion of recognisable or involution-recognisable multisets*

The tests performed in this section are designed to illustrate that most multisets are either recognisable or involution-recognisable. Each test consisted of choosing 100 multisets in $A^{\{m\}}$ at random, and noting how many were recognisable, clearly recognisable, involution-recognisable or clearly involution-recognisable. These quantities are listed in the columns

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

Table 2: Numbers of recognisable or involution-recognisable multisets found in test runs for various groups

m	A	# RI	# R	# CR	# I	# CI
5	CY(5^2)	63	35	12	28	25
5	CY(5^4)	100	99	99	1	1
5	CY(5^6)	100	99	99	1	1
10	CY(10^2)	0	0	0	0	0
10	CY(10^4)	100	100	100	0	0
10	CY(10^6)	100	100	100	0	0
15	CY(15^2)	0	0	0	0	0
15	CY(15^4)	100	100	100	0	0
15	CY(15^6)	100	100	100	0	0
5	EA(2^5)	80	0	0	80	0
5	EA(2^{10})	100	0	0	100	0
5	EA(2^{14})	100	0	0	100	0
10	EA(2^7)	55	0	0	55	55
10	EA(2^{14})	100	0	0	100	100
10	EA(2^{20})	100	0	0	100	100
15	EA(2^8)	8	0	0	8	8
15	EA(2^{16})	100	0	0	100	100
15	EA(2^{24})	100	0	0	100	100

of Table 2 headed # R, # CR, # I, # CI respectively. The total number of multisets which were either recognisable or involution-recognisable is also presented in the column headed # RI. The first column holds the value of m, while the second column holds a description of the group from which the test set was taken. Two kinds of abelian group are considered. If A is the additive group of the integers modulo N, then we write CY(N) to describe the group. The other kind of group considered is an elementary abelian group of order 2^t, which we describe as EA(2^t). For each value of m we consider six abelian groups. The first three are the groups CY(m^{2j}) for $1 \leqslant j \leqslant 3$, while the final three are the groups EA($2^{\lceil \log(m^{2j}) \rceil}$) for $1 \leqslant j \leqslant 3$.

When $|A|$ is of the order of m^2, we do not find a large proportion of multisets to be recognisable or involution-recognisable. However, the situation improves enormously when $|A| \geqslant m^4$. Here *all* the multisets chosen in our tests were either recognisable or involution-recognisable. This suggests that Algorithm MULT might work quite well even in situations where the analysis of Section 6 is not reassuring. Also notice that, when $m = 5$, no involution-recognisable multiset consisting of elements from an elementary abelian 2-group was found to be clearly involution-recognisable. This illustrates the analysis presented at the end of Section 7.1. In all other tests with $|A| \geqslant m^4$, every recognisable multiset was also clearly recognisable; likewise, every involution-recognisable multiset was also clearly involution-recognisable. This lends further support to the heuristic arguments of Section 5.2.

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

8. *The special case of multisets of eigenvalues*

The definition of the exterior square of a multiset was motivated by the relationship between the eigenvalues of a matrix X and the eigenvalues of the matrix which represents the action of X on the exterior square of the underlying vector space (with respect to some fixed choice of basis). Denote the latter matrix by $X^{\wedge 2}$, and call it the *exterior square* of X. An algorithm which can determine whether a given matrix is *equal* to the exterior square of another is described in [2].

Another question is to determine whether a given matrix is *conjugate* to the exterior square of another matrix. We now describe how solve this problem when the given matrix is conjugate to the exterior square of an irreducible matrix.

A matrix is said to be *separable* if it has no repeated eigenvalues. Suppose that Y is a separable matrix in $M(n, F)$ with set of eigenvalues β. Let $X \in M(m, F)$. Then Y is conjugate to $X^{\wedge 2}$ if and only if the set α of eigenvalues of X satisfies $\alpha^{\wedge 2} = \beta$ (for proof, see [1]). Suppose that we could find an exterior square root α of β. Let

$$f(x) = \prod_{i=1}^{m} (x - \alpha_i),$$

and let X_f be the companion matrix of f. Any matrix with characteristic polynomial f is conjugate to X_f. Finally, ${X_f}^{\wedge 2}$ and Y are conjugate. In fact, we can easily construct a matrix w such that $\left({X_f}^{\wedge 2}\right)^w = Y$ (see [1] for details).

The difficulty lies in finding an exterior square root of the set β of eigenvalues of Y. If $\beta = \alpha^{\wedge 2}$ where α is recognisable or involution-recognisable, then Algorithm MULT will succeed in finding an exterior square root of β. What is the likelihood that α is recognisable or involution-recognisable? For the remainder of the paper, assume that F is finite. The analysis of Section 6 is not applicable, because α has a very complicted distribution even if X is chosen uniformly at random from, say, $\mathrm{GL}(m, F)$ (or $M(m, F)$).

Instead, we can show that α is recognisable (or involution-recognisable) whenever X satisfies certain conditions. For example, suppose that $X \in \mathrm{GL}(m, F)$ is irreducible. Let K be the splitting field of the characteristic polynomial of X. Then $K = F[\theta]$ for some eigenvalue θ of X. Moreover,

$$\alpha = \{\theta^{q^i} : 0 \leqslant i < m\}$$

where $q = |F|$. It is not difficult to show that α is recognisable (for example, take $g = \theta^{q-1}$ in the definition of recognisability). Suppose that $Y \in \mathrm{GL}(n, F)$ is conjugate to $X^{\wedge 2}$, and that β is the (multi)set of eigenvalues of Y. Then Algorithm MULT will certainly succeed in finding an exterior square root of β. Therefore we can construct (X, w) such that $\left(X^{\wedge 2}\right)^w = Y$, as above.

Thus we know how to determine whether a given matrix Y is conjugate to the exterior square of a another matrix X, at least in the case where X is irreducible. The map $X \mapsto X^{\wedge 2}$, when restricted to $\mathrm{GL}(m, F)$, is a group homomorphism. Therefore we can define the exterior square of a matrix group. The problem of recognising the exterior square of a matrix, up to conjugation, was motivated by the following problem: to construct an algorithm to recognise the exterior square of the special linear group, up to conjugation. This is the same thing as recognising the special linear group in its action on the exterior square of the underlying vector space. A polynomial-time Monte Carlo algorithm for recognising the special linear group in its natural action was given by Neumann and Praeger [5].

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

I am very grateful to the referee of this paper for bringing the recent work of Kantor and Seress [3] to my attention. They describe a Monte Carlo algorithm which takes as input a list of generators of a black box group. (A *black box group* is one in which elements are represented as bit strings of uniform length N, and the group operations can be performed on these elements. Matrix groups are examples of black box groups. For subgroups of $\mathrm{GL}(n, F)$ we have $N = O(n^2 \log(|F|))$.) The algorithm determines whether the input group is isomorphic (modulo scalars) to some classical group over a field of given characteristic, and if so returns an explicit representation. The running time is polynomial in N and q, where q is the size of the field over which the output representation is given. This algorithm could be used to determine whether a given subgroup $H \leqslant \mathrm{GL}(n, F)$ is isomorphic to $\mathrm{SL}(m, F)$ modulo scalars, and to construct an explicit representation if so. Then standard meataxe methods could be used to determine whether the representation is the exterior square representation. This would give an algorithm for recognising the exterior square of the special linear group with running time polynomial in n and $|F|$. (The referee also alerted me to the recent work of Bratus, Cooperman, Finkelstein and Linton. They have announced a similar algorithm, which determines whether the input group is isomorphic modulo scalars to the special linear group over a field of given characteristic, and returns an explicit representation if so. Their algorithm is said to be simpler and more efficient than that of Kantor and Seress (when the classical group is a special linear group), but still has running time which is polynomial in N and q, with notation as above.)

We now outline an approach which uses the multiset algorithm described in this paper, which could lead to an algorithm with running time polynomial in n and $\log(|F|)$. Let H be the input group; that is, $H \leqslant \mathrm{GL}(n, F)$ is given as a finite list L_H of generators. Say $Y \in H$ is *helpful* if Y is conjugate to the exterior square of an irreducible matrix. Let r be a small positive integer constant, say $r = 2$ or $r = 3$. Choose elements $Y \in H$ uniformly at random until one of the following happens: (i) we have found r helpful elements $Y_1, \ldots, Y_r$, or (ii) some maximum number of choices is exceeded. If $\mathrm{SL}(m, F) \leqslant G \leqslant \mathrm{GL}(m, F)$ then the proportion of irreducible matrices in G is at least $1/(m+1)$ [5, Lemma 2.3]. Therefore, if H is conjugate to the exterior square of a subgroup G containing $\mathrm{SL}(m, F)$ then H should contain a fair proportion of helpful matrices. By making sufficiently many random choices from H, we can ensure that the probability that we do not find at least r helpful matrices Y is at most $\varepsilon/2$, for any given tolerance ε. The number of choices required is polynomial in m and $\log(\varepsilon^{-1})$.

If (ii) happens, we return the message *'false'*, meaning that H is not conjugate to the exterior square of a matrix group containing $\mathrm{SL}(m, F)$. The probability that this output is incorrect is at most $\varepsilon/2$. Otherwise we have r matrices $Y_1, \ldots, Y_r \in H$ such that

$$Y_i = \left(X_i{}^{\wedge 2}\right)^{w_i},$$

where $(X_i, w_i) \in \mathrm{GL}(m, F) \times \mathrm{GL}(n, F)$ and X_i is irreducible for $1 \leqslant i \leqslant r$. If H is conjugate to the exterior square of some group G such that $\mathrm{SL}(m, F) \leqslant G \leqslant \mathrm{GL}(m, F)$ then the conjugating element w is unique up to scalar multiplication. This follows since $V \wedge V$ is an absolutely irreducible $F\mathrm{SL}(m, F)$-module. The challenge is to use the information we have to find a candidate conjugating matrix $w \in \mathrm{GL}(n, F)$: in particular, to find it in time polynomial in n and $\log(|F|)$.

If we could find a candidate w, up to scalar multiplication, then we proceed as follows. Let $L_H = [Z_1, \ldots, Z_k]$ be the list of generators of the input group H. Apply the algorithm

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press

given in [2] to ${Z_i}^{w^{-1}}$ to determine whether there exists $Q_i \in \mathrm{GL}(m, F)$ such that

$$Q_i{}^{\wedge 2} = {Z_i}^{w^{-1}},$$

for $1 \leqslant i \leqslant k$. If such a matrix cannot be found, for some i, then H is not conjugate to the exterior square of any subgroup of $\mathrm{GL}(m, F)$. Otherwise, let $L = [Q_1, \ldots, Q_k]$ and let G be the group generated by these matrices. We know that $H = \left(G^{\wedge 2}\right)^w$. Use the Neumann–Praeger algorithm [5] to determine whether $\mathrm{SL}(m, F) \leqslant G$. There is a small probability of an incorrect negative response, which we can ensure is at most $\varepsilon/2$. Thus the overall probability of an incorrect negative response is at most ε. Note that all known elements of the algorithm outlined above have running time which is polynomial in n and $\log(|F|)$ (see [**1, 5**]).

Acknowledgements. Much of this work was carried out while I was a graduate student at the Mathematical Institute, University of Oxford. I would like to thank my supervisor, Dr. Peter Neumann, for suggesting this problem and for his generous assistance throughout my doctorate. I would especially like to thank Peter Neumann and Prof. Cheryl Praeger for helpful discussions on multiset factorisation problems. This research was supported by the University of Queensland, the Gowrie Scholarship Trust Fund and the Overseas Research Students Awards Scheme.

References

1. Catherine Greenhill, 'From multisets to matrix groups: some algorithms related to the exterior square', D. Phil. Thesis, The Mathematical Institute, University of Oxford, 1996. 114, 114, 116

2. Catherine Greenhill, 'An algorithm for recognising the exterior square of a matrix', *Linear and Multilinear Algebra* 46 (1999) 213–244. 114, 116

3. William M. Kantor and Ákos Seress, 'Black box classical groups', *Mem. Amer. Math. Soc.* To appear. 115

4. D. E. Knuth, *The art of computer programming, Vol.* 3*: Sorting and searching*, 2nd edn (Addison–Wesley, Reading, MA, 1981). 106

5. Peter M. Neumann and Cheryl E. Praeger, 'A recognition algorithm for special linear groups', *Proc. London Math. Soc.* (3) 65 (1992) 555–603. 114, 115, 116

6. Peter M. Neumann and Cheryl E. Praeger, 'On tensor factorisation problems', Unpublished manuscript, Oxford, 1997. 96

7. Martin Schönert and others, *GAP – groups, algorithms, and programming*, 5th edn (Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 1995). Available from the Department of Computer Science, University of St. Andrews, http://www-gap.dcs.st-and.ac.uk/ gap/. 111

Catherine Greenhill csg@scs.leeds.ac.uk

School of Computer Studies
University of Leeds
Leeds LS2 9JT

https://doi.org/10.1112/S1461157000000231 Published online by Cambridge University Press