COMPUTING SCIENCE

On $O(n^2 \log n)$ algorithms for $n \times n$ matrix operations

James Eve

TECHNICAL REPORT SERIES

No. CS-TR-1169 August 2009

TECHNICAL REPORT SERIES

No. CS-TR-1169 August, 2009

On $O(n^2 \log n)$ algorithms for $n \times n$ matrix operations

J. Eve

Abstract

If (without loss of generality) $n = p^t$, where p is prime, divide and conquer Fourier transforms using $O(n^2 \log n)$ operations reduce multiplying, or inverting nonsingular, complex $n \times n$ matrices to abelian group algebra convolutions.

If M is a complex $2^t \times 2^t$ matrix, constructing a unitary matrix T and an upper triangular matrix $T^{-1}MT$ reduces to $n(n-1)/2$ such constructions in which a 2×2 matrix μ is transformed to an upper triangular matrix $\tau^{-1}\mu\tau$ by a unitary matrix τ that represents a quaternion. The diagonal elements of $T^{-1}MT$ are the eigenvalues of M and, if M is normal, $T^{-1}MT$ is diagonal and the columns of T are then a complete orthonormal set of eigenvectors. So there is also an algorithm for the classical problem of solving polynomial equations.

Printed and published by the University of Newcastle upon Tyne,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

EVE, J.

On $O(n^2 \log n)$ algorithms for $n \times n$ matrix operations
[By] J. Eve
Newcastle upon Tyne: University of Newcastle upon Tyne: Computing Science, 2009.

(University of Newcastle upon Tyne, Computing Science, Technical Report Series, No. CS-TR-1169)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE
Computing Science. Technical Report Series. CS-TR-1169

Abstract

If (without loss of generality) $n = p^t$, where p is prime, divide and conquer Fourier transforms using $O(n^2 \log n)$ operations reduce multiplying, or inverting nonsingular, complex $n \times n$ matrices to abelian group algebra convolutions. If M is a complex $2^t \times 2^t$ matrix, constructing a unitary matrix T and an upper triangular matrix $T^{-1}MT$ reduces to $n(n-1)/2$ such constructions in which a 2×2 matrix μ is transformed to an upper triangular matrix $\tau^{-1}\mu\tau$ by a unitary matrix τ that represents a quaternion. The diagonal elements of $T^{-1}MT$ are the eigenvalues of M and, if M is normal, $T^{-1}MT$ is diagonal and the columns of T are then a complete orthonormal set of eigenvectors. So there is also an algorithm for the classical problem of solving polynomial equations.

About the author

James Eve joined the staff of Computing Laboratory, as it was then called, of the University of Newcastle upon Tyne in 1957. In 1960 he was appointed to a Lectureship, and in 1968 to a Senior Lectureship, a post he held until he retired in 1996. He continued his complexity theory research after his retirement, even after he became ill, until very shortly before he passed away in February 2009.

Suggested keywords
MATRIX MULTIPLICATION
EIGENVALUES
COMPLEXITY THEORY

Introductory Remarks

Dr James (Jim) Eve passed away on 24 February 2009. He had worked on the subject of this report for many years, but in August 2008 he wrote:

> I am not being overly optimistic about the outcome of my present illness. Just in case pessimism is justified, I have worked quite hard in the last few weeks to get my stuff on matrix algorithms documented as fully and clearly as I can. My previous programming ventures have all revealed minor flaws in my reasoning which have easily been remedied but, since I have not yet been able to program the current versions, I am still not able to guarantee that I have all the details correct.
>
> I am very confident that I have found the right approach and that what I have done has cracked or is very close to cracking the problem of efficient algorithms for multiplying and inverting matrices and, more surprisingly, for solving the matrix eigenvalue problem since, at present, there is no known algorithm for the latter.

In line with Jim's wishes, his final draft is being issued as this Technical Report. As he wrote of his draft:

> Sadly, it all hinges on group representation theory which is not familiar territory even to most mathematicians. Even worse, the only current references seem to be of the Bourbaki school (fine if you already know but impenetrable if you are trying to find out).

He therefore also produced an informal explanatory document "Notes on the theories of finite groups and their representations" – this note is provided here in the form of an Appendix to the final draft.

Also attached is a note by Professor Donald Knuth, who kindly offered to read Jim's draft – unfortunately, Jim's health did not permit him to respond to this note before he passed away. Finally, there is a copy of the Address that I was honoured to be invited to make at the very well-attended Celebration of Jim's life, held on 9 March 2009.

Brian Randell

Newcastle upon Tyne
August 2009

On $O(n^2 \log n)$ algorithms for $n \times n$ matrix operations

James Eve

August 25, 2008

Abstract

If (without loss of generality) $n = p^t$, where p is prime, divide and conquer Fourier transforms using $O(n^2 \log n)$ operations reduce multiplying, or inverting non-singular, complex $n \times n$ matrices to abelian group algebra convolutions.

If M is a complex $2^t \times 2^t$ matrix, constructing a unitary matrix T and an upper triangular matrix $T^{-1}MT$ reduces to $n(n-1)/2$ such constructions in which a 2×2 matrix μ is transformed to an upper triangular matrix $\tau^{-1}\mu\tau$ by a unitary matrix τ that represents a quaternion. The diagonal elements of $T^{-1}MT$ are the eigenvalues of M and, if M is normal, $T^{-1}MT$ is diagonal and the columns of T are then a complete orthonormal set of eigenvectors. So there is also an algorithm for the classical problem of solving polynomial equations.

1 Introduction

In supplying algorithms to multiply, invert and compute determinants of $n \times n$ matrices in $O(n^\alpha)$ arithmetic operations, where $\alpha = \log_2 7 < 3$, Strassen [26] instigated a search for more efficient matrix multiplication algorithms. The motivation is considerable; apart from obvious applications in computational linear algebra, the best algorithms currently known for diverse problems, including computing the transitive closure of a directed graph [15] and recognising a sentence in a context free language [27], have complexities dominated by that of matrix multiplication. It has subsequently been shown [1] that if matrices can be multiplied in $O(n^{2+\varepsilon})$ arithmetic operations, where $\varepsilon > 0$, then $O(n^{2+\varepsilon})$ operations suffice for matrix inversion and computing determinants. Modification of the proof of theorem 6.4 in [1] to accommodate the even more optimistic assumption of matrix multiplication in $O(n^2 \log n)$ operations shows that $O((n \log n)^2)$ algorithms would exist for the other two problems.

More recent work has been reported and surveyed by Pan [19, 20], Schönhage [24] and Coppersmith and Winograd [8, 9]. This shows $\alpha < 2.5$ is possible for extremely large n but seems to offer little prospect of practical methods. An alternative approach was suggested by an observation relating to a set of equations with solutions defining matrix multiplication algorithms.

Proposition 1.1 (Brent [4].) Elements of the $n \times n$ matrix product $C = AB$ are to be constructed from linear combinations of κ products in which the operands are linear combinations of the elements of A and B respectively. Specifically, given κ triples of constant $n \times n$ matrices, $((\alpha_{mk}^{(v)}), (\beta_{li}^{(v)}), (\gamma_{js}^{(v)}))$ where $1 \le v \le \kappa$, if

$$C_{js} = \sum_{v=1}^{\kappa} \Big(\sum_{m,k} A_{km} \alpha_{mk}^{(v)} \Big) \Big(\sum_{l,i} B_{il} \beta_{li}^{(v)} \Big) \gamma_{js}^{(v)}, \text{ for all } j \text{ and } s \text{ in } [0, n) \tag{1.1}$$

then the $3n^2\kappa$ elements of the 3κ constant matrices satisfy Brent's set of n^6 equations,

$$\sum_{v=1}^{\kappa} \gamma_{js}^{(v)} \beta_{li}^{(v)} \alpha_{mk}^{(v)} = \delta_{ls} \delta_{mi} \delta_{jk}, \text{ for all } i, j, k, l, m \text{ and } s \text{ in } [0, n), \tag{1.2}$$

where $\delta_{xy} = 1$ if $x = y$ and $\delta_{xy} = 0$ if $x \ne y$.

Proof Equate coefficients of $A_{km}B_{il}$ in (1.1) with those in $C_{js} = \sum_r A_{jr}B_{rs}$. ∎

The standard $O(n^3)$ method of multiplying matrices provides solutions of (1.2), for all n, with $\kappa = n^3$. Strassen's method, for $2^t \times 2^t$ matrices, implies solutions with $\kappa = 7^t$. The κ multiplications in these algorithms in which neither operand is a constant have been called *active multiplications* [2]. Their significance, in the context of matrix multiplication, stems from Brent's generalisation of Strassen's method. He showed (alternatively, see [1, theorem 2.1 and (6.2) with 2 replaced by c in the latter]) that any solution of (1.2) for $c \times c$ matrices with $\kappa > c^2$ active multiplications implies an $O(n^{\log_c \kappa})$ algorithm for multiplying $n \times n$ matrices when $n = c^t$. Effort subsequently has largely been devoted to finding (c, κ) pairs that reduce $\log_c \kappa$. (If $\kappa = c^2$, theorem 2.1 in [1], known as the divide and conquer theorem, implies an $O(n^2 \log n)$ algorithm.)

Equations similar to Brent's occur in the theory of representations of finite groups. The next proposition covers one of two cases that arise in deriving the orthogonality relations for the irreducible matrix representations of such groups [25, corollaries 1 to 3 of proposition 4]. Corollary 1.2 appears to be new.

Proposition 1.2 If X is any $n \times n$ matrix, ρ is an irreducible $n \times n$ matrix representation of a finite group G of order $|G|$ and $\rho(g)$ is the representation of g in G by ρ then

(i) $$\sum_{g \in G} \sum_{s,l} \rho_{ms}(g) X_{sl} \rho_{li}(g^{-1}) = |G| n^{-1} \sum_{s,l} X_{sl} \delta_{ls} \delta_{mi},$$

(ii) $$\sum_{g \in G} \rho_{ms}(g) \rho_{li}(g^{-1}) = |G| n^{-1} \delta_{ls} \delta_{mi}.$$

Proof Let $A = \sum_{g \in G} \rho(g) X \rho(g^{-1})$; if h is any element in G then

$$\rho(h) A \rho(h^{-1}) = \sum_{g \in G} \rho(hg) X \rho((hg)^{-1}) = A$$

and A commutes with every matrix in the irreducible representation ρ. By Schur's Lemma [25, proposition 4] $A = \lambda 1_n$, a scalar multiple of the $n \times n$ unit matrix, so

$$\lambda \;=\; n^{-1} \sum_{g \in G} \mathrm{tr}(\rho(g) X \rho(g^{-1})) \;=\; n^{-1} \sum_{g \in G} \mathrm{tr}(\rho(g^{-1}) \rho(g) X) \;=\; |G| n^{-1} \sum_{s,l} X_{sl} \delta_{ls}$$

and $\sum_{g \in G} \sum_{s,l} \rho_{ms}(g) X_{sl} \rho_{li}(g^{-1}) = A_{mi} = \lambda \delta_{mi} = |G| n^{-1} \sum_{s,l} X_{sl} \delta_{ls} \delta_{mi}$ proving (i). Equating coefficients of X_{sl} in (i) results in the orthogonality relations (ii).

Corollary 1.2 If X and Y are any $n \times n$ matrices then

(i) $$\sum_{g_0, g_1 \in G} \sum_{s,l,i,m} \rho_{js}(g_0 g_1) X_{sl} \rho_{li}(g_1^{-1}) Y_{im} \rho_{mk}(g_0^{-1}) = |G|^2 n^{-2} \sum_{s,l,i,m} X_{sl} Y_{im} \delta_{ls} \delta_{mi} \delta_{jk},$$

(ii) $$\sum_{g_0, g_1 \in G} \rho_{js}(g_0 g_1) \rho_{li}(g_1^{-1}) \rho_{mk}(g_0^{-1}) = |G|^2 n^{-2} \delta_{ls} \delta_{mi} \delta_{jk}.$$

Proof Let $A = \sum_{g_0, g_1 \in G} \rho(g_0 g_1) X \rho(g_1^{-1}) Y \rho(g_0^{-1})$; $A = \lambda 1_n$ again follows and similarly

$$\begin{aligned}
\lambda &= n^{-1} \sum_{g_0, g_1 \in G} \mathrm{tr}(\rho(g_0 g_1) X \rho(g_1^{-1}) Y \rho(g_0^{-1})) \\
&= n^{-1} \sum_{g_0, g_1 \in G} \mathrm{tr}(\rho(g_0^{-1}) \rho(g_0 g_1) X \rho(g_1^{-1}) Y) \\
&= n^{-1} \sum_{g_0, g_1 \in G} \mathrm{tr}(\rho(g_1) X \rho(g_1^{-1}) Y) \\
&= |G| n^{-1} \sum_{g \in G} \mathrm{tr}(\rho(g) X \rho(g^{-1}) Y) \\
&= |G| n^{-1} \sum_{i,m} \Big(\sum_{g \in G} \sum_{s,l} \rho_{ms}(g) X_{sl} \rho_{li}(g^{-1}) \Big) Y_{im}.
\end{aligned}$$

So, by proposition 1.2(i), $\lambda = |G|^2 n^{-2} \sum_{s,l,i,m} X_{sl} Y_{im} \delta_{ls} \delta_{mi}$ and

$$\sum_{g_0,g_1 \in G} \sum_{s,l,i,m} \rho_{js}(g_0 g_1) X_{sl} \rho_{li}(g_1^{-1}) Y_{im} \rho_{mk}(g_0^{-1}) =$$
$$A_{jk} = \lambda \delta_{jk} = |G|^2 n^{-2} \sum_{s,l,i,m} X_{sl} Y_{im} \delta_{ls} \delta_{mi} \delta_{jk}$$

proving (i), from which (ii) follows on equating coefficients of $X_{sl} Y_{im}$. ∎

Corollary 1.2(ii) shows that any group with $n \times n$ irreducible representations provides a solution of Brent's equations. Comparing (1.2) with corollary 1.2(ii), the factors $\sum_{m,k} A_{km} \alpha_{mk}^{(v)}$ and $\sum_{l,i} B_{il} \beta_{li}^{(v)}$ in (1.1) can be identified with $n|G|^{-1}\mathrm{tr}(A\rho(g_0^{-1}))$ and $n|G|^{-1}\mathrm{tr}(B\rho(g_1^{-1}))$, $\gamma^{(v)}$ with $\rho(g_0 g_1)$ and κ with $|G|^2$. As any group with $n \times n$ irreducible matrix representations must contain at least n^2 elements [25, corollary 2(a) of proposition 5], these solutions are of no direct interest since there are at least n^4 active multiplications. Their existence does however suggest a closer examination of families of groups with arbitrarily large irreducible matrix representations.

A second observation also points to group representations; there is a Fourier transform algorithm for multiplying elements in a group algebra. Fourier transform algorithms compute a convolution equivalent to multiplication and seem invariably to lead to efficient algorithms for multiplying ring elements. In [2], it is shown that such an algorithm, using matrix multiplication with the irreducible representations of the group, can significantly reduce the number of arithmetic operations needed to compute group algebra products. Darwin's "Other-Way-Round" principle [16] suggests that group algebra products may also be the source of efficient matrix multiplication algorithms.

By inductive extension,

$$\sum_{\substack{g_r \in G \\ 0 \le r < q}} \rho_{k_0 k'_q}(g_0 g_1 \dots g_{q-1}) \rho_{k_q k'_{q-1}}(g_{q-1}^{-1}) \dots \rho_{k_1 k'_0}(g_0^{-1}) = |G|^q n^{-q} \prod_{r=0}^{q} \delta_{k_r k'_r}.$$

Solutions provide algorithms for the product of q rather than two matrices.

In section 2, a family of groups $G(p,t)$ is introduced where p is an arbitrary prime; these groups have one dimensional and $p^t \times p^t$ irreducible matrix representations. The groups and, for $p = 2$, the form and some of the properties of their representations, are known though the results are widely scattered and, in any event, require some reformulation for use here. Basic results from the theory of representations of finite groups [10, 25] are used throughout this section; most can be more easily found, concisely and elegantly derived, in part I of the latter reference which is preferentially cited. The following results are also used.

Proposition 1.3 [1, lemma 7.1] If ω is a principal mth root of 1 and i and j are integers in the range $[0, m)$ then $\sum_{k=0}^{m-1} \omega^{(i-j)k} = m\delta_{ij}$.

Corollary 1.3 The $m \times m$ matrix M with elements $M_{ik} = \omega^{ik}$ has an inverse with elements $(M^{-1})_{ik} = (mM_{ik})^{-1}$. ∎

After constructing the irreducible representations, it is shown that a basis for complex $p^t \times p^t$ matrices is provided by the matrices in $\rho_\Phi^{(t)}$, the restriction of an irreducible $p^t \times p^t$ representation $\rho^{(t)}$ of $G(p,t)$ to a subset Φ of its elements. This implies a bijective mapping between $\mathbf{C}^{p^t \times p^t}$, the vector space of complex $p^t \times p^t$ matrices, and $\mathbf{C}\rho_\Phi^{(t)}$, the vector space over $\mathbf{C}$ with matrices in $\rho_\Phi^{(t)}$ as basis. Some properties of these representations are also established.

Section 3 treats two Fourier transforms. One permits efficient transformation between vectors in $\mathbf{C}\rho_\Phi^{(t)}$ and the corresponding matrices in $\mathbf{C}^{p^t \times p^t}$, the other stems from representations of the abelian group of inner automorphisms of $G(p,t)$.

The matrix algebra algorithms based on these transforms appear in section 4.

2 The groups $G(p,t)$

Let p be any prime; C_{p^r} and C_p^s denote the cyclic group of order p^r and the direct product of s copies of C_p. The abbreviations $\sum$ for $\sum_{j=1}^{t}$ and $\prod$ for $\prod_{j=1}^{t}$ are used throughout; otherwise, unless it is clear from context, limits are stated explicitly.

The groups $G(p,t)$ for odd primes differ markedly from the $p=2$ family. Accordingly, let $\sigma=2$ if $p=2$ and $\sigma=1$ if p is odd. For $p=2$ there are three subfamilies denoted by $G_0(2,t)$, $G_1(2,t)$ and $G_2(2,t)$ when distinction is necessary.

Proposition 2.1 There are groups $G(p,t)$ of order p^{2t+1} and exponent σp with generators A_k where $-t\le k\le t$ and elements

$$A_0^{a_0}\prod A_{-j}^{a_{-j}}A_j^{a_j},\quad 0\le a_r<p,\quad -t\le r\le t \tag{2.1}$$

given that the generators satisfy

$$\begin{aligned}&\text{(i) } A_rA_s=\begin{cases}A_0A_sA_r & \text{if } r=-s \text{ and } s>0,\\ A_sA_r & \text{otherwise,}\end{cases}\\ &\text{(ii) } A_k^p=1 \text{ except } A_k^2=A_0 \text{ for } k>0 \text{ in } G_1(2,t) \text{ and for } k\ne 0 \text{ in } G_2(2,t).\end{aligned} \tag{2.2}$$

Proof The relations (2.2(i)) enable the transposition of adjacent generators and assert that A_0 commutes with all other generators so, for two elements from (2.1),

$$\Big(A_0^{a_0}\prod A_{-j}^{a_{-j}}A_j^{a_j}\Big)\Big(A_0^{b_0}\prod A_{-j}^{b_{-j}}A_j^{b_j}\Big)=A_0^{a_0+b_0+c}\prod A_{-j}^{a_{-j}+b_{-j}}A_j^{a_j+b_j},$$

where A_0^c combines all factors A_0^{-1} introduced by using (2.2(i)). Exponents in this last expression can be brought into the ranges specified in (2.1) by applying (2.2(ii)) where necessary; for $G(2,t)$ the exponent of A_0 is treated last enabling any further factors of A_0 to be combined with $A_0^{a_0+b_0+c}$. The elements (2.1) are therefore closed under multiplication which is associative since the multiplication of generators is associative.

For $g=A_0^{a_0}\prod A_{-j}^{a_{-j}}A_j^{a_j}$, by the second of (2.2(i)) and $A_0^p=1$, $g^{\sigma p}=\prod(A_{-j}^{a_{-j}}A_j^{a_j})^{\sigma p}$. But $(A_{-j}^{a_{-j}}A_j^{a_j})^{\sigma p}=A_{-j}^{a_{-j}}A_j^{a_j}\,.\,A_{-j}^{a_{-j}}A_j^{a_j}\,.\,A_{-j}^{a_{-j}}A_j^{a_j}\ldots A_{-j}^{a_{-j}}A_j^{a_j}$ and moving the second instance of $A_{-j}^{a_{-j}}$ left past $A_j^{a_j}$, using the first of (2.2(i)), creates an initial factor $A_{-j}^{2a_{-j}}$ and introduces $A_0^{-a_{-j}a_j}$. Moving the next instance of $A_{-j}^{a_{-j}}$ left past *two* instances of $A_j^{a_j}$ creates an initial factor $A_{-j}^{3a_{-j}}$ and introduces $A_0^{-2a_{-j}a_j}$. By induction, on summing the arithmetic progression for the exponent of A_0 then using (2.2(ii)) with the fact that $\sigma(\sigma p-1)/2$ is an integer

$$(A_{-j}^{a_{-j}}A_j^{a_j})^{\sigma p}=(A_{-j}^{\sigma p})^{a_{-j}}(A_j^{\sigma p})^{a_j}(A_0^p)^{-\sigma(\sigma p-1)a_{-j}a_j/2}=1.$$

Hence $g^{\sigma p}=1$ and $g^{-1}=g^{\sigma p-1}$ completing the proof that the set of elements (2.1) form a group with exponent σp. ∎

Proposition 2.2 $Z_p=\{A_0^{a_0}:0\le a_0<p\}=C_p$ is the centre of $G(p,t)$.
Proof Let $g=A_0^{a_0}\prod A_{-j}^{a_{-j}}A_j^{a_j}$; for $r>0$, by (2.2(i)), $A_{-r}g=A_0^{a_r}gA_{-r}$. So if g commutes with A_{-r} then $a_r=0$. Similarly, if g commutes with A_r then $a_{-r}=0$. If g is in the centre, it commutes with all elements and so all generators of $G(p,t)$. But then $a_j=0$ for all nonzero j and $g=A_0^{a_0}$. ∎

2.1 The irreducible representations of $G(p,t)$

Proposition 2.3 $G(p,t)$ has p^{2t} one dimensional and $p-1$ classes of $p^t\times p^t$ irreducible matrix representations.
Proof For elements h and g in $G(p,t)$, (2.2) implies $hg=A_0^rgh$ for some r in $[0,p)$. So

(i) $h^{-1}g^{-1}hg = A_0^r$ and Z_p is also the commutator subgroup of $G(p,t)$. As the quotient group of any group by its commutator subgroup is the largest abelian quotient group [23, theorem 3.52], there are p^{2t} one dimensional representations of $G(p,t)/Z_p$ [25, theorem 9] and so of $G(p,t)$—see (2.4) below.

(ii) $g^{-1}hg = A_0^r h$ and conjugate classes of $G(p,t)$ other than those of a single commuting element from the centre are cosets of Z_p in $G(p,t)$.

Proposition 2.2 implies p single element classes; according to (ii), the remaining $p(p^{2t}-1)$ elements of $G(p,t)$ split into $p^{2t}-1$ classes making $p^{2t}+p-1$ conjugate classes in all. As this is also the number of classes of irreducible representations [25, theorem 7], in addition to the p^{2t} one dimensional classes there are $p-1$ others.

The order of a group is equal to the sum of the squares of the matrix dimension for each irreducible class [25, corollary 2(a) of proposition 5] and

$$p^{2t+1} = p^{2t}.1^2 + (p-1).(p^t)^2 \tag{2.3}$$

suggests $p-1$ $p^t \times p^t$ representations. Proposition 2.6 completes the proof. ∎

It is convenient to use ω to denote both the generator of C_p and also a value which represents the generator. When $p=2$, the real value $\omega=-1$ is unique and when p is odd, there are $p-1$ possible values for ω, all complex.

The one dimensional representations are easily obtained. Putting $A_0 = 1$ annihilates Z_p and (2.2) then shows that $G(p,t)$ degenerates to C_p^{2t}. This is the quotient group. It supplies representations of $G(p,t)$ through the homomorphism,

$$G(p,t) \to G(p,t)/Z_p \;;\; A_0^{a_0} \prod A_{-j}^{a_{-j}} A_j^{a_j} \mapsto \prod \omega_{-j}^{a_{-j}} \omega_j^{a_j}, \tag{2.4}$$

where ω_j for $1 \le |j| \le t$ are the generators of the $2t$ copies of C_p.

If a_j where $1 \le |j| \le t$ are regarded as the $2t$ digits of a radix p integer then each such integer, through its digits (as shown in (2.4)), specifies the exponents of a unique quotient group element. Let r and s be such integers with digits r_j and s_j for $1 \le |j| \le t$. The one dimensional representations can be displayed in a $p^{2t} \times p^{2t}$ array in which the (r,s) element is the representation of the quotient group element with exponents defined by the digits of s in the rth representation. Its elements are those of the nonsingular matrix W,

$$W_{rs} = \prod \omega^{(r_{-j}s_{-j} + r_j s_j)}, \quad (W^{-1})_{rs} = (p^{2t} W_{rs})^{-1}. \tag{2.5}$$

The identity $W^{-1}W = 1$ is an extension of corollary 1.3 and shows the satisfaction of the orthogonality relations [25, corollaries 2 and 3 of proposition 4] for these representations.

The *tensor product* $U \otimes V$ of a $u \times u$ matrix U and a $v \times v$ matrix V is a $uv \times uv$ matrix with elements $(U \otimes V)_{(u_1,v_1)(u_2,v_2)} = U_{u_1 u_2} V_{v_1 v_2}$. Ordering of rows and columns of $U \otimes V$ is chosen here so that $UV_{v_1 v_2}$ is the (v_1, v_2) $u \times u$ submatrix of $U \otimes V$; that is, (u_i, v_i) precedes (u_j, v_j) if $v_i < v_j$ or if $v_i = v_j$ and $u_i < u_j$.

In a *p-Hadamard matrix* all elements in the first row and first column are 1; in every other row or column only the p distinct pth roots of 1 occur, each equally often.

The matrix W in (2.5) is p-Hadamard for all p. Denoting it by $W^{(2t)}$, to indicate that it is the matrix of one dimensional representations of C_p^{2t}, its definition implies $W^{(2)} = W^{(1)} \otimes W^{(1)}$ and $W^{(2t)} = W^{(2)} \otimes W^{(2t-2)}$. Since the tensor product of p-Hadamard matrices is a p-Hadamard matrix and $W^{(1)}$ is a $p \times p$ p-Hadamard matrix, it follows by induction on t that $W^{(2t)}$ is a p-Hadamard matrix.

Any set of $2t+1$ $p^t \times p^t$ matrices satisfying (2.2) is a set of generator representations that will generate a $p^t \times p^t$ representation. Construction of such a representation then reduces to constructing a set of generator representations. Let $S(p,t)$ denote such a set

with members $A_j^{(t)}$, $-t \le j \le t$; when t is not in question, superscripts are suppressed so that A_j too, like ω, subsequently denotes both generator and representation.

A *monomial matrix* has one nonzero element in each row and column. The $r\times r$ unit matrix, 1_r, is monomial. A *homothety* is a scalar multiple of an algebra identity element such as the unit matrix. The notation $[u]_v$ is preferred to $u(\mathrm{mod}\ v)$.

Factors $\omega^{(p-1)/2}$ occur below; when p is odd these are powers of ω but, for $p=2$, it is necessary to introduce ζ such that $\zeta^2=\omega$, where ζ is represented by $\pm\sqrt{-}1$.

Proposition 2.4 For $0 \le j < p$, the $p\times p$ monomial matrices X and Y have nonzero elements $X_{j\,[j+1]_p}=1$ and $Y_{jj}=\omega^j$. They satisfy $X^p=Y^p=1_p$ and $XY=\omega YX$.
Proof The sets $\{X^j : 0\le j<p\}$ and $\{Y^j : 0\le j<p\}$ are respectively the regular and irreducible representations of C_p so $X^p=Y^p=1_p$. The nonzero elements of XY and YX are $(XY)_{j\,[j+1]_p}=\omega^{j+1}$ and $(YX)_{j\,[j+1]_p}=\omega^j$.

Corollary 2.4 Let $Y'=\omega^{-(p-\sigma)/2}Y$. Then $X^p=(Y')^p=1_p$ and $XY'=\omega Y'X$.
Proof If $p=2$, $Y'=Y$ and there is nothing more to prove.

If p is odd, $(Y')^p=(\omega^p)^{-(p-1)/2}Y^p=1_p$ and $XY'=\omega Y'X$ is merely $XY=\omega YX$ multiplied by $\omega^{-(p-1)/2}$. ∎

As A_0 commutes with all generators, it is represented by a homothety and, as $A_0^p=1$, ω is a suitable scalar. Corollary 2.4 justifies

$$\begin{aligned}
&\text{(i) for } G_2(2,1):\ S(2,1)=\{A_0=\omega 1_2,\quad A_{-1}=\zeta X,\quad A_1=\zeta Y'\},\\
&\text{(ii) for } G_1(2,1):\ S(2,1)=\{A_0=\omega 1_2,\quad A_{-1}=X,\quad A_1=\zeta Y'\},\\
&\text{(iii) otherwise}\quad :\ S(p,1)=\{A_0=\omega 1_2,\quad A_{-1}=X,\quad A_1=Y'\}.
\end{aligned}\tag{2.6}$$

The representations generated by $S(2,1)$ contain

$$\begin{aligned}
&\text{(i)}\ \text{ for } G_0(2,1):\ 1=\begin{pmatrix}1&\\&1\end{pmatrix},\ A_{-1}=\begin{pmatrix}&1\\1&\end{pmatrix},\ A_1=\begin{pmatrix}1&\\&-1\end{pmatrix},\ A_{-1}A_1=\begin{pmatrix}&-1\\1&\end{pmatrix},\\
&\text{(ii)}\ \text{ for } G_1(2,1):\ 1=\begin{pmatrix}1&\\&1\end{pmatrix},\ A_{-1}=\begin{pmatrix}&1\\1&\end{pmatrix},\ A_1=\begin{pmatrix}\zeta&\\&-\zeta\end{pmatrix},\ A_{-1}A_1=\begin{pmatrix}&-\zeta\\\zeta&\end{pmatrix},\\
&\text{(iii)}\ \text{ for } G_2(2,1):\ 1=\begin{pmatrix}1&\\&1\end{pmatrix},\ A_{-1}=\begin{pmatrix}&\zeta\\\zeta&\end{pmatrix},\ A_1=\begin{pmatrix}\zeta&\\&-\zeta\end{pmatrix},\ A_{-1}A_1=\begin{pmatrix}&1\\-1&\end{pmatrix}
\end{aligned}\tag{2.7}$$

and these matrices multiplied by $A_0=\omega 1_2$.

The representation generated by $S(3,1)$ contains

$$\begin{aligned}
1&=\begin{pmatrix}1&&\\&1&\\&&1\end{pmatrix},\quad A_1=\begin{pmatrix}\omega^2&&\\&1&\\&&\omega\end{pmatrix},\quad A_1^2=\begin{pmatrix}\omega&&\\&1&\\&&\omega^2\end{pmatrix},\\
A_{-1}&=\begin{pmatrix}&1&\\&&1\\1&&\end{pmatrix},\quad A_{-1}A_1=\begin{pmatrix}&1&\\&&\omega\\\omega^2&&\end{pmatrix},\quad A_{-1}A_1^2=\begin{pmatrix}&1&\\&&\omega^2\\\omega&&\end{pmatrix},\\
A_{-1}^2&=\begin{pmatrix}&&1\\1&&\\&1&\end{pmatrix},\quad A_{-1}^2A_1=\begin{pmatrix}&&\omega\\\omega^2&&\\&1&\end{pmatrix},\quad A_{-1}^2A_1^2=\begin{pmatrix}&&\omega^2\\\omega&&\\&1&\end{pmatrix}
\end{aligned}$$

and these matrices multiplied by $A_0=\omega 1_3$ and A_0^2.

For $t>1$, $S(p,t)$ is constructed by induction on t using $S(p,1)$ as a base.

Proposition 2.5 Given $S(p,1)$, as defined in (2.6), then

$$S(p,t)=\{A_j^{(t)}=A_j^{(t-1)}\otimes 1_p :\ A_j^{(t-1)}\in S(p,t-1)\}\bigcup \{A_{-t}^{(t)}=1_{p^{t-1}}\otimes A_{-1}^{(1)},\ A_t^{(t)}=1_{p^{t-1}}\otimes A_1^{(1)}\}$$

Proof It must be shown that these matrices satisfy (2.2).

The pair $A_{-t}^{(t)}$, $A_t^{(t)}$ satisfy (2.2) because $A_{-1}^{(1)}$, $A_1^{(1)}$ do so; scalar elements in the latter are replaced by corresponding homotheties in the former.

The first subset of $S(p,t)$ contains block diagonal matrices with identical diagonal blocks which will multiply homotheties in members of the second subset so allowing members of the first subset to commute with both members of the second subset.

Finally, members of the first subset collectively satisfy (2.2) as the diagonal blocks, being the members of $S(p,t-1)$, do so by the inductive hypothesis. ∎

As there are $p-1$ possible values for ω, proposition 2.5 delivers $p-1$ distinct $p^t\times p^t$ representations. When p is odd, they split into $(p-1)/2$ complex conjugate pairs.

Proposition 2.6 The $p-1$ $p^t\times p^t$ representations generated by proposition 2.5 with the p^{2t} one dimensional representations defined by (2.4) and (2.5) are a complete set of irreducible representations for $G(p,t)$.

Proof With (2.3) satisfied, it suffices [25, remark(1) after proposition 5 and corollary 2 of theorem 4] to show that the representations have distinct characters.

The nonsingularity of W in (2.5) guarantees this for the subset of one dimensional representations. In the $p^t\times p^t$ representations, $\mathrm{tr}(A_0)=\omega p^t$ for distinct values ω while (2.4) and (2.5) specify $\mathrm{tr}(A_0)=1$ in all of the one dimensional representations. ∎

2.2 The linear independence property of the $p^t\times p^t$ representations

Sets, containing one element from each coset of Z_p in $G(p,t)$, are defined by

$$\Phi^{(t)}=\Big\{\prod A_0^{(p-\sigma)a_{-j}a_j/2}A_{-j}^{a_{-j}}A_j^{a_j}:0\le a_r<2,\ 1\le|r|\le t\Big\}. \tag{2.8}$$

Unless it is essential to specify a particular value, the superscript attached to Φ is suppressed. The element from Z_p contained in Φ is the identity element. (When $p=2$, there are three sets: Φ_0, Φ_1 and Φ_2 are subsets of $G_0(2,t)$, $G_1(2,t)$ and $G_2(2,t)$ respectively; again subscripts are only used where distinction is necessary.)

Let $\rho^{(t)}$ be a $p^t\times p^t$ representation and $\rho_\Phi^{(t)}$ be its restriction to the Φ subset.

Proposition 2.7 There is a bijection between $\mathbf{C}^{p^t\times p^t}$ and $\mathbf{C}\rho_\Phi^{(t)}$.

Proof As $\rho_\Phi^{(t)}$ contains p^{2t} $p^t\times p^t$ matrices, it is only necessary to show that these matrices are linearly independent over $\mathbf{C}$.

Let g_j for $0\le j<p^{2t}$ be the elements in Φ with g_0 denoting the identity element; η_{g_j} is a constant in $\mathbf{C}$ associated with g_j. Abbreviating $\rho_\Phi^{(t)}(g_j)$ to ρ_j and η_{g_j} to η_j, it must be shown that $\sum_{g_j\in\Phi}\eta_j\rho_j=0$ implies $\eta_j=0$ for all j. But $\sum_{g_j\in\Phi}\eta_j\rho_j\rho_k^{-1}=0$ is certainly implied and η_k replaces η_0 as the coefficient of ρ_0 in this sum. While $\rho_j\rho_k^{-1}$ does not necessarily represent an element in Φ, it represents an element in some coset of Z_p in $G(p,t)$ and, since $A_0=\omega 1_{p^t}$, it differs, if at all, from the representation of an element in Φ by a scalar factor that is a power of ω. Postmultiplying $\sum_{g_j\in\Phi}\eta_j\rho_j$ by ρ_k^{-1} then effectively permutes the coefficients η_j and multiplies them by a nonzero scalar. It follows that $\eta_j=0$ for all j if $\eta_j=0$ for any j.

For A_r where $r\ne 0$ define $\theta_r^{(v)}=\{g_m\in\Phi:A_rg_m=A_0^vg_mA_r\}$. Then, for any s in $[0,p)$, using (2.2(i)) and $A_0=\omega 1_{p^t}$,

$$\sum_{g_j\in\Phi}\eta_j\rho_j=0\ \Rightarrow\ \sum_{g_j\in\Phi}\eta_jA_r^s\rho_jA_r^{-s}=0\ \Rightarrow\ \sum_{v=0}^{p-1}\omega^{sv}\sum_{g_j\in\theta_r^{(v)}}\eta_j\rho_j=0.$$

By corollary 1.3, $\sum_{g_j\,\in\,\theta_r^{(v)}}\eta_j\rho_j=0$ for all v since the $p\times p$ matrix with ω^{sv} as its (s,v) element is nonsingular. The sum for $v=0$ is restricted to those elements in Φ that commute with A_r. It can similarly be further restricted to those elements that commute with all generators. But $\Phi\cap Z_p=\{g_0\}$ so $\eta_0=0$. ∎

2.3 The history of the groups $G(p,t)$

Propositions 2.1 to 2.7 are extensions of known results so it is appropriate and, at this point, convenient to relate them to their precursors.

Temporarily discarding the generators A_j, where $-t \le j \le 0$, and replacing (2.2) by

$$\begin{aligned} &\text{(i) } A_r A_s = -A_s A_r,\ r \ne s, \\ &\text{(ii) } A_r^2 \in \{1,-1\},\ 1 \le r < t, \end{aligned} \tag{2.9}$$

these are the relations defining the generators of the Clifford algebras with t generators; each generator can be independently chosen to have a square of 1 or -1. Certain properties of the real and complex Clifford algebras have been classified [22] in terms of t_+ and t_-, the numbers of generators with squares 1 and -1 respectively. The algebra elements are linear combinations, with scalars from $\mathbf{R}$ or $\mathbf{C}$, of the algebra basis elements $A_1^{a_1} A_2^{a_2} \dots A_t^{a_t}$ where $0 \le a_r < 2$ and $1 \le r \le t$. Denoting the basis elements more succinctly by B_j where $0 \le j < 2^t$ the operations of addition, scalar multiplication and algebra multiplication are respectively defined by

$$\begin{aligned} &\sum_j a_j B_j + \sum_j b_j B_j = \sum_j (a_j + b_j) B_j, \\ &\alpha \sum_j a_j B_j = \sum_j (\alpha a_j) B_j\ ,\ \alpha \in \mathbf{R} \text{ or } \alpha \in \mathbf{C}, \\ &\sum_k a_k B_k \sum_h b_h B_h = \sum_{k,h} a_k b_h B_k B_h = \sum_j c_j B_j. \end{aligned}$$

(For each pair B_k and B_h, (2.9) implies $B_k B_h = \sigma_{kh} B_{j'}$ for some j' and σ_{kh} is either 1 or -1; c_j is the sum of those products $\sigma_{kh} a_k b_h$ for which $B_k B_h = \sigma_{kh} B_j$.)

Clifford [6] introduced his algebras as generalizations of the $t_+ = 0, t_- = 2$ quaternion algebra. Notwithstanding the anticommuting property (2.9(i)) of the generators, he proved that algebras with an even number of generators—in his terminology, "algebras with an odd number of units"—can be constructed from commuting sets of quaternion bases; this result suggested replacing (2.9(i)) here by the more tractable (2.2(i)).

With Clifford's early death and no significant development of them, his algebras were apparently forgotten. An instance, other than the quaternions, appeared some fifty years later in Dirac's theory of the electron [11]. Dirac's use of the $t_+ = 3, t_- = 1$ generator representations (derived from those initially presented for $t_+ = 4, t_- = 0$) attracted the attention of Eddington [12, 13]. He considered representations of a generalization of the $t_+ = 0, t_- = 4$ algebra in which some of the basis elements are multiplied by powers of ζ so that the square of every basis element is -1. For each pair B_k and B_h in Eddington's algebra there exists B_j such that $B_k B_h = \sigma_{kh} B_j$ where σ_{kh} is now 1, -1, ζ or $-\zeta$.

Newman [18], stimulated by Eddington's results, rediscovered the infinite family of $t_+ = 0$ algebras. Littlewood [17], commenting on the papers by Eddington and Newman, considered the number and dimensions of the irreducible matrix representations of the groups underlying these algebras. The group associated with Eddington's algebra lies in a family $\mathcal{G}(2,t)$ which differs from $G(2,t)$ in having centres isomorphic to C_{2^2}. In his analysis for arbitrary t, Littlewood substituted groups of half the order with C_2 as centre. Proposition 2.3 is merely the extension to arbitrary primes of Littlewood's analyses of the $p = 2$ and $p = 3$ cases. The use of (2.2(i)) here, as opposed to (2.9(i)) used by Littlewood, does not alter the outcome; consideration of the representations shows that isomorphic groups are generated with different subsets of elements serving as generators. Clifford's result reflects this.

The groups $\mathcal{G}(2,t)$ are closely related to $G(2,t)$ and their properties can be established similarly. $\mathcal{G}(2,t)$ takes over A_0 and the other generators of $G(2,t)$ with the same

properties but A_0, in its role as a generator, is replaced by an element B such that $B^2 = A_0$. $\mathcal{G}(2,t)$ then has twice as many elements as $G(2,t)$; its centre $\{B^b : 0 \le b < 4\}$ is now C_{2^2} but the commutator subgroup remains C_2. Accordingly, it has twice as many one dimensional representations as $G(2,t)$ and two classes of $2^t \times 2^t$ irreducible representations distinguished by B having two distinct representations, $\zeta 1_{2^t}$ and $-\zeta 1_{2^t}$. The one dimensional representations, inherited from $\mathcal{G}(2,t)/Z_2$, consist of two sets of 2^{2t} representations in which B is represented by 1 and -1 respectively. The matrix of one dimensional representations is the 2-Hadamard matrix $W^{(1)} \otimes W^{(2t)}$.

There is a subset of $\mathcal{G}_0(2,t)$ containing one element from each coset of its centre,

$$\Phi_{0'}^{(t)} = \Big\{ \prod B^{a_{-j}a_j} A_{-j}^{a_{-j}} A_j^{a_j} : 0 \le a_r < 2,\ 1 \le |r| \le t \Big\}. \tag{2.10}$$

Henceforth, when $p = 2$, Φ denotes $\Phi_{0'}$, Φ_1 or Φ_2; there is no further interest in Φ_0. Proposition 2.7 holds for $\rho_{\Phi_{0'}}^{(t)}$ so it also provides a basis for $\mathbf{C}^{2^t \times 2^t}$.

Letting $B = \zeta 1_2$, the representation $\rho_{\Phi_{0'}}^{(1)}$ contains,

$$1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix},\ A_{-1} = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix},\ A_1 = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix},\ BA_{-1}A_1 = \begin{pmatrix} & -\zeta \\ \zeta & \end{pmatrix}. \tag{2.11}$$

The groups $\mathcal{G}_1(2,t)$ and $\mathcal{G}_2(2,t)$ are subgroups of $G_1(2,t+1)$ and $G_2(2,t+1)$ respectively since the generator B can be identified with the generator A_{t+1}.

By proposition 2.5, $A_j^{(t+1)}$ for $1 \le |j| \le t$ are block diagonal matrices consisting of two $2^t \times 2^t$ blocks. Such matrices are subsequently referred to as $2^t \times 2^t$ *bimatrices*. For these bimatrices, the two diagonal blocks are identical but A_{t+1} in $G_1(2,t+1)$ or $G_2(2,t+1)$ is represented by two diagonal blocks $\zeta 1_{2^t}$ and $-\zeta 1_{2^t}$ so it corresponds to B. The bimatrix representations $\mathcal{P}^{(t)}$ for each of $\mathcal{G}_1(2,t)$ and $\mathcal{G}_2(2,t)$ then are the direct sum of two $2^t \times 2^t$ irreducible representations. Moreover, these bimatrix representations inherit properties from the representations $\rho_{\Phi_1}^{(t+1)}$ and $\rho_{\Phi_2}^{(t+1)}$ of which they are subsets.

$G_0(2,t+1)$ does not contain an element corresponding to B so there is no subgroup of $G_0(2,t+1)$ providing a bimatrix representation of $\mathcal{G}_0(2,t)$.

Let $\Theta^{(t)} = \{g, Bg : g \in \Phi^{(t)}\}$. The restrictions $\mathcal{P}_{\Theta_1}^{(t)}$ and $\mathcal{P}_{\Theta_2}^{(t)}$ (collectively $\mathcal{P}_{\Theta}^{(t)}$) provide bases for $2^t \times 2^t$ bimatrices since they inherit the linear independence property of the representations $\rho_{\Phi}^{(t+1)}$.

A $U : V$ *bimatrix* has an upper matrix U and a lower matrix V.

Littlewood observed that families of groups with $p^t \times p^t$ irreducible representations exist for any prime p; he discussed the particular case $p = 3$ using a generalization of (2.9(i)) and a condition in place of (2.2(ii)) that is wrong—if p is odd and the group is of order p^{2t+1} then proposition 2.1 shows the group exponent to be p. He also noted the representational form of Clifford's result: each basis element in the $t_+ = 0, t_- = 2t$ algebras identified by Newman is represented by the tensor product of t matrices taken from a set of four 2×2 matrices that represent the quaternion algebra basis elements.

Eddington's algebra is defined by a 4×4 matrix representation and he used the fact that it provides a basis for 4×4 matrices. Proposition 2.7 is a generalization, in terms of matrix representations of $G(p,t)$, of the proof by Porteous [22] of the linear independence of the basis elements of the Clifford algebras.

Other uses for the rediscovered $p = 2$ algebras were found in theoretical physics; their attribution to Clifford appears in [3] as does the $p = 2$ case of proposition 3.1. Interest by topologists has resulted in the extensive account of them by Porteous who gives a construction similar to that in proposition 2.5. His treatment of the involutions of the Clifford algebras suggested section 2.4.1; the entry in his table 11.52 for the double fields with his immediately following comments on their endomorphisms directed attention to the bimatrix representations. In addition, his treatment of coset space representations,

with the following well known results [23, 2.19–2.21 and exercise 117], prompt some remarks about the set Φ which are exploited in section 4.

For each element g in a group G, there is an automorphism I_g of G, defined by

$I_g \ : \ G \to G \ ; \ h \mapsto g^{-1}hg$

where $I_g(h) = g^{-1}hg$ is the *conjugate* of h by g and I_g is the *inner automorphism* of G induced by g. The set of maps $\{I_g : g \in G\}$ form a group, the group of inner automorphisms of G, while the map $I \ : \ G \to \Sigma_G \ ; \ g \mapsto I_g$ into Σ_G (the symmetric group on the set of elements of G) has the centre of G as its kernel so the quotient group of G by its centre is the group of inner automorphisms of G.

As Φ contains one element from each coset of the centre in its parent group, Φ is a coset space representation by the parent of its abelian group of inner automorphisms.

For $p = 2$, Φ (or the set of basis elements for any of the aforementioned algebras with $2t$ generators) is simply one of the $4^{2^{2t}}$ possible coset space representations by $\mathcal{G}(2,t)$ of its own abelian group of inner automorphisms. The definition of the Clifford algebras, by restricting the factors σ_{kh} to values ± 1, severely curtails the possible choices of coset space representation—precluding $\Phi_{0'}$ for example. All of these coset space representations have $2^t \times 2^t$ matrix representations that, over $\mathbf{C}$, generate vector spaces and algebras isomorphic to $\mathbf{C}^{2^t \times 2^t}$. Regarding $\mathbf{C}$ as being of dimension two over $\mathbf{R}$, the vector spaces over $\mathbf{R}$, being of half the dimension of those over $\mathbf{C}$, span only subspaces of $\mathbf{C}^{2^t \times 2^t}$ and, due to occurrences of factors $\sigma_{kh} = \pm\zeta$, are not always algebras over $\mathbf{R}$.

2.4 Properties of the representation $\rho_\Phi^{(t)}$

The next proposition was suggested by Littlewood's comment on the tensor product structure of the representations of Newman's algebras. Both implicit and explicit use is made of the fact that if U_1 and U_2 are $u \times u$ matrices and V_1 and V_2 are $v \times v$ matrices then $(U_1 \otimes V_1)(U_2 \otimes V_2) = U_1U_2 \otimes V_1V_2$.

Proposition 2.8 Let $U_-^{(t)}$ and $U_+^{(t)}$ be matrices in $\rho_\Phi^{(t)}$ representing $\prod A_{-j}^{a_{-j}}$ and $\prod A_j^{a_j}$ respectively. Then $U_-^{(t)}U_+^{(t)} = U_-^{(t-1)}U_+^{(t-1)} \otimes (A_{-1}^{(1)})^{a_{-t}}(A_1^{(1)})^{a_t}$

Proof By proposition 2.5, for $1 \le |j| < t$, $A_j^{(t)} = A_j^{(t-1)} \otimes 1_p$ and $A_{\pm t}^{(t)} = 1_{p^{t-1}} \otimes A_{\pm 1}^{(1)}$. With the definitions of $U_-^{(t)}$ and $U_+^{(t)}$ these imply

$$\begin{aligned} U_-^{(t)}U_+^{(t)} &= (U_-^{(t-1)} \otimes 1_p)(1_{p^{t-1}} \otimes A_{-1}^{(1)})^{a_{-t}}(U_+^{(t-1)} \otimes 1_p)(1_{p^{t-1}} \otimes A_1^{(1)})^{a_t} \\ &= (U_-^{(t-1)} \otimes (A_{-1}^{(1)})^{a_{-t}})(U_+^{(t-1)} \otimes (A_1^{(1)})^{a_t}) \\ &= U_-^{(t-1)}U_+^{(t-1)} \otimes (A_{-1}^{(1)})^{a_{-t}}(A_1^{(1)})^{a_t}. \end{aligned}$$

Corollary 2.8 For any matrix $U^{(t)}$ in $\rho_\Phi^{(t)}$, there are unique matrices $U^{(t-1)}$ in $\rho_\Phi^{(t-1)}$ and $U^{(1)}$ in $\rho_\Phi^{(1)}$ such that $U^{(t)} = U^{(t-1)} \otimes U^{(1)}$.

Proof By (2.2(i)), for all t, $\prod A_{-j}^{a_{-j}} A_j^{a_j} = (\prod A_{-j}^{a_{-j}})(\prod A_j^{a_j}) = U_-^{(t)}U_+^{(t)}$.

Define $f_\Phi(r,s) = 1$ for Φ_1 or Φ_2 and $f_\Phi(r,s) = \prod_{j=r}^{s} \omega^{(p-1)a_{-j}a_j/2}$ otherwise. Putting $U^{(t)} = f_\Phi(1,t)U_-^{(t)}U_+^{(t)}$, $U^{(t-1)} = f_\Phi(1,t-1)U_-^{(t-1)}U_+^{(t-1)}$ and $U^{(1)} = f_\Phi(t,t)(A_{-1}^{(1)})^{a_{-t}}(A_1^{(1)})^{a_t}$, the claim follows from the proposition since $f_\Phi(1,t) = f_\Phi(1,t-1)f_\Phi(t,t)$ and the exponents a_j for $1 \le |j| \le t$ in $U^{(t)}$ uniquely determine those in $U^{(t-1)}$ and $U^{(1)}$. ∎

2.4.1 The involutions of $\rho_\Phi^{(t)}$

The definition of matrix multiplication implies that matrix algebras possess two transposition anti-involutions and an involution which results from their composition. For square matrices U and V,

$(UV)^\top = V^\top U^\top, \ \ (UV)^\vdash = V^\vdash U^\vdash, \ \ (UV)^{\top\vdash} = U^{\top\vdash}V^{\top\vdash}$

where $U^\top$, as usual, denotes transposition of U about the main diagonal, $U^\vdash$ denotes transposition of U about the secondary diagonal orthogonal to the main diagonal while $U^{\top\vdash}$ signifies the composition of these two commuting transpositions applied to U. The matrices $U^\top$, $U^\vdash$ and $U^{\top\vdash}$ are referred to respectively as the *transpose*, *orthotranspose* and *centrotranspose* of U. These, with negation, complex conjugation and inversion imply that matrix algebras are richly endowed with involutions. Matrices among the following types appear. Matrices U which satisfy,

(i) $U = U^\top$, $U = U^\vdash$ and $U = U^{\top\vdash}$ are respectively *symmetric*, *orthosymmetric* and *centrosymmetric*,

(ii) $U = \bar{U}^\top$, $U = \bar{U}^\vdash$ and $U = \bar{U}^{\top\vdash}$ are respectively *hermitian*, *orthohermitian* and *centrohermitian*,

(iii) $U = -\bar{U}^\top$ and $U = -U^\vdash$ are respectively *skew hermitian* and skew *orthosymmetric*,

(iv) $U^{-1} = U^\top$ and $U^{-1} = \bar{U}^\top$ are respectively *orthogonal* and *unitary*.

There is an alternative preferred notation $U^* = \bar{U}^\top$ for the *adjoint* of U.

Proposition 2.9 The matrices in $\rho^{(t)}$ are unitary and monomial with nonzero elements that are powers of ω if p is odd and ζ if $p = 2$.
Proof The matrices X and Y in proposition 2.4 are monomial with nonzero elements that are powers of ω; it is readily verified that $X^*X = Y^*Y = 1_2$ so X and Y are unitary. Since matrices $\omega 1_s$ and $\zeta 1_s$ are also unitary and both matrix and tensor products preserve these properties, (2.6) and proposition 2.5 imply that matrices in $\rho^{(t)}$ possess them. ∎

Proposition 2.10 Let g denote one of $\prod A_{-j}^{a_{-j}} A_j^{a_j}$ or $\prod B^{a_{-j}a_j} A_{-j}^{a_{-j}} A_j^{a_j}$.

(i) If g is in Φ_1 then $\rho^{(t)}_{\Phi_1}(g)$ is centrohermitian and either $\sum a_{-j}a_j + a_j$ is even when $g^{-1} = g$ and $\rho^{(t)}_{\Phi_1}(g)$ is also hermitian and orthosymmetric or $\sum a_{-j}a_j + a_j$ is odd when $g^{-1} = A_0 g$ and $\rho^{(t)}_{\Phi_1}(g)$ is also skew hermitian and skew orthosymmetric.

(ii) If g is in Φ_2, either $\sum a_{-j}a_j + a_{-j} + a_j$ is even when $g^{-1} = g$ and $\rho^{(t)}_{\Phi_2}(g)$ is hermitian or $\sum a_{-j}a_j + a_{-j} + a_j$ is odd when $g^{-1} = A_0 g$ and $\rho^{(t)}_{\Phi_2}(g)$ is skew hermitian.

(iii) If g is in $\Phi_{0'}$ then $g^{-1} = g$ and $\rho^{(t)}_{\Phi_{0'}}(g)$ is hermitian.

Proof (i) Inverting reverses the order of noncommuting generators so, using (2.2(i)),

$$g^{-1} = \prod A_j^{-a_j} A_{-j}^{-a_{-j}} = \prod A_0^{a_{-j}a_j} A_{-j}^{-a_{-j}} A_j^{-a_j}.$$

By (2.2(ii)), $A_{-j}^{-1} = A_{-j}$ and $A_j^{-1} = A_0 A_j$ for $1 \le j \le t$ so the inverses are as stated and $\rho^{(t)}_{\Phi_1}(g) = [\rho^{(t)}_{\Phi_1}(g)]^{-1}$ or $\rho^{(t)}_{\Phi_1}(g) = -[\rho^{(t)}_{\Phi_1}(g)]^{-1}$. As $\rho^{(t)}_{\Phi_1}$ is unitary, the hermitian or skew hermitian properties follow. However $\rho^{(t)}_{\Phi_1}$ is also centrohermitian. The matrices in (2.7(ii)) are centrohermitian, so this is true for $t = 1$; since the tensor product of centrohermitian matrices is centrohermitian, by corollary 2.8, it is true for all t.

But now a matrix which is both hermitian and centrohermitian is orthosymmetric while one which is skew hermitian and centrohermitian is skew orthosymmetric.

(ii) Since $\rho^{(t)}_{\Phi_2}$ is also unitary, the proof is as in (i) but with $A_j^{-1} = A_0 A_j$ for all $j \neq 0$.

(iii) In this case, using $(BA_0)^{-1} = B^{-3} = B$ and $A_j^{-1} = A_j$ for all j,

$$g^{-1} = \prod B^{-a_{-j}a_j} A_j^{-a_j} A_{-j}^{-a_{-j}} = \prod B^{-a_{-j}a_j} A_0^{-a_{-j}a_j} A_{-j}^{-a_{-j}} A_j^{-a_j} = g$$

so $\rho^{(t)}_{\Phi_{0'}}(g)$, being self-inverse and unitary, is hermitian.

Corollary 2.10 (i) Since $\rho^{(t)}_{\Phi_{0'}}(g)$ is hermitian, $\bar{\rho}^{(t)}_{\Phi_{0'}}(g) = (\rho^{(t)}_{\Phi_{0'}}(g))^\top$.
(ii) Since $\rho^{(t+1)}_{\Phi_1}$ is centrohermitian, $\mathcal{P}^{(t)}_{\Theta_1}$ is centrohermitian and, since $\rho^{(t)}_{\Phi_1}$ is unitary and centrohermitian, the group anti-involution, $g \to g^{-1}$ sends

(i) $\rho^{(t)}_{\Phi_1}(g) \mapsto (\rho^{(t)}_{\Phi_1}(g))^{\vdash}$ in the representation $\rho^{(t)}$ and

(ii) $(\rho^{(t)}_{\Phi_1}(g))^{\top\vdash} \mapsto (\rho^{(t)}_{\Phi_1}(g))^{\top}$ in the representation $\bar{\rho}^{(t)}$. ∎

Proposition 2.11 If p is odd, $\bar{\rho}^{(t)}_{\Phi}(g) = [\rho^{(t)}_{\Phi}(g)]^{\vdash}$

Proof To prove the orthohermitian property when $t = 1$, since the nonzero elements of matrices in $\rho^{(t)}_{\Phi}$ are powers of ω, it suffices to show that a nonzero element of the matrix $\omega^{\frac{1}{2}(p-1)a_{-1}a_1} A^{a_{-1}}_{-1} A^{a_1}_1$ is the complex conjugate of the element in the orthotransposed position or, equivalently, that their product is 1. By (2.6) and proposition 2.4,

$$(A^{a_{-1}}_{-1})_{j\,[j+a_{-1}]_p} = 1 \text{ and } (A^{a_1}_1)_{[j+a_{-1}]_p\,[j+a_{-1}]_p} = \omega^{(-\frac{1}{2}(p-1)+j+a_{-1})a_1}$$

so $(A^{a_{-1}}_{-1} A^{a_1}_1)_{j\,[j+a_{-1}]_p} = \omega^{(-\frac{1}{2}(p-1)+j+a_{-1})a_1}$. But then the orthotransposed element is $(A^{a_{-1}}_{-1} A^{a_1}_1)_{[p-1-j-a_{-1}]_p\,p-1-j} = \omega^{(\frac{1}{2}(p-1)-j)a_1}$ and

$$\omega^{\frac{1}{2}(p-1)a_{-1}a_1} . \omega^{(-\frac{1}{2}(p-1)+j+a_{-1})a_1} . \omega^{\frac{1}{2}(p-1)a_{-1}a_1} . \omega^{(\frac{1}{2}(p-1)-j)a_1} = \omega^{pa_{-1}a_1} = 1.$$

Since $\rho^{(1)}_{\Phi}$ is orthohermitian and tensor products preserve the orthohermitian property, by corollary 2.8, $\rho^{(t)}_{\Phi}$ is orthohermitian.

Corollary 2.11 When p is odd, the group anti-involution, $g \to g^{-1}$ sends

(i) $\rho^{(t)}_{\Phi}(g) \mapsto (\rho^{(t)}_{\Phi}(g))^{\top\vdash}$ in the representation $\rho^{(t)}$ and

(ii) $(\rho^{(t)}_{\Phi}(g))^{\vdash} \mapsto (\rho^{(t)}_{\Phi}(g))^{\top}$ in the representation $\bar{\rho}^{(t)}$.

Proof Since the representation is unitary and orthohermitian, $\rho^{(t)}(g^{-1}) = (\rho^{(t)}_{\Phi}(g))^{\top\vdash}$ proving (i) while (ii) merely restates the orthohermitian property. ∎

When p is odd, the inverse of every element in the set Φ is also in Φ. (For $p = 2$ and the set $\Phi_{0'}$, this is already evident from proposition 2.10(iii).) The proof consists of showing that inverses are preserved by the bijection

$$y : C^{2t}_p \to \Phi \; ; \; \prod \omega^{a_{-j}}_{-j} \omega^{a_j}_j \mapsto \prod A^{(p-1)a_{-j}a_j/2}_0 A^{a_{-j}}_{-j} A^{a_j}_j .$$

Proposition 2.12 For any h in C^{2t}_p, $[y(h)]^{-1} = y(h^{-1})$.

Proof The following are used.

(i) Since $A^p_0 = 1$, $A^{(p-1)a_{-j}a_j}_0 = A^{-a_{-j}a_j}_0$.

(ii) For $1 \le |j| \le t$, define $d_j = 0$ if $a_j = 0$ and $d_j = p - a_j$ if $a_j \neq 0$.

(iii) $A^{(p-1)a_{-j}a_j/2}_0 = A^{(p-1)d_{-j}d_j/2}_0$ is an immediate consequence of (ii) if either a_{-j} or a_j is zero; if both are nonzero

$$A^{(p-1)d_{-j}d_j/2}_0 = A^{(p-1)(p-a_{-j})(p-a_j)/2}_0 = A^{(p-1)a_{-j}a_j/2}_0 (A^p_0)^{(p-1)(p-a_{-j}-a_j)/2}$$

and $(A^p_0)^{(p-1)(p-a_{-j}-a_j)/2} = 1$ since either $A^p_0 = 1$ and $(p-1)/2$ is an integer if p is odd or $p - a_{-j} - a_j = 0$ if $p = 2$.

Now, if $h = \prod \omega^{a_{-j}}_{-j} \omega^{a_j}_j$ then $h^{-1} = \prod \omega^{d_{-j}}_{-j} \omega^{d_j}_j$ and, recalling that inverting reverses the order of noncommuting generators,

$$\begin{aligned}
[y(h)]^{-1} &= \prod A^{-(p-1)a_{-j}a_j/2}_0 A^{-a_j}_j A^{-a_{-j}}_{-j} \\
&= \prod A^{-(p-1)a_{-j}a_j/2}_0 A^{-a_j}_j A^{-a_{-j}}_{-j} && \text{, by (2.2(i))} \\
&= \prod A^{(p-1)a_{-j}a_j/2}_0 A^{-a_{-j}}_{-j} A^{-a_j}_j && \text{, by (i)} \\
&= \prod A^{(p-1)d_{-j}d_j/2}_0 A^{-a_{-j}}_{-j} A^{-a_j}_j && \text{, by (iii)} \\
&= \prod A^{(p-1)d_{-j}d_j/2}_0 A^{d_{-j}}_{-j} A^{d_j}_j && \text{, (ii) and (2.2(ii))} \\
&= y(h^{-1}). &&
\end{aligned}$$

∎

Proposition 2.13. For $h_a = \prod \omega_{-j}^{a_{-j}} \omega_j^{a_j}$ and $h_b = \prod \omega_{-j}^{b_{-j}} \omega_j^{b_j}$ in $G(p,t)/Z_p$, when p is odd, $y(h_a)y(h_b) = A_0^r y(h_a h_b)$ and $r = 0$ if and only if $y(h_a)$ and $y(h_b)$ commute.

Proof. By (2.2(i)), $\prod A_0^{-a_j b_{-j}} = \prod A_0^{-b_j a_{-j}}$ if $y(h_a)$ and $y(h_b)$ commute but, in any case, for some s in $[0,p)$, $\prod A_0^{-a_j b_{-j}} = A_0^s \prod A_0^{-b_j a_{-j}}$. As p is odd $A_0^s = A_0^{2r}$, where r is $s/2$ if s is even and $(p+s)/2$ if s is odd; also, since $A_0^p = 1$ and $p \neq 2$, it follows that

$$\begin{aligned}
\prod A_0^{(p-1)a_j b_{-j}} &= A_0^{2r} \prod A_0^{(p-1)b_j a_{-j}} = A_0^r \prod A_0^{(p-1)(a_j b_{-j} + b_j a_{-j})/2} \\
\text{so } y(h_a)y(h_b) &= A_0^r \prod A_0^{(p-1)(a_{-j}a_j + a_j b_{-j} + b_j a_{-j} + b_j b_{-j})/2} A_{-j}^{(a_{-j}+b_{-j})} A_j^{(a_j+b_j)} \\
&= A_0^r \prod A_0^{(p-1)(a_{-j}+b_{-j})(a_j+b_j)/2} A_{-j}^{(a_{-j}+b_{-j})} A_j^{(a_j+b_j)} \\
&= A_0^r \prod A_0^{(p-1)c_{-j}c_j} A_{-j}^{c_{-j}} A_j^{c_j}, \quad \text{where } c_k = [a_k + b_k]_p \text{ for } 1 \le |k| \le t \\
&= A_0^r y(h_a h_b).
\end{aligned}$$

Conversely, $r = 0$ ultimately implies $[a_j b_{-j}]_p = [b_j a_{-j}]_p$ so $y(h_a)$ and $y(h_b)$ commute. ∎

Proposition 2.13 shows that, when p is odd, the product of elements in Φ is also in Φ precisely when the elements commute. For $p = 2$, the proposition is false; clearly, the two elements $A_{-1}A_{-2}$ and A_1A_2 of $\Phi_{0'}^{(2)}$ commute but their product is $A_0 g$ where $g = B^2 \prod_{j=1}^2 A_{-j}A_j$ is in $\Phi_{0'}^{(2)}$. The proof above fails since averaging the two exponents involves division by two in a field of characteristic p which is not defined when $p = 2$.

3 The Fourier transforms

By proposition 2.7, there is a matrix in $\mathbf{C}^{p^t \times p^t}$ equivalent to each vector in $\mathbf{C}\rho_\Phi^{(t)}$. Given the components $\{a_g \in \mathbf{C}\}_{g\in\Phi}$ of such a vector then the equivalent matrix is

$$A = \sum_{g\in\Phi} a_g \rho_\Phi^{(t)}(g). \tag{3.1}$$

Proposition 3.1 If $g = 1$ then $\mathrm{tr}(\rho_\Phi^{(t)}(g)) = p^t$; otherwise $\mathrm{tr}(\rho_\Phi^{(t)}(g)) = 0$.

Proof For each A_r where $r \neq 0$, $\mathrm{tr}(A_r^{-1}\rho_\Phi^{(t)}(g)A_r) = \mathrm{tr}(A_r A_r^{-1}\rho_\Phi^{(t)}(g)) = \mathrm{tr}(\rho_\Phi^{(t)}(g))$. But if $g = \prod A_{-j}^{a_{-j}} A_j^{a_j}$ or $g = \prod A_0^{(p-1)a_{-j}a_j/2} A_{-j}^{a_{-j}} A_j^{a_j}$, by (2.2(i)) and $A_0 = \omega 1_{p^t}$, then also

$$\mathrm{tr}(A_r^{-1}\rho_\Phi^{(t)}(g)A_r) = \mathrm{tr}(A_0^{a_{-r}} A_r^{-1} A_r \rho_\Phi^{(t)}(g)) = \omega^{a_{-r}}\mathrm{tr}(\rho_\Phi^{(t)}(g)).$$

Now $\mathrm{tr}(\rho_\Phi^{(t)}(g)) = \omega^{a_{-r}}\mathrm{tr}(\rho_\Phi^{(t)}(g))$ for $1 \le |r| \le t$ implies $\mathrm{tr}(\rho_\Phi^{(t)}(g)) = 0$ unless $a_r = 0$ for all nonzero r. That is unless $g = 1$ when $\mathrm{tr}(1_{p^t}) = p^t$. ∎

Postmultiplying (3.1) by $[\rho_\Phi^{(t)}(k)]^{-1}$ and taking traces,

$$\mathrm{tr}(A[\rho_\Phi^{(t)}(k)]^{-1}) = \sum_{g\in\Phi} a_g \mathrm{tr}(\rho_\Phi^{(t)}(g)[\rho_\Phi^{(t)}(k)]^{-1}).$$

All terms in this last sum are zero unless $g = k$; this follows from proposition 3.1 since, as observed in the proof of proposition 2.7, $\rho_\Phi^{(t)}(g)[\rho_\Phi^{(t)}(k)]^{-1}$ differs, if at all, from the representation of an element in Φ by a scalar factor. So the inverse to (3.1) is

$$\{a_g = p^{-t}\mathrm{tr}(A[\rho_\Phi^{(t)}(g)]^{-1})\}_{g\in\Phi}. \tag{3.2}$$

Let $n = p^t$ hereafter. By proposition 2.9, the matrices in $\rho_\Phi^{(t)}$ are monomial with nonzero elements that are powers of ω or ζ. There are n^2 such matrices in which $\omega^0 = 1$ or $\zeta^0 = 1$ and $\zeta^2 = -1$ occur so using (3.1) or (3.2) directly requires $n^2(n-1)$ additions (or subtractions if $p = 2$) and less than n^3 multiplications by ζ or powers of ω. The inverse transform (3.2) also requires n^2 multiplications by n^{-1}.

In that (3.1) and (3.2) are the specialization to a Φ subset of more general formulae (see (3.5) and (3.6)), which apply to all irreducible representations of any finite group, they may be regarded as the standard formulae for computing these transforms. For $\rho_\Phi^{(t)}$, there are better methods.

3.1 The fast Fourier transform connecting $\mathbf{C}^{p^t\times p^t}$ and $\mathbf{C}\rho_\Phi^{(t)}$

When $r = s+1$, $a\langle r,s\rangle$ denotes an empty sequence; if $r \le s$, the sequence $a\langle r,s\rangle$ of $2(s-r+1)$ integers in $[0,p)$ is recursively defined by $a\langle r,s\rangle = a_{-r}\ a_r\ a\langle r+1,s\rangle$. With f_Φ as defined in corollary 2.8, let $\alpha_j^{(k,r)} = f_\Phi(r,r)(A_{-j}^{(k)})^{a_{-r}}(A_j^{(k)})^{a_r}$.

Sets containing $p^{2(t-k)}$ $p^k\times p^k$ matrices are defined by

$$\left\{ Z^{(k)}_{a\langle k+1,t\rangle} = \sum_{\substack{a_j=0\\ 1\le|j|\le k}}^{p-1} Z^{(0)}_{a\langle 1,t\rangle} \prod_{j=1}^{k} \alpha_j^{(k,j)} \ :\ 0\le a_s<p\ ,\ k<|s|\le t \right\}\ ,\ 1\le k\le t. \quad (3.3)$$

When $k=t$, (3.3) specifies a set containing only the $p^t\times p^t$ matrix $Z^{(t)}_{a\langle t+1,t\rangle} = Z^{(t)}$ and $\{Z^{(0)}_{a\langle 1,t\rangle}\in\mathbf{C}\ :\ 0\le a_r<p\ ,\ 1\le|r|\le t\}$ is the set of components of the equivalent vector in $\mathbf{C}\rho_\Phi^{(t)}$. When $k<t$, selecting particular values for a_s where $k<|s|\le t$ identifies a subset of the components, namely, those that have these particular values in the latter subscript positions in the sequences $a\langle 1,t\rangle$. Then (3.3) specifies $Z^{(k)}_{a\langle k+1,t\rangle}$ to be the $p^k\times p^k$ matrix equivalent to the vector in $\mathbf{C}\rho_\Phi^{(k)}$ that has this subset as components.

Computing the sets (3.3) for $k=1$, $k=2,\ldots,$ $k=t$, is an alternative method of computing the transform. The inverse transform requires the sets to be computed in the reverse sequence. Each set can be efficiently computed from its predecessor.

Proposition 3.2 $Z^{(k)}_{a\langle k+1,t\rangle} = \sum_{a_{-k},a_k=0}^{p-1} Z^{(k-1)}_{a\langle k,t\rangle}\otimes\alpha_1^{(1,k)}$.

Proof By (3.3) and then corollary 2.8,

$$Z^{(k)}_{a\langle k+1,t\rangle} \ =\ \sum_{a_{-k},a_k=0}^{p-1}\Bigg(\sum_{\substack{a_j=0\\ 1\le|j|<k}}^{p-1} Z^{(0)}_{a\langle 1,t\rangle}\prod_{j=1}^{k-1}\alpha_j^{(k-1,j)}\Bigg)\otimes\alpha_1^{(1,k)} \ =\ \sum_{a_{-k},a_k=0}^{p-1} Z^{(k-1)}_{a\langle k,t\rangle}\otimes\alpha_1^{(1,k)}.\ \blacksquare$$

Using proposition 3.2 entails partitioning $Z^{(k)}_{a\langle k+1,t\rangle}$ into p^2 $p^{k-1}\times p^{k-1}$ submatrices (denoted by M_{rs} below); also $Z^{(k-1)}_{a\langle k,t\rangle} = Z^{(k-1)}_{a_{-k}a_k a\langle k+1,t\rangle}$ and the latter is abbreviated to $Z_{a_{-k}a_k}$. The matrices $\alpha_1^{(1,k)}$ are the members of $\rho_\Phi^{(1)}$; for $\rho^{(1)}_{\Phi_{0'}}$ these are shown in (2.11). Using them with proposition 3.2 and expressing $Z^{(k)}_{a\langle k+1,t\rangle}$ as

$$\begin{pmatrix} M_{00} & M_{01}\\ M_{10} & M_{11}\end{pmatrix} = \begin{pmatrix} Z_{00} & \\ & Z_{00}\end{pmatrix} + \begin{pmatrix} & Z_{10}\\ Z_{10} & \end{pmatrix} + \begin{pmatrix} Z_{01} & \\ & -Z_{01}\end{pmatrix} + \begin{pmatrix} & -\zeta Z_{11}\\ \zeta Z_{11} & \end{pmatrix},$$

$$\begin{aligned} &\text{(i)} && M_{00}=Z_{00}+Z_{01},\quad M_{01}=Z_{10}-\zeta Z_{11},\\ &&& M_{11}=Z_{00}-Z_{01},\quad M_{10}=Z_{10}+\zeta Z_{11},\\ &\text{(ii)} && 2Z_{00}=M_{00}+M_{11},\quad 2Z_{10}=M_{01}+M_{10},\\ &&& 2Z_{01}=M_{00}-M_{11},\quad 2Z_{11}=\zeta(M_{01}-M_{10}).\end{aligned} \quad (3.4)$$

In a typical stage of computing the transform, $2^{2(t-k)}$ $2^k\times 2^k$ matrices $Z^{(k)}_{a\langle k+1,t\rangle}$ are computed from $2^{2(t-k+1)}$ $2^{k-1}\times 2^{k-1}$ matrices $Z^{(k-1)}_{a\langle k,t\rangle}$. By (3.4(i)), one addition or subtraction is used in computing each matrix element and, for every four such operations, there is one multiplication by ζ. So 2^{2t} additions or subtractions and 2^{2t-2} multiplications by ζ are needed in each of the t stages. That is, $n^2\log_2 n$ additions or subtractions and $(n^2\log_2 n)/4$ multiplications by ζ suffice to compute the transform.

For the inverse transform, as the form of the equations in (3.4(ii)) suggest, it is more economical to compute the matrices $2^{t-k}Z^{(k)}_{a\langle k+1,t\rangle}$, rather than $Z^{(k)}_{a\langle k+1,t\rangle}$, as this too can be achieved with $n^2\log_2 n$ additions or subtractions and $(n^2\log_2 n)/4$ multiplications by ζ. Then a further n^2 multiplications by n^{-1} recover the components $Z^{(0)}_{a\langle 1,t\rangle}$.

The transforms for $\rho^{(1)}_{\Phi_1}$ and $\rho^{(1)}_{\Phi_2}$ are similar but require twice as many multiplications by ζ or $-\zeta$.

For $p=3$, the identities corresponding to those in (3.4) are

$$
\begin{array}{lll}
M_{00}=Z_{00}+\omega^2 Z_{01}+\omega Z_{02}, & M_{01}=Z_{10}+\omega Z_{11}+\omega^2 Z_{12}, & M_{02}=Z_{20}+Z_{21}+Z_{22},\\
M_{11}=Z_{00}+Z_{01}+Z_{02}, & M_{12}=Z_{10}+\omega^2 Z_{11}+\omega Z_{12}, & M_{10}=Z_{20}+\omega Z_{21}+\omega^2 Z_{22},\\
M_{22}=Z_{00}+\omega Z_{01}+\omega^2 Z_{02}, & M_{20}=Z_{10}+Z_{11}+Z_{12}, & M_{21}=Z_{20}+\omega^2 Z_{21}+\omega Z_{22},
\end{array}
$$

$$
\begin{array}{lll}
3Z_{00}=M_{00}+M_{11}+M_{22}, & 3Z_{10}=M_{01}+M_{12}+M_{20}, & 3Z_{20}=M_{02}+M_{10}+M_{21},\\
3Z_{01}=\omega M_{00}+M_{11}+\omega^2 M_{22}, & 3Z_{11}=\omega^2 M_{01}+\omega M_{12}+M_{20}, & 3Z_{21}=M_{02}+\omega^2 M_{10}+\omega M_{21},\\
3Z_{02}=\omega^2 M_{00}+M_{11}+\omega M_{22}, & 3Z_{12}=\omega M_{01}+\omega^2 M_{12}+M_{20}, & 3Z_{22}=M_{02}+\omega M_{10}+\omega^2 M_{21}.
\end{array}
$$

In general there are p^2 identities for computing each transform and the right hand side of each identity contains p terms. For odd p, ω does not appear in p of the identities while, in the remaining p^2-p of each set, the $p-1$ distinct nonzero powers of ω each appear once. These properties stem from the definitions of X and Y in proposition 2.4.

For the odd primes, it follows that $(p-1)n^2\log_p n$ additions, $(p-2+p^{-1})n^2\log_p n$ multiplications by powers of ω and, in the inverse transform, n^2 multiplications by n^{-1} are used in computing the transforms.

As the number and complexity of the identities increase rapidly with p, the transforms become computationally correspondingly less attractive.

3.2 The group algebra Fourier transform

The group algebra $\mathbf{A}G$ for a finite group G over an associative algebra $\mathbf{A}$ defined over $\mathbf{C}$ consists of formal sums $\sum_{g\in G} a_g g$ with a_g in $\mathbf{A}$. The operations of addition, scalar multiplication and algebra multiplication on these sums are respectively defined by

$$
\begin{array}{l}
\displaystyle\sum_{g\in G} a_g g+\sum_{g\in G} b_g g=\sum_{g\in G}(a_g+b_g)g,\\
\displaystyle\alpha\sum_{g\in G} a_g g=\sum_{g\in G}(\alpha a_g)g\ ,\ \alpha\in\mathbf{C},\\
\displaystyle\sum_{g\in G} a_g g\sum_{k\in G} b_k k=\sum_{g,k\in G} a_g b_k gk=\sum_{g,h\in G} a_g b_{g^{-1}h}h=\sum_{h\in G} c_h h \text{ where } c_h=\sum_{g\in G} a_g b_{g^{-1}h}.
\end{array}
$$

(It is the requirement in this last definition that g and b_k commute that dictates the use of (2.2(i)) rather than (2.9(i)). $\mathbf{A}$ can then be identified with $\mathbf{C}^{p^{t-s}\times p^{t-s}}$ and G with $G(p,s)$, for varying s. Formally, using (2.2(i)) allows an algebra multiplication to be defined on modules $\mathbf{C}^{p^{t-s}\times p^{t-s}}\Phi^{(s)}$ for $0<s<t$ as well as the vector space $\mathbf{C}\Phi^{(t)}$.)

Multiplication of elements in a group algebra requires the computation of the convolution $\{c_h\}_{h\in G}$ of the set $\{a_g\}_{g\in G}$ with the set $\{b_g\}_{g\in G}$. There is a Fourier transform algorithm for this.

Proposition 3.3 (Atkinson [2].) If R is a complete set of irreducible matrix representations of a finite group G of order $|G|$ and $\rho(g)$ is a $d_\rho\times d_\rho$ representation of g in G by ρ in R then the Fourier transform of $\{a_g\}_{g\in G}$ is the set of matrices

$$
\left\{A_\rho=\sum_{g\in G} a_g\rho(g)\right\}_{\rho\in R}. \tag{3.5}
$$

The set $\{a_g\}_{g\in G}$ can be recovered from $\{A_\rho\}_{\rho\in R}$ by the inverse transform

$$
\left\{a_g=|G|^{-1}\sum_{\rho\in R} d_\rho\mathrm{tr}(A_\rho\rho(g^{-1}))\right\}_{g\in G} \tag{3.6}
$$

and the convolution $\{c_g\}_{g\in G}$ of $\{a_g\}_{g\in G}$ with $\{b_g\}_{g\in G}$ is obtained by computing,

(i) the transforms $\{A_\rho\}_{\rho\in R}$ of $\{a_g\}_{g\in G}$ and $\{B_\rho\}_{\rho\in R}$ of $\{b_g\}_{g\in G}$,

(ii) the set of matrix products $\{A_\rho B_\rho\}_{\rho\in R}$,

(iii) the inverse transform $\{c_g\}_{g\in G}$ of $\{A_\rho B_\rho\}_{\rho\in R}$. ∎

If the standard $O(d_\rho^3)$ method of matrix multiplication is used in step (ii) of this algorithm then this step alone, in general, will require $O(|G|^{3/2})$ arithmetic operations in $\mathbf{A}$; $G(p,t)$ is such a group. However, if G is abelian then the $|G|$ irreducible representations are one dimensional and step (ii) requires only $|G|$ multiplications in $\mathbf{A}$. Moreover, in the abelian case, G is necessarily either a cyclic group of prime power order or the direct product of such groups. It follows [2, 5, 7] that steps (i) and (iii) need only $O(|G|\sum_{j=1}^r p_j t_j)$ operations where $|G| = \prod_{j=1}^r p_j^{t_j}$ and p_j for $1 \le j \le r$ are primes. If $r = 1$ then $O(|G|\log|G|)$ operations in $\mathbf{A}$ are sufficient to compute the convolution.

Proposition 3.4 Computing a convolution in $\mathbf{A}C_p^{2t}$ requires $O(n^2 \log n)$ arithmetic operations in $\mathbf{A}$. ∎

The transforms for computing a convolution in $\mathbf{A}C_p^{2t}$ are described using the sequence notation of section 3.1.

Let $\{X^{(0)}_{r\langle 1,t\rangle} \in \mathbf{A} \ : \ 0 \le r_u < p \ , \ 1 \le |u| \le t\}$ be the coefficients of the elements $\prod \omega_{-j}^{r_{-j}} \omega_j^{r_j}$ of C_p^{2t}. The irreducible representations of this group are provided by the matrix W in (2.5). The transform is obtained in t stages by computing the t sets,

$$\Big\{ X^{(t-i+1)}_{r\langle 1,i-1\rangle\, s\langle i,t\rangle} = \sum_{r_{-i},r_i=0}^{p-1} \omega^{r_{-i}s_{-i}+r_i s_i} X^{(t-i)}_{r\langle 1,i\rangle\, s\langle i+1,t\rangle} \ : \\ 0 \le r_u < p,\ 1 \le |u| < i \text{ and } 0 \le s_v < p,\ i \le |v| \le t \Big\},$$

for $i = t,\ i = t-1, \ldots,\ i = 1$ in turn.

It is more economical to split the computation of each set into two substages. In computing $\{X^{(t-i+1)}_{r\langle 1,i-1\rangle\, s\langle i,t\rangle}\}$ it is advantageous to perform all of the sums over one of r_{-i} or r_i, recording the intermediate results, before performing any of the sums over the other. In this way, the cost per element $X^{(t-i+1)}_{r\langle 1,i-1\rangle\, s\langle i,t\rangle}$ is $O(p)$ rather than $O(p^2)$ operations. In each of the $2t$ substages, n^2 elements are computed each requiring $p-1$ additions (or subtractions if $p = 2$). When p is odd, for each element there are also, on average, $(p-1)^2/p$ multiplications by powers of ω.

In all, $2(p-1)n^2\log_p n$ additive operations and, if p is odd, $2(p-2+p^{-1})n^2\log_p n$ multiplications by powers of ω are needed to compute the transforms.

The inverse transform involves the similar computation of the sets,

$$\Big\{ p^{2i} X^{(t-i)}_{r\langle 1,i\rangle\, s\langle i+1,t\rangle} = \sum_{s_{-i},s_i=0}^{p-1} \omega^{-(r_{-i}s_{-i}+r_i s_i)} X^{(t-i+1)}_{r\langle 1,i-1\rangle\, s\langle i,t\rangle} \ : \\ 0 \le r_u < p,\ 1 \le |u| \le i \text{ and } 0 \le s_v < p,\ i < |v| \le t \Big\},$$

for $i = 1,\ i = 2, \ldots,\ i = t$ in turn.

Here there are an additional n^2 multiplications by n^{-2} to recover the component values from those in the final set.

The transforms for C_p^{2t} can be computed recursively from those for C_p^2; when $p = 2$, for example, these are

$$\begin{aligned}
X^{(1)}_{00} &= (X^{(0)}_{00} + X^{(0)}_{10}) + (X^{(0)}_{01} + X^{(0)}_{11}), & X^{(0)}_{00} &= 2^{-2}[(X^{(1)}_{00} + X^{(1)}_{10}) + (X^{(1)}_{01} + X^{(1)}_{11})],\\
X^{(1)}_{10} &= (X^{(0)}_{00} - X^{(0)}_{10}) + (X^{(0)}_{01} - X^{(0)}_{11}), & X^{(0)}_{10} &= 2^{-2}[(X^{(1)}_{00} - X^{(1)}_{10}) + (X^{(1)}_{01} - X^{(1)}_{11})],\\
X^{(1)}_{01} &= (X^{(0)}_{00} + X^{(0)}_{10}) - (X^{(0)}_{01} + X^{(0)}_{11}), & X^{(0)}_{01} &= 2^{-2}[(X^{(1)}_{00} + X^{(1)}_{10}) - (X^{(1)}_{01} + X^{(1)}_{11})],\\
X^{(1)}_{11} &= (X^{(0)}_{00} - X^{(0)}_{10}) - (X^{(0)}_{01} - X^{(0)}_{11}), & X^{(0)}_{11} &= 2^{-2}[(X^{(1)}_{00} - X^{(1)}_{10}) - (X^{(1)}_{01} - X^{(1)}_{11})].
\end{aligned}$$

Again, the transforms rapidly become computationally unattractive as p increases.

The transforms and inverses for these cyclic groups are respectively referred to as $\mathcal{T}_2$ and $\mathcal{T}_2^{-1}$ transforms. Similarly the transforms for computing (3.1) and (3.2), based

on proposition 3.2, are referred to as $\mathcal{T}_1$ and $\mathcal{T}_1^{-1}$ transforms. Some comment now on the use of these transforms simplifies presentation later.

The $\mathcal{T}_1$ and $\mathcal{T}_1^{-1}$ transforms are defined for a designated set—either one of the sets $\rho_\Phi^{(1)}$ or, in the matrix inverse algorithms, $\{[\rho_\Phi^{(1)}(g)]^{-1}\}_{g\in\Phi^{(1)}}$.

The transforms are used recursively. In the notation preceding (3.4), one stage of a $\mathcal{T}_1^{-1}$ transform reduces a matrix $Z^{(k)}_{a\langle k+1,t\rangle}$ (for some value k) to p^2 $p^{k-1}\times p^{k-1}$ matrices $Z_{a_{-1}a_1}$ for a_{-1} and a_1 in $[0,p)$. These are respectively identified with the inputs $X^{(0)}_{r_{-1}r_1}$ of a $\mathcal{T}_2$ transform for C_p^2 which is applied to produce the corresponding outputs $X^{(1)}_{s_{-1}s_1}$.

Accordingly, a $\mathcal{T}_3$ *transform for a designated set* is defined to be the composition of one stage of a $\mathcal{T}_1^{-1}$ transform for the designated set followed by a $\mathcal{T}_2$ transform for C_p^2. Similarly, a $\mathcal{T}_3^{-1}$ *transform for a designated set* is the inverse—a $\mathcal{T}_2^{-1}$ transform for C_p^2 followed by one stage of a $\mathcal{T}_1$ transform for the designated set.

For $\mathcal{P}_\Theta$, *half* $\mathcal{T}_3$ and $\mathcal{T}_3^{-1}$ transforms are required. From

$$\begin{pmatrix} M_{00} & \\ & M_{11} \end{pmatrix} = \begin{pmatrix} Z_0 & \\ & Z_0 \end{pmatrix} + \begin{pmatrix} \zeta Z_1 & \\ & -\zeta Z_1 \end{pmatrix},$$

it follows that the half $\mathcal{T}_3$ transforms use,

$$X_0^{(0)} = Z_0 = (M_{11}+M_{00})/2, \quad X_1^{(0)} = Z_1 = \zeta(M_{11}-M_{00})/2,$$
$$X_0^{(1)} = X_0^{(0)} + X_1^{(0)}, \quad X_1^{(1)} = X_0^{(0)} - X_1^{(0)}$$

and the corresponding half $\mathcal{T}_3^{-1}$ transforms use,

$$Z_0 = X_0^{(0)} = (X_0^{(1)} + X_1^{(1)})/2, \quad Z_1 = X_1^{(0)} = (X_0^{(1)} - X_1^{(1)})/2$$
$$M_{00} = Z_0 + \zeta Z_1, \quad M_{11} = Z_0 - \zeta Z_1.$$

The half $\mathcal{T}_3$ and $\mathcal{T}_3^{-1}$ transforms for $\{[\rho_\Phi^{(1)}(g)]^{-1}\}_{g\in\Phi^{(1)}}$ are obtained by negating ζ.

Proposition 3.5 Given a complex $2^t\times 2^t$ matrix M, there is a is a direct sum decomposition $M = M_1 + \zeta M_2$ into the unique hermitian matrices M_1 and M_2.
Proof As is well known, $M_1 = (M+M^*)/2$ and $M_2 = (M-M^*)/2\zeta$.

Remark 3.5 One stage of a $\mathcal{T}_1^{-1}$ transform for $\rho^{(1)}_{\Phi_{0'}}$ applied to a hermitian matrix produces hermitian transforms since the relations (3.4(ii)) imply that if $Z^{(k)}_{a<k+1,t>}$ is hermitian then M_{00} and M_{11} are hermitian while $M_{10} = M_{01}^*$ so Z_{00}, Z_{01}, Z_{10} and Z_{11} are also hermitian. If $Z^{(t)}$ is hermitian then the sets (3.1) will all contain only hermitian matrices so $Z^{(t)}$ represents an element in $\mathbf{R}\Phi^{(t)}_{0'}$. Since the $\mathcal{T}_2$ part of a $\mathcal{T}_3$ transform forms only sums and differences, a $\mathcal{T}_3$ transform produces hermitian transforms. ∎

For $z = \Re(z) + \zeta\Im(z)$ in $\mathbf{C}$, $\Re(z)$ and $\Im(z)$ in $\mathbf{R}$ are the real and imaginary parts.

Proposition 3.6 Given a complex $2^t\times 2^t$ matrix M, there is a centrohermian bimatrix

$$\begin{pmatrix} M & \\ & M^{*\vdash} \end{pmatrix} = \begin{pmatrix} M_1+\zeta M_2 & \\ & M_1-\zeta M_2 \end{pmatrix}$$

representing an element in $\mathbf{R}\Theta_1^{(t)}$, where M_1 and M_2 are centrohermitian matrices representing elements in $\mathbf{R}\Phi_1^{(t)}$.
Proof A $\mathcal{T}_1^{-1}$ transform for $\rho^{(1)}_{\Phi_1}$ applied to M determines complex components a_g such that $M = \sum_{g\in\Phi_1} a_g \rho^{(t)}_{\Phi_1}(g)$ so $M_1 = \sum_{g\in\Phi_1} \Re(a_g)\rho^{(t)}_{\Phi_1}(g)$ and $M_2 = \sum_{g\in\Phi_1} \Im(a_g)\rho^{(t)}_{\Phi_1}(g)$ represent elements in $\mathbf{R}\Phi_1^{(t)}$ and, by proposition 2.10(i), are centrohermitian.

But $M = M_1 + \zeta M_2$ is a direct sum decomposition of M into the unique centrohermitian matrices $M_1 = (M+M^{*\vdash})/2$ and $M_2 = (M-M^{*\vdash})/2\zeta$.

It follows from the form of the representation of B and the definition of $\Theta_1^{(t)}$ that the bimatrix $M : M^{*\vdash}$ represents an element in $\mathbf{R}\Theta_1^{(t)}$.

Remark 3.6 Here, a half $\mathcal{T}_3$ transform applied to the $M : M^{*\vdash}$ bimatrix produces centrohermitian transforms $\mathcal{M}_1$ and $\mathcal{M}_2$ also representing elements in $\mathbf{R}\Phi_1^{(t)}$.

Also, in this case, if $Z^{(t)}$ is centrohermitian, the sets (3.1) will all contain only centrohermitian matrices. ∎

Proposition 3.7 Given a complex $2^t \times 2^t$ matrix M, there is a bimatrix

$$\begin{pmatrix} M & \\ & M_B \end{pmatrix} = \begin{pmatrix} M_1 + \zeta M_2 & \\ & M_1 - \zeta M_2 \end{pmatrix}$$

representing an element in $\mathbf{R}\Theta_2^{(t)}$, where M_1 and M_2 represent elements in $\mathbf{R}\Phi_2^{(t)}$.

Proof A $\mathcal{T}_1^{-1}$ transform for $\rho_{\Phi_2}^{(1)}$ applied to M determines complex components a_g such that $M = \sum_{g\in\Phi_2} a_g \rho_{\Phi_2}^{(t)}(g)$ so $M_1 = \sum_{g\in\Phi_2} \Re(a_g)\rho_{\Phi_2}^{(t)}(g)$ and $M_2 = \sum_{g\in\Phi_2} \Im(a_g)\rho_{\Phi_2}^{(t)}(g)$ represent elements in $\mathbf{R}\Phi_2^{(t)}$. Letting $M_B = M_1 - \zeta M_2$, by the form of the representation of B and the definition of $\Theta_2^{(t)}$, the bimatrix $M : M_B$ represents an element in $\mathbf{R}\Theta_2^{(t)}$.

Remark 3.7 The $\mathcal{T}_1^{-1}$ part of a half $\mathcal{T}_3$ transform applied to the $M : M_B$ bimatrix produces the matrices M_1 and M_2. Since the $\mathcal{T}_2$ part of a half $\mathcal{T}_3$ transform forms the sum and difference of M_1 and M_2, the matrix transforms $\mathcal{M}_1$ and $\mathcal{M}_2$ also represent elements in $\mathbf{R}\Phi_2^{(t)}$.

Here there is no convenient symmetry property permitting a simpler method of decomposing M into the matrices M_1 and M_2. ∎

4 Algorithms for matrix operations

The algorithms developed here stem from three features of $G(p,t)$ and $\mathcal{G}(2,t)$.

(i) The quotient group of these groups by their centres is the abelian group C_p^{2t}. The quotient group of $\mathcal{G}_1(2,t)$ and $\mathcal{G}_2(2,t)$ by their commutator subgroups is the abelian group C_2^{2t+1}.

(ii) The coset space representations $\Phi^{(t)}$ of C_p^{2t} provided by the groups have matrix representations that form a basis for $p^t \times p^t$ matrices. The coset space representations $\Theta_1^{(t)}$ and $\Theta_2^{(t)}$ of C_2^{2t+1} provided by $\mathcal{G}_1(2,t)$ and $\mathcal{G}_2(2,t)$ have bimatrix representations that form a basis for $2^t \times 2^t$ bimatrices.

(iii) With the generator A_0 represented by $\omega 1_{2^t}$, the matrix representation of the group algebra element $a_g g$, where g is in Φ or Θ, is identical to the representation of the group algebra element $a_g \omega^{-r} A_0^r g$, for $0 < r < p$. For g in $\Phi_{0'}$ and $0 \le r < 4$, $a_g \zeta^{-r} B^r g$ all have the same representation.

For matrix products, efficient algorithms exist if the operands and product can simultaneously each be represented by specific (possibly different) coset space representations; then the product is a function of the cosets rather than of the elements in a coset. As the group with the cosets as its elements is abelian, evidently such products can be computed by a convolution for this abelian group.

A candidate is the product of a $2^t \times 2^t$ unitary matrix and its inverse since the coset space representation of the matrix uniquely determines a coset space representation of the inverse. As all components in the product vanish except that for the identity element which is always in Φ, this product clearly meets the requirement and implies a convolution algorithm for inverting these matrices. Though less efficient than simply forming the adjoint, a special case of this algorithm appears implicitly in solving the matrix eigenvalue problem which also involves a product that is a function of the cosets. It also serves as an introduction to all of the subsequent algorithms.

4.1 A characterization of $2^t \times 2^t$ unitary matrices

The algebra $\mathbf{R}\Phi_2^{(1)}$ is the quaternion algebra. There is also interest in $\mathbf{C}\Phi_2^{(1)}$.

Adopting the currently more convenient alternative notation $i = A_{-1}$, $j = A_1$, an element $m = a.1+b.i+c.j+d.ij$ in $\mathbf{C}\Phi_2^{(1)}$ is the direct sum of $Z(m) = a.1$, the component of m in $\mathbf{C}$ which is the centre of $\mathbf{C}\Phi_2^{(1)}$ and $NZ(m) = b.i + c.j + d.ij$, the non-central part. (For quaternions, the real and pure parts respectively.)

The multiplication table 4.1 for the basis elements of the $\mathbf{C}\Phi_2^{(1)}$ algebra (obtained from (2.2) on identifying A_0 with -1) is that of the quaternion algebra.

	1	i	j	ij
1	1	i	j	ij
i	i	-1	ij	$-j$
j	j	$-ij$	-1	i
ij	ij	j	$-i$	-1

Table 4.1

Negating entries in rows (or columns) other than the first, diagonal entries become 1 and the (non-central) off-diagonal entries become skew symmetric about the diagonal. Consequently, defining $\widetilde{m} = Z(m) - NZ(m) = a.1 + b.i^{-1} + c.j^{-1} + d.(ij)^{-1}$, it follows that $NZ(m\widetilde{m}) = NZ(\widetilde{m}m) = 0$, so

$$m\widetilde{m} = \widetilde{m}m = (a^2 + b^2 + c^2 + d^2)1. \tag{4.1}$$

Let $|M|$ denote the determinant of a matrix M.

Proposition 4.1 For $m = a.1+b.i+c.j+d.ij$ in $\mathbf{C}\Phi_2^{(1)}$, matrices M and $\widetilde{M}$, representing m and $\widetilde{m}$, satisfy $M\widetilde{M} = \widetilde{M}M = |M|1_2$ so if $|M| \neq 0$ then $M^{-1} = |M|^{-1}\widetilde{M}$.

Proof Using the representation of $\Phi_2^{(1)}$ shown in (2.7(iii)),

$$M = \begin{pmatrix} a & \\ & a \end{pmatrix} + \begin{pmatrix} & \zeta b \\ \zeta b & \end{pmatrix} + \begin{pmatrix} \zeta c & \\ & -\zeta c \end{pmatrix} + \begin{pmatrix} & d \\ -d & \end{pmatrix} = \begin{pmatrix} a+\zeta c & \zeta b + d \\ \zeta b - d & a - \zeta c \end{pmatrix},$$

$$\widetilde{M} = \begin{pmatrix} a & \\ & a \end{pmatrix} - \begin{pmatrix} & \zeta b \\ \zeta b & \end{pmatrix} - \begin{pmatrix} \zeta c & \\ & -\zeta c \end{pmatrix} - \begin{pmatrix} & d \\ -d & \end{pmatrix}$$

and $|M| = a^2 + b^2 + c^2 + d^2$ so the claims follows from (4.1). ∎

If m is a quaternion, a, b, c and d are real and (4.1) shows that nonzero quaternions have inverses so $\mathbf{R}\Phi_2^{(1)}$ is the quaternion field $\mathbf{H}$.

For any $n\times n$ matrix M, both $M\widetilde{M} = \widetilde{M}M = |M|1_n$ and $M^{-1} = |M|^{-1}\widetilde{M}$ are known from the theory of determinants; $\widetilde{M}$ is the unique *adjugate* of M in which $\widetilde{M}_{ji}$ is the cofactor of M_{ij}. (An alternative name, the *classical adjoint*, risks confusion with the adjoint, M^*.)

If M is a unitary $2^t\times 2^t$ matrix and $t > 1$ there is a divide and conquer matrix inverse algorithm for which proposition 4.1 provides the base case.

Fourier transforms reduce the problem to inverting four $2^{t-1}\times 2^{t-1}$ (and, by recursion, to inverting $n^2/4$ 2×2) unitary matrices. Since $M = \sum_{g\in\Phi_2^{(t)}} a_g \rho_{\Phi_2}^{(t)}(g)$ and $\rho_{\Phi_2}^{(t)}$ are unitary, $M^* = \sum_{h\in\Phi_2^{(t)}} \bar{a}_h [\rho_{\Phi_2}^{(t)}(h)]^{-1}$. So $M^*M = 1_{2^t}$ implies not only $\sum_{g\in\Phi_2} \bar{a}_g a_g = 1$ but also that the terms $\bar{a}_h a_g [\rho_{\Phi_2}^{(t)}(h)]^{-1}\rho_{\Phi_2}^{(t)}(g)$ with $g \neq h$ will cancel.

For all k in $\Phi_2^{(t)}$, as $[\rho_{\Phi_2}^{(t)}(k)]^{-1}M^{-1}\rho_{\Phi_2}^{(t)}(k) \,.\, [\rho_{\Phi_2}^{(t)}(k)]^{-1}M\rho_{\Phi_2}^{(t)}(k) = 1_{2^t}$, representations of the inner automorphisms I_k preserve inverses: the inverse of the inner automorphism induced transform of M is the inner automorphism induced transform of M^{-1}.

Calculating the product $M^{-1}M$ by averaging these equivalent products eventually reduces to computing the coefficient of the identity element in a convolution in $\mathbf{C}^{2\times 2}C_2^{2t-2}$. The proof uses induction on t and the following definitions.

If $M = \sum_{g_{-t},g_t=0}^{1} M_{g_{-t}g_t}^{(t-1)} \otimes A_{-1}^{g_{-t}} A_1^{g_t}$ represents an element in $\mathbf{C}^{2^{t-1}\times 2^{t-1}}\Phi_2^{(1)}$, since $A_{-t}^{k_{-t}} A_t^{k_t} = 1_{2^{t-1}} \otimes A_{-1}^{k_{-t}} A_1^{k_t}$, the inner automorphism induced transform of M is

$$
\begin{aligned}
I_{k_{-t}k_t}(M) &= 1_{2^{t-1}} \otimes (A_{-1}^{k_{-t}} A_1^{k_t})^{-1} . \sum_{g_{-t},g_t=0}^{1} M_{g_{-t}g_t}^{(t-1)} \otimes A_{-1}^{g_{-t}} A_1^{g_t} \; . \; 1_{2^{t-1}} \otimes A_{-1}^{k_{-t}} A_1^{k_t} \\
&= \sum_{g_{-t},g_t=0}^{1} M_{g_{-t}g_t}^{(t-1)} \otimes [(A_{-1}^{k_{-t}} A_1^{k_t})^{-1} \; . \; A_{-1}^{g_{-t}} A_1^{g_t} \; . \; A_{-1}^{k_{-t}} A_1^{k_t}] \\
&= \sum_{g_{-t},g_t=0}^{1} M_{g_{-t}g_t}^{(t-1)} \otimes [A_0^{g_{-t}k_t - g_t k_{-t}} \; . \; A_{-1}^{g_{-t}} A_1^{g_t}] \qquad \text{, by (2.2)}, \\
&= \sum_{g_{-t},g_t=0}^{1} M_{g_{-t}g_t}^{(t-1)} \omega^{g_{-t}k_t - g_t k_{-t}} \otimes A_{-1}^{g_{-t}} A_1^{g_t}.
\end{aligned}
$$

Let $\mathcal{M}_{k_{-t}k_t}^{(t-1)} = \sum_{g_{-t},g_t=0}^{1} M_{g_{-t}g_t}^{(t-1)} \omega^{g_{-t}k_t - g_t k_{-t}}$, for $0 \le k_{-t} < 2$ and $0 \le k_t < 2$, denote the $\mathbf{C}^{2^{t-1}\times 2^{t-1}} C_2^2$ transforms of the four components $M_{g_{-t}g_t}^{(t-1)}$.

Similarly, for $M^* = \sum_{h_{-t},h_t=0}^{1} (M_{h_{-t}h_t}^{(t-1)})^* \otimes (A_{-1}^{h_{-t}} A_1^{h_t})^{-1}$,

$$
I_{k_{-t}k_t}(M^*) = \sum_{h_{-t},h_t=0}^{1} (M_{h_{-t}h_t}^{(t-1)})^* \omega^{-(h_{-t}k_t - h_t k_{-t})} \otimes (A_{-1}^{h_{-t}} A_1^{h_t})^{-1}
$$

and the $\mathbf{C}^{2^{t-1}\times 2^{t-1}} C_2^2$ transforms $\sum_{h_{-t},h_t=0}^{1} (M_{h_{-t}h_t}^{(t-1)})^* \omega^{-(h_{-t}k_t - h_t k_{-t})}$ of the four components $(M_{h_{-t}h_t}^{(t-1)})^*$ are the adjoints of $\mathcal{M}_{k_{-t}k_t}^{(t-1)}$.

Now, the average $M^*M = 2^{-2} \sum_{k_{-t},k_t=0}^{1} I_{k_{-t}k_t}(M^*) I_{k_{-t}k_t}(M)$ implies

$$
M^*M = 2^{-2} \sum_{g_{-t},g_t=0}^{1} \sum_{h_{-t},h_t=0}^{1} (M_{h_{-t}h_t}^{(t-1)})^* M_{g_{-t}g_t}^{(t-1)} \otimes A_1^{-h_t} A_{-1}^{(g_{-t}-h_{-t})} A_1^{g_t} \times \sum_{k_{-t},k_t=0}^{1} \omega^{k_t(g_{-t}-h_{-t}) - k_{-t}(g_t - h_t)}.
$$

By proposition 1.3, the coefficients of terms $A_1^{-h_t} A_{-1}^{(g_{-t}-h_{-t})} A_1^{g_t}$ vanish on summing over k_t and k_{-t} unless $g_{-t} = h_{-t}$ and $g_t = h_t$. But then $A_1^{-h_t} A_{-1}^{(g_{-t}-h_{-t})} A_1^{g_t} = 1_2$ and so

$$
M^*M = 2^{-2} \sum_{k_{-t},k_t=0}^{1} (\mathcal{M}_{k_{-t}k_t}^{(t-1)})^* \mathcal{M}_{k_{-t}k_t}^{(t-1)} \otimes 1_2.
$$

Proposition 4.2 The matrix $M = \sum_{g\in\Phi_2} a_g \rho_{\Phi_2}^{(t)}(g)$ is unitary if and only if the transforms $\mathcal{M}_{k_{-t}k_t}^{(t-1)}$ are unitary.

Proof One stage of a $\mathcal{T}_1^{-1}$ transform for $\rho_{\Phi_2}^{(1)}$ applied to M determines the components of an equivalent element in $\mathbf{C}^{2^{t-1}\times 2^{t-1}} \Phi_2^{(1)}$. These, with zero components for elements of $G_2(2,1)$ not in $\Phi_2^{(1)}$, form components of an element $m = \sum_{g\in G_2(2,1)} a_g g$ in the group algebra $\mathbf{C}^{2^{t-1}\times 2^{t-1}} G_2(2,1)$.

In principle, m and $m^* = \sum_{g\in G_2(2,1)} a_g^* g^{-1}$ could be multiplied using the Fourier transform algorithm in proposition 3.3. In step (iii) of the algorithm, components of the product element mm^* are shown by (3.6) to be the sum of contributions from each of the irreducible representations of $G_2(2,1)$.

If g is in $\Phi_2^{(1)}$ then $A_0 g$ is not; however, the one dimensional representations do not distinguish $A_0 g$ from g and so if the one dimensional representations together contribute a value a to the component of g they will also contribute a to the component of $A_0 g$. On the other hand, if the 2×2 representation contributes a value b to the component of g, since $\rho_{\Phi_2}^{(1)}(A_0 g) = -\rho_{\Phi_2}^{(1)}(g)$, the contribution to the component of $A_0 g$ is $-b$.

If mm^* is the identity element then the component of $A_0 g$ is zero so $a = b$ and the convolution is completely determined by the contributions of the one dimensional representations. But the component of g in $\Phi_2^{(1)}$ must also vanish if $g \ne 1$ and must be $1_{2^{t-1}}$ if $g = 1$.

The matrix of one dimensional representations is a 2-Hadamard matrix so the inverse transform for the one dimensional representations will yield zero components for elements $g \neq 1$ and a component $1_{2^{t-1}}$ for $g = 1$ precisely when the $\mathbf{C}^{2^{t-1}\times 2^{t-1}}$matrix products $(\mathcal{M}^{(t-1)}_{k_{-t}k_t})^*\mathcal{M}^{(t-1)}_{k_{-t}k_t}$ in step (ii) of the convolution algorithm are each equal to $1_{2^{t-1}}$. But then the matrices $\mathcal{M}^{(t-1)}_{k_{-t}k_t}$ are unitary.

Since Fourier transforms convert the unitary matrix M to unitary matrices $\mathcal{M}^{(t-1)}_{k_{-t}k_t}$, the inverse transforms must convert these to the unitary matrix M. ∎

Proposition 4.2 shows that $\mathcal{T}_3$ transforms preserve the unitary property and also that they can reduce multiplying a $2^t\times 2^t$ unitary matrix by its adjoint to a convolution in $\mathbf{C}^{2\times 2}C_2^{2t-2}$ in which $n^2/4$ 2×2 unitary matrices are multiplied by their adjoints.

Each of the $n^2/4$ 2×2 products reduces to multiplying a pair of quaternions by their inverses. (Since $2^t\times 2^t$ unitary bimatrices represent the $\mathbf{R}\Theta^{(t)}_2$ subset of $\mathbf{R}\Phi^{(t+1)}_2$, inverses are preserved by representations of inner automorphisms I_k for k in $\Phi^{(t+1)}_2$ and A_{-t-1}, which anticommutes with A_{t+1}, introduces a further n^2 automorphisms which correspond to swapping the upper and lower matrices in the bimatrix. This creates a further factor of C_2 in the convolution which in this case is in $\mathbf{H}C_2^{2t-1}$.)

Proposition 4.3 Given a 2×2 unitary matrix M, the corresponding 2×2 $M : M_B$ bimatrix defined in proposition 3.7 is unitary. Also, the matrices $\mathcal{M}_1$ and $\mathcal{M}_2$ derived from the $M : M_B$ bimatrix by a half $\mathcal{T}_3$ transform represent quaternions and are unitary precisely when the bimatrix is unitary.

Proof For $t = 1$, by proposition 3.7, M_1 and M_2 represent quaternions. So, in

$$M^*M = (M_1^* - \zeta M_2^*)(M_1 + \zeta M_2) = M_1^*M_1 + M_2^*M_2 + \zeta(M_1^*M_2 - M_2^*M_1) = 1_2,$$

as in the proof of proposition 4.1, the noncentral parts of $M_1^*M_1$ and $M_2^*M_2$ are zero. Also, since $M_1^*M_2 - M_2^*M_1$ represents a quaternion and the right hand side of the final equality is 1_2, $\zeta(M_1^*M_2 - M_2^*M_1) = 0$. But then M_B is unitary since

$$M_B^*M_B = M_1^*M_1 + M_2^*M_2 = M^*M = 1_2.$$

The matrices $\mathcal{M}_1$ and $\mathcal{M}_2$ represent quaternions since, by remark 3.7, they represent elements of $\mathbf{R}\Phi^{(1)}_2$. The proof that they are unitary precisely when M is unitary follows as in the proof of proposition 4.2 from the fact that, for a convolution in $\mathbf{H}C_2$, the 2×2 matrix of one dimensional representations is a Hadamard matrix. ∎

Together propositions 4.2 and 4.3 imply that there is an algorithm for multiplying a $2^t\times 2^t$ unitary matrix by its inverse which involves a convolution in $\mathbf{H}C_2^{2t-1}$. They also show that if M is unitary, the $\mathcal{T}_3$ and half $\mathcal{T}_3$ transforms preserve the unitary property in the matrices they produce.

4.2 Inverting and multiplying $2^t\times 2^t$ matrices

Proposition 4.4 If A° denotes any anti-involution of a matrix A then $(AB)^\circ = A^\circ B^\circ$ if and only if A and B commute.

Proof If A and B commute, $(AB)^\circ = (BA)^\circ = A^\circ B^\circ$.

If $(AB)^\circ = A^\circ B^\circ$ then $AB = (A^\circ B^\circ)^\circ = BA$. ∎

Algorithms for inverting or multiplying $2^t\times 2^t$matrices use $\rho^{(t)}_{\Phi_1}$ and $\mathcal{P}^{(t)}_{\Theta_1}$.

Corollary 2.10(ii) shows that if $M = \sum_{g\in\Phi_1^{(t)}} a_g\rho^{(t)}_{\Phi_1}(g)$, $M^{\top\vdash} = \sum_{g\in\Phi_1^{(t)}} a_g\bar{\rho}^{(t)}_{\Phi_1}(g)$, $M^{\vdash} = \sum_{g\in\Phi_1^{(t)}} a_g\rho^{(t)}_{\Phi_1}(g^{-1})$ and $M^{\top} = \sum_{g\in\Phi_1^{(t)}} a_g\bar{\rho}^{(t)}_{\Phi_1}(g^{-1})$ so, since $\Phi_1^{(t)}$ is centrohermitian, the components of an element in $\mathbf{R}\Phi_1^{(t)}$ simultaneously represents all four involutions of a centrohermitian matrix M. Proposition 4.4 shows that the product of

such matrices will likewise be represented by an element in $\mathbf{R}\Phi_1^{(t)}$ precisely when the matrices commute.

In the case of an arbitrary complex matrix M, the bimatrix $M : M^{*\vdash}$ is centrohermitian. It follows that the product of commuting representations and hence elements of $\mathbf{R}\Theta_1^{(t)}$ are similarly in $\mathbf{R}\Theta_1^{(t)}$.

These products are a function of the cosets of C_2 in their parent groups and again through the inner automorphism induced transforms reduce to convolutions in abelian group algebras.

Since any matrix commutes with its powers, there are algorithms for inverting, squaring (and hence multiplying) centrohermitian matrices and bimatrices.

Proposition 4.5 Let M be a nonsingular centrohermitian $2^s \times 2^s$ matrix. If $s = 0$, M^{-1} is the reciprocal of M. When $s > 0$, M^{-1} is determined by

(i) applying a $\mathcal{T}_3$ transform for $\rho_{\Phi_1}^{(1)}$ to M to get $\{\mathcal{M}_{uv}\}_{u,v\in[0,2)}$,
(ii) invoking this algorithm recursively to invert the four $2^{s-1}\times 2^{s-1}$ matrices $\mathcal{M}_{uv}$,
(iii) applying a $\mathcal{T}_3^{-1}$ transform for $\{[\rho_{\Phi_1}^{(1)}(g)]^{-1}\}_{g\in\Phi_1}$ to $\{\mathcal{M}_{uv}^{-1}\}_{u,v\in[0,2)}$ to get M^{-1}.

Proof As for proposition 4.2. ∎

Proposition 4.6 Let $M : M^{*\vdash}$ be a nonsingular centrohermitian $2^t \times 2^t$ bimatrix. M^{-1} is obtained using

(i) a half $\mathcal{T}_3$ transform to get $\mathcal{M}_1$ and $\mathcal{M}_2$,
(ii) proposition 4.3 to invert $\mathcal{M}_1$ and $\mathcal{M}_2$,
(iii) a half $\mathcal{T}_3^{-1}$ transform for $\{[\rho_{\Phi_1}^{(1)}(g)]^{-1}\}_{g\in\Phi_1}$ to get $M^{-1} : (M^{*\vdash})^{-1}$ and hence M^{-1} from $\mathcal{M}_1^{-1}$ and $\mathcal{M}_2^{-1}$.

Proof The proof here differs only in that cosets of C_2 in $\mathcal{G}_1(2,t)$, rather than $G_1(2,t)$, are involved so the convolution is in $\mathbf{R}C_2^{2t+1}$. ∎

In these algorithms if M is singular, one or more of the reciprocals will be infinite.

Proposition 4.7 Let M be a $2^s \times 2^s$ centrohermitian matrix. M^2 is the square of M if $s = 0$ and is otherwise obtained by

(i) using a $\mathcal{T}_3$ transform for $\rho_{\Phi_1}^{(1)}$ to get $\{\mathcal{M}_{uv}\}_{u,v\in[0,2)}$ from M,
(ii) recursively computing the $2^{s-1}\times 2^{s-1}$ the squares of $\{\mathcal{M}_{uv}\}_{u,v\in[0,2)}$,
(iii) using a $\mathcal{T}_3^{-1}$ transform for $\rho_{\Phi_1}^{(1)}$ to get M^2 from $\{\mathcal{M}_{uv}^2\}_{u,v\in[0,2)}$.

Proof Again, this is similar to the proof of proposition 4.2. ∎

Proposition 4.8 The square of a $2^t \times 2^t$ centrohermitian bimatrix $M : M^{*\vdash}$ is obtained

(i) using a half $\mathcal{T}_3$ transform to get $\mathcal{M}_1$ and $\mathcal{M}_2$ from $M : M^{*\vdash}$,
(ii) using proposition 4.7 to get $\mathcal{M}_1^2$ and $\mathcal{M}_2^2$,
(iii) using a half $\mathcal{T}_3^{-1}$ transform to get $M^2 : (M^2)^{*\vdash}$ from $\mathcal{M}_1^2$ and $\mathcal{M}_2^2$.

Proof As in proposition 4.6, the convolution is in $\mathbf{R}C_2^{2t+1}$. ∎

In these algorithms, the $O(n^2 \log n)$ operations for the transforms dominate the $O(n^2)$ other operations. Now

$$\begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix}^2 = \begin{pmatrix} AB & 0 \\ 0 & BA \end{pmatrix}$$

implies that, for A and B in $\mathbf{C}^{2^t\times 2^t}$, AB and BA are obtained using a convolution which is in $\mathbf{R}C_2^{2t+2}$ rather than $\mathbf{R}C_2^{2t+3}$ since the special form of the operand implies that the only nonzero terms of $\mathbf{R}\Phi_1^{t+2}$ contain $A_{-t-2}^{(t+2)}$ as a factor; this means ω_{-t-2} can be factored from the convolution.

4.3 Inverting and multiplying $p^t \times p^t$ matrices

When p is odd, the algorithms are slightly different.

Proposition 2.12 shows that the map y from elements in C_p^{2t} to $\Phi^{(t)}$ preserves inverses; it also preserves the identity element. It does not possess the other property of group maps since there exist a, b and c in C_p^{2t} such that $ab = c$ while $y(a)y(b) \neq y(c)$.

The representations of Φ are, however, projective representations [10, §53] of C_p^{2t} in that $y(a)y(b) = A_0^r y(c)$, for some r, and A_0 is represented by the scalar ω. These representations also possess another property shown by proposition 4.4.

Corollary 2.11 shows that if $M = \sum_{g \in \Phi^{(t)}} a_g \rho_\Phi^{(t)}(g)$ then the components $\{a_g\}_{g \in \Phi}$ again specify all four involutions of M so proposition 4.4 then implies that when p is odd products of elements in $\mathbf{C}\Phi^{(t)}$ are in $\mathbf{C}\Phi^{(t)}$ precisely when the elements commute.

When calculating a product of two elements in $\mathbf{C}\Phi^{(t)}$, in order that the product is also in $\mathbf{C}\Phi^{(t)}$, the convolution algorithm in proposition 3.3 shows that the contributions made to the component of a product term in $\Phi(t)$ made by the one dimensional representations is exactly equal to the the contributions that the matrix representations make to that component.

For any term not in $\Phi^{(t)}$, the contributions made by the one dimensional representations exactly cancel the contributions made by the matrix representations.

Consequently, such a convolution is completely determined by the one dimensional representations and so matrices can be inverted or squared by a $\mathbf{C}C_p^{2t}$ convolution and hence multiplied by a $\mathbf{C}C_p^{2t+1}$ convolution.

When p is odd, $\mathbf{C}\Phi^{(t)}$ is the algebra of commuting $p^t \times p^t$ complex matrices.

The inner automorphism induced transforms again respect such commuting products and, since any matrix commutes with its own powers, they reduce inverting or squaring a $p^t \times p^t$ matrix M to a convolution in $\mathbf{C}C_p^{2t}$.

Proposition 4.9 Let M be a nonsingular complex $p^s \times p^s$ matrix where p is odd. If $s = 0$, M^{-1} is the reciprocal of M and, if $s > 0$, M^{-1} is determined by

(i) applying a $\mathcal{T}_3$ transform for $\rho_\Phi^{(1)}$ to M to get $\{\mathcal{M}_{uv}\}_{u,v \in [0,p)}$,

(ii) recursively computing the p^2 $p^{s-1} \times p^{s-1}$ matrices $\mathcal{M}_{uv}^{-1}$,

(iii) using a $\mathcal{T}_3^{-1}$ transform for $\{\rho_\Phi^{(1)}(g^{-1})\}_{g \in \Phi^{(1)}}$ to get M^{-1} from $\{\mathcal{M}_{uv}^{-1}\}_{u,v \in [0,p)}$.

Proof One stage of a $\mathcal{T}_1^{-1}$ transform for $\rho_\Phi^{(1)}$ applied to M determines components of an element in $\mathbf{C}^{p^{s-1} \times p^{s-1}} \Phi^{(1)}$. With zero components for group elements not in $\Phi^{(1)}$, they specify an element m in the algebra $\mathbf{C}^{p^{s-1} \times p^{s-1}} G(p, 1)$. M^{-1} similarly determines m^{-1}.

As in proposition 4.2, the formation of the product mm^{-1} using the convolution algorithm of proposition 3.3 is examined: in particular, the contributions made by the various irreducible representations to the components of the product element mm^{-1}.

If the one dimensional representations contribute a value a to the component of an element g in $\Phi^{(1)}$, they will also contribute a to the components of $A_0^r g$, for $1 \leq r < p$.

One matrix representation will contribute a value b_1 to the component of g and $\omega^{-r} b_1$ to the components of $A_0^r g$, for $1 \leq r < p$.

A second matrix representation will contribute b_2 to the component of g and $\omega^{-2r} b_2$ to the components of $A_0^r g$, for $1 \leq r < p$.

In general, for $1 \leq k < p$, the kth matrix representation will contribute b_k to the component of g and $\omega^{-kr} b_k$ to the components of $A_0^r g$, for $1 \leq r < p$.

The sum of the distinct pth roots of unity is zero so the components of $A_0^r g$, for $1 \leq r < p$, vanish precisely when $a = b_k$ for all k. This and the matrix of one dimensional representations being p-Hadamard completes the proof as in proposition 4.2. ∎

Evidently if M is singular at least one of the reciprocals will involve division by zero.

Proposition 4.10 Let M be a $p^s \times p^s$ complex matrix where p is odd; M^2 is the square of the complex number M if $s = 0$ and, if $s > 0$, M^2 is determined by

(i) applying a $\mathcal{T}_3$ transform for $\rho_\Phi^{(1)}$ to M to get $\{\mathcal{M}_{uv}\}_{u,v\in[0,p)}$,

(ii) recursively computing the p^2 $p^{s-1}\times p^{s-1}$ products $\mathcal{M}^2_{uv}$,

(iii) using a $\mathcal{T}_3^{-1}$ transform for $\rho_\Phi^{(1)}$ to get M^2 from $\{\mathcal{M}^2_{uv}\}_{u,v\in[0,p)}$. ∎

It is well known that an algorithm for $n = p^t$ extends to an algorithm for matrices of any size. For $N\times N$ matrices where $N \neq p^t$, as there is an integer t such that $N < p^t < pN$, appending a diagonal block 1_{p^t-N} to an $N\times N$ matrix makes a $p^t\times p^t$ matrix to which the $p^t\times p^t$ algorithm can be applied and the $N\times N$ result inferred. Since $p^t < pN$, an $O(n^2\log n)$ algorithm always implies an $O(N^2\log N)$ algorithm.

Similarly, an $O(N^2\log N)$ algorithm for an $N\times N$ matrix implies that, if k is constant, $kN\times kN$ matrices also need only $O(N^2\log N)$ operations.

For $p = 3$, squaring a $3^{t+1}\times 3^{t+1}$ matrix

$$\begin{pmatrix} & A & \\ & & B \\ C & & \end{pmatrix}^2 = \begin{pmatrix} & & AB \\ BC & & \\ & CA & \end{pmatrix}$$

determines the products of adjacent pairs from the cyclic sequence A, B and C of three $3^t\times 3^t$ matrices. The convolution is in $\mathbf{C}C_3^{2t+1}$ since the only nonzero terms in the element of $\mathbf{C}\Phi^{(t+1)}$ being squared are those containing $A^{(t+1)}_{-t-1}$ as a factor; this means ω_{-t-1} can be factored from the convolution.

In general, when p is odd, a convolution in $\mathbf{C}C_p^{2t+1}$ determines the products of adjacent pairs in a cyclic sequence of p $n\times n$ matrices.

4.4 The matrix eigenvalue problem

A *diagonal matrix* has (i, j) elements that are zero if $i \neq j$; an *upper triangular matrix* has (i, j) elements that are zero if $i > j$. For matrices M and T where T is nonsingular the transform $T^{-1}MT$ of M by T is called a *similarity transform* and the matrices $T^{-1}MT$ and M are said to be *similar*; if T is unitary then they are *unitarily similar*. Similar matrices have the same eigenvalues [28, Chapter1, §5].

The product $T^{-1}MT$ is another product which is a function of the cosets. For any nonsingular matrix T, $\{T^{-1}\rho^{(t)}(g)T\}_{g\in G(p,t)}$ is a representation in the same equivalence class as $\rho^{(t)}$ and $\{T^{-1}\rho_\Phi^{(t)}(g)T\}_{g\in\Phi}$ is a coset space basis. But then, if M represents an element in $\mathbf{C}\Phi^{(t)}$ so does $T^{-1}MT$ and the corresponding group algebra product is determined again by an abelian group algebra.

For any square matrix M there is a unitarily similar matrix $T^{-1}MT = V$ that is diagonal when M is normal and upper triangular otherwise; in either case, the diagonal elements are the eigenvalues of M [28, Chapter1, §47and §48]. In the former case, the columns of T are a complete orthonormal set of eigenvectors. Here the convolution is induced by the transforms $I_k^{-1}[I_k(T^{-1})I_k(M)I_k(T)] = V$.

Repeated use is made of the next proposition, in which, for z in $\mathbf{C}$, $|z|^2 = z\bar{z}$.

Proposition 4.11 If M is a complex 2×2 matrix then there is a unitary matrix T representing a quaternion such that $T^{-1}MT$ is upper triangular.

Proof Using the representation $\rho^{(1)}_{\Phi_{0'}}$,

$$M = \begin{pmatrix} a & \\ & a \end{pmatrix} + \begin{pmatrix} & b \\ b & \end{pmatrix} + \begin{pmatrix} c & \\ & -c \end{pmatrix} + \begin{pmatrix} & -\zeta d \\ \zeta d & \end{pmatrix} = \begin{pmatrix} a+c & b-\zeta d \\ b+\zeta d & a-c \end{pmatrix},$$

If $b = -\zeta d$ then $T = 1_2$ suffices.

If $b \neq -\zeta d$ then a construction suggested by Wilkinson [28, Chapter1, §47 and §44] can be used. From $|M - \lambda 1_2| = 0$, the eigenvalues of M are $\lambda = a \pm q$, where $q^2 = b^2 + c^2 + d^2$. Also v where $v^\top = (q + c, b + \zeta d)$ is an eigenvector for the eigenvalue $a + q$.

The matrix T with elements $T_{00} = r, T_{01} = -\bar{s}, T_{10} = s$ and $T_{11} = \bar{r}$ is unitary if $|r|^2 + |s|^2 = 1$. Since $b \neq -\zeta d$, $|v|^2 = |q + c|^2 + |b + \zeta d|^2 > 0$ so let $r = (q + c)/|v|$ and $s = (b + \zeta d)/|v|$ making T unitary and $(T^{-1}v)^\top = (|v|, 0)$. Now,

$$Mv = \lambda v \;\Rightarrow\; (T^{-1}MT)T^{-1}v = \lambda T^{-1}v \;\Rightarrow\; (T^{-1}MT)\begin{pmatrix}|v|\\0\end{pmatrix} = \lambda\begin{pmatrix}|v|\\0\end{pmatrix}$$

which implies that $T^{-1}MT$ is upper triangular and

$$T = |v|^{-1}[\Re(q + c).1_2 + \Im(b + \zeta d).A_{-1} + \Im(q + c).A_1 - \Re(b + \zeta d).A_{-1}A_1]$$

where 1_2, A_{-1}, A_1 and $A_{-1}A_1$ are the matrices in (2.7(iii)) which represent the quaternion basis elements. As their coefficients are real, T represents a quaternion. ∎

The set of $v \times v$ matrices with matrix elements in $\mathbf{C}^{u\times u}$ is denoted subsequently by $(\mathbf{C}^{u\times u})^{v\times v}$ while $\mathbf{C}^{v\times v}$ is retained for the special case $(\mathbf{C}^{1\times 1})^{v\times v}$. A monomial matrix P in which all nonzero elements are one is a *permutation matrix*, so-called because $P^{-1}MP = P^\top MP$ permutes of the rows and columns of M.

Proposition 4.12 If $\widehat{M}$ in $(\mathbf{C}^{2^{s-1}\times 2^{s-1}})^{2\times 2}$ has upper triangular matrix elements, there is a unitary matrix $P\tau$ in $\mathbf{C}^{2^s\times 2^s}$ such that $\tau^{-1}P^{-1}\widehat{M}P\tau$ in $\mathbf{C}^{2^s\times 2^s}$ is upper triangular.
Proof The transform $P^{-1}\widehat{M}P$ by the permutation matrix P with nonzero elements

$$P_{j\,2j} = P_{j+2^{s-1}\,2j+1} = 1, \quad 0 \leq j < 2^{s-1}$$

interleaves rows in the upper half of $\widehat{M}$ above those in the lower half and similarly interleaves columns in the left half to the left of those in the right half. So $P^{-1}\widehat{M}P$ in $(\mathbf{C}^{2\times 2})^{2^{s-1}\times 2^{s-1}}$ is upper triangular. Let the 2×2 matrix elements of $P^{-1}\widehat{M}P$ be denoted m_{jk}, for j and k in $[0, 2^{s-1})$. Using proposition 4.11, a diagonal unitary matrix τ in $(\mathbf{C}^{2\times 2})^{2^{s-1}\times 2^{s-1}}$ can be constructed so that its 2×2 diagonal elements τ_j leave $\tau_j^{-1}m_{jj}\tau_j$ for $0 \leq j < 2^{s-1}$ in upper triangular form. But now,

$$\tau^{-1}P^{-1}\widehat{M}P\tau = \begin{pmatrix} \tau_0^{-1}m_{00}\tau_0 & \tau_0^{-1}m_{01}\tau_1 & \tau_0^{-1}m_{02}\tau_2 & \cdots \\ & \tau_1^{-1}m_{11}\tau_1 & \tau_1^{-1}m_{12}\tau_2 & \\ & & \tau_2^{-1}m_{22}\tau_2 & \\ & & & \ddots \end{pmatrix}$$

in $\mathbf{C}^{2^s\times 2^s}$ is upper triangular and $P\tau$ is unitary since P and τ are unitary.

Proposition 4.13 Given a $2^s\times 2^s$ matrix M, a unitary matrix T and an upper triangular matrix $T^{-1}MT$ are obtained from proposition 4.11 if $s = 1$ and otherwise by

(i) applying a $\mathcal{T}_3$ transform for $\rho^{(1)}_{\Phi_{0'}}$ to M to get $\{M_{uv}\}_{u,v\in[0,2)}$,

(ii) recursively computing $2^{s-1}\times 2^{s-1}$ unitary matrices T_{uv} and upper triangular matrices $T_{uv}^{-1}M_{uv}T_{uv}$,

(iii) (a) applying a $\mathcal{T}_3^{-1}$ transform for $\rho^{(1)}_{\Phi_2}$ to $\{T_{uv}\}_{u,v\in[0,2)}$ to get $\widehat{T}$ and
(b) applying a $\mathcal{T}_3^{-1}$ transform for $\rho^{(1)}_{\Phi_{0'}}$ to $\{T_{uv}^{-1}M_{uv}T_{uv}\}_{u,v\in[0,2)}$ to get $\widehat{M}$,

(iv) using the matrices P and τ defined in the proof of proposition 4.12 to compute the required matrices $T = (\widehat{T}P)\tau$ and $T^{-1}MT = \tau^{-1}(P^{-1}\widehat{M}P)\tau$.

Proof If M represents an element in $\mathbf{C}^{2^{s-1}\times 2^{s-1}}\Phi^{(1)}_{0'}$ and T is unitary then T^*MT also represents an element in $\mathbf{C}^{2^{s-1}\times 2^{s-1}}\Phi^{(1)}_{0'}$ so this product is a function of the cosets of C_{2^2} in $\mathcal{G}_0(2, 1)$.

Using proposition 3.3 to form this product, consideration is given to the contributions made in step (iii) of the algorithm to the components of the group elements g, Bg, A_0g and B^3g, of which only g is in $\Phi^{(1)}_{0'}$.

There are two sets of one dimensional irreducible representations distinguished by B being represented by 1 in one set and -1 in the other. It follows that the contributions made by the two sets of one dimensional representations to these four elements respectively will be of the form

$$a, \quad a, \quad a, \quad a \quad \text{and} \quad a, \ -a, \quad a, \ -a$$

while the two 2×2 representations similarly provide

$$b, \quad \zeta b, \quad -b, \ -\zeta b \quad \text{and} \quad b, \ -\zeta b, \quad -b, \quad \zeta b$$

so the product is in $\mathbf{C}^{2^{s-1}\times 2^{s-1}}\Phi^{(1)}_{0'}$ precisely when $a = b$. Again, the convolution is completely determined by the abelian group of inner automorphisms.

It remains to show that T is indeed unitary. The proof is by induction on s based on proposition 4.12 for the $s = 1$ case. By the inductive hypothesis, the matrices T_{uv} in step (iii) are unitary. By proposition 4.2, $\widehat{T}$ in step (iii)(a) is also unitary and $T = (\widehat{T}P)\tau$ in step (iv), being the product of unitary matrices, is unitary. ∎

If $s = t$ initially, proposition 4.13 employs a convolution in $\mathbf{C}^{2\times 2}C_2^{2t-2}$ and $O(n^2\log n)$ arithmetic operations are needed for the transforms. Proposition 4.11 is used $n(n-1)/2$ times with $n(2n\log_2 n - 3n + 2)/4$ 2×2 products in applying proposition 4.12 and computing T. Frequently (for example when applying proposition 4.17) only the eigenvalues are wanted. If T and the off diagonal elements of T^*MT are of no interest, the 2×2 matrix products and the transforms to recover T are redundant.

The following facts are well known [28, Chapter1].

(i) If, for all j in $[0, n)$, M has eigenvalues λ_j then M^* has eigenvalues $\bar{\lambda}_j$.

(ii) If $M = M^*$, M is hermitian and hermitian matrices have real eigenvalues.

(iii) Being self adjoint, hermitian matrices are normal so if M is hermitian then there is a unitary matrix T such that T^*MT is real and diagonal.

There appears to be no simpler way of recognizing whether a matrix M is normal than checking that $MM^* = M^*M$. Nor, apparently, is there any other simple characterization of normal matrices though their close relationship with hermitian matrices offers something of a remedy. If $M = M_1 + \zeta M_2$ is the unique decomposition of M into the hermitian matrices $M_1 = (M + M^*)/2$ and $M_2 = (M - M^*)/2\zeta$, it follows that, if M is normal, $M_1M_2 = M_2M_1$ is an alternative test. Of greater interest, there is a unitary matrix T such that $T^*M_1T + \zeta T^*M_2T = \Lambda$ is diagonal. Equating the hermitian and skew hermitian parts: $T^*M_1T = \Re(\Lambda)$ and $T^*M_2T = \Im(\Lambda)$.

The columns of T are unique to within multiplication by a scalar of modulus one so a normal matrix is one where an orthonormal set of eigenvectors can be determined by diagonalizing either M_1 or M_2. Given an algorithm for this, it is possible to determine T such that $T^*M_1T = \Re(\Lambda)$. Then, since M is normal, the columns of M_2T are real multiples of the columns of T and the real multiples determine $\Im(\Lambda)$.

Since the converse is trivial, M is normal if and only if there are real diagonal matrices D_1 and D_2 and a unitary matrix T such that $M = TD_1T^* + \zeta TD_2T^*$. The tests for normality, $M_1M_2 = M_2M_1$ and $MM^* = M^*M$, simply reflect the fact that D_1 and D_2, being diagonal, commute.

Normal matrices are certainly of interest. Penrose [21] remarks that quantum observables are conventionally represented by hermitian operators to guarantee real eigenvalues. Occasionally, however, the essential requirement is not that the eigenvalues are real but rather that the eigenvectors are orthogonal and correspond to distinct eigenvalues. This requires normal rather than hermitian operators.

Variants of propositions 4.11, 4.12 and 4.13 for hermitian matrices are needed.

Proposition 4.14 If M is a 2×2 hermitian matrix there is a unitary matrix T representing a quaternion such that T^*MT is real and diagonal.
Proof Using the representation $\rho^{(1)}_{\Phi_{0'}}$, there exist a, b, c and d in $\mathbf{R}$ such that

$$M = \begin{pmatrix} a & \\ & a \end{pmatrix} + \begin{pmatrix} & b \\ b & \end{pmatrix} + \begin{pmatrix} c & \\ & -c \end{pmatrix} + \begin{pmatrix} & -\zeta d \\ \zeta d & \end{pmatrix} = \begin{pmatrix} a+c & b-\zeta d \\ b+\zeta d & a-c \end{pmatrix}.$$

If $b = d = 0$, M is already diagonal with eigenvalues $a \pm c$, and $T = 1_2$ suffices. Otherwise the eigenvalues of M are again $\lambda = a \pm q$ where $q^2 = b^2 + c^2 + d^2$ so q too is real and, as in proposition 4.11,

$$T = |v|^{-1} \begin{pmatrix} q+c & -b+\zeta d \\ b+\zeta d & q+c \end{pmatrix} = |v|^{-1}((q+c)1_2 + dA_{-1} - bA_{-1}A_1)$$

represents a quaternion while T^*MT, being hermitian and upper triangular, is real and diagonal. ∎

Proposition 4.15 If $\widehat{M}$ in $(\mathbf{C}^{2^{s-1}\times 2^{s-1}})^{2\times 2}$ is hermitian with diagonal matrix elements, there is a unitary matrix $P\tau$ such that $\tau^{-1}P^{-1}\widehat{M}P\tau$ in $\mathbf{C}^{2^s\times 2^s}$ is real and diagonal.
Proof The transform $P^{-1}\widehat{M}P$ by the permutation matrix P with nonzero elements

$$P_{j\,2j} = P_{j+2^{s-1}\,2j+1} = 1, \quad 0 \le j < 2^{s-1},$$

in this case, leaves $P^{-1}\widehat{M}P$ in $(\mathbf{C}^{2\times 2})^{2^{s-1}\times 2^{s-1}}$ diagonal and hermitian. Let the diagonal 2×2 hermitian matrix elements of $P^{-1}\widehat{M}P$ be denoted by m_j. Using proposition 4.14, a diagonal unitary matrix τ in $(\mathbf{C}^{2\times 2})^{2^{s-1}\times 2^{s-1}}$ can be constructed so that its 2×2 diagonal elements τ_j leave $\tau_j^{-1}m_j\tau_j$, in real diagonal form. But now, $\tau^{-1}P^{-1}\widehat{M}P\tau$ in $\mathbf{C}^{2^s\times 2^s}$ is real and diagonal and $P\tau$ is unitary since P and τ are unitary. ∎

Proposition 4.16 Given a $2^s\times 2^s$ hermitian matrix M, a unitary matrix T and a real diagonal matrix $T^{-1}MT$ are obtained from proposition 4.14 if $s = 1$ and otherwise by

(i) applying a $\mathcal{T}_3$ transform for $\rho^{(1)}_{\Phi_{0'}}$ to M to get the hermitian set $\{M_{uv}\}_{u,v\in[0,2)}$,

(ii) recursively computing $2^{s-1}\times 2^{s-1}$ unitary matrices T_{uv} and real diagonal matrices $T_{uv}^{-1}M_{uv}T_{uv}$,

(iii) (a) applying a $\mathcal{T}_3^{-1}$ transform for $\rho^{(1)}_{\Phi_2}$ to $\{T_{uv}\}_{u,v\in[0,2)}$ to get $\widehat{T}$ and
(b) applying a $\mathcal{T}_3^{-1}$ transform for $\rho^{(1)}_{\Phi_{0'}}$ to $\{T_{uv}^{-1}M_{uv}T_{uv}\}_{u,v\in[0,2)}$ to get the hermitian matrix $\widehat{M}$,

(iv) using the matrices P and τ, defined in the proof of proposition 4.15, to compute the required matrices $T = (\widehat{T}P)\tau$ and $T^{-1}MT = \tau^{-1}(P^{-1}\widehat{M}P)\tau$. ∎

Some minor inefficiencies in these algorithms were traded for expository convenience. The similarity transforms involving the permutation matrix P mentioned in propositions 4.12, 4.13, 4.15 and 4.16 are not necessary and with some rearrangement of the computation they can be discarded. Similarly, the $\mathcal{T}_1$ part of the $\mathcal{T}_3^{-1}$ transform which produces the matrix $\widehat{M}$ in step (iii(b)) of propositions 4.13 and 4.16 is immediately undone in the process of determining the diagonal matrix τ.

4.5 Related algorithms

Proposition 4.17 The zeros of an arbitrary polynomial of degree n with complex coefficients can be determined with $O(n^2\log n)$ operations using proposition 4.13.
Proof After dividing the coefficients of the given polynomial by the coefficient of the term of degree n, let the resulting polynomial be $\lambda^n - \sum_{j=0}^{n-1} a_j\lambda^j$. The zeros of this

polynomial are the eigenvalues of its companion matrix M [28, Chapter 1, §10], which has nonzero elements $M_{r+1r} = 1$ for $0 \leq r < n-1$ and $M_{0s} = a_{n-1-s}$ for $0 \leq s < n$. ■

An algorithm for finding the zeros of a polynomial implies that a construction in [14] for the economical evaluation of real polynomials becomes an algorithm.

$O(N^2 \log N)$ algorithms for $N \times N$ matrix operations imply $O(N^2 \log N)$ algorithms in many disciplines for many other problems including those mentioned in the introduction: recognizing a sentence of length N in an arbitrary context free language or computing the transitive closure of a directed graph with N nodes or, equivalently, computing the transitive closure of a relation on a finite set of cardinality N.

Acknowledgements

I am indebted to several colleagues, particularly the late J.S. Rose, for their patience and encouragement over the apparently interminable period in which this work was carried out. I also wish to express my gratitude to the late W.L. James, the late H.C. Bolton, the late G.S. Rushbrooke and the late A.J. Perlis; their contributions were greater than they could ever conceive.

References

[1] A.V.Aho, J.E.Hopcroft and J.D.Ullman, The Design and Analysis of Computer Algorithms (Addison-Wesley, Reading, Mass., 1974).

[2] M.D.Atkinson, The complexity of group algebra computations, Theoret. Computer Sci. **5**(1977)205–209.

[3] E.W.Bastin and C.W.Kilmister, The analysis of observations, Proc. Roy. Soc. **A212**(1952) 559–576.

[4] R.P.Brent, Algorithms for matrix multiplication, Stanford University Technical Report STAN-CS-70-157(AD 705509).

[5] T.W.Cairns, On the fast Fourier transform on finite abelian groups, IEEE Trans. Computers **20**(1971)569–571.

[6] W.K.Clifford, Applications of Grassman's extensive algebra, Amer. J. Math. **1**(1878)350–358.

[7] J.M.Cooley and J.W.Tukey, An algorithm for the machine computation of complex Fourier series, Math. Comp. **19**(1965)297–301.

[8] D.Coppersmith and S.Winograd, On the asymptotic complexity of matrix multiplication, SIAM J. Comput. **11**(1982)472–492.

[9] ———, Matrix multiplication and arithmetic progressions, Proc. Nineteenth ACM Theory of Computing Symposium, New York, 1986, 1–6.

[10] C.W.Curtis and I.R.Reiner, Representation Theory of Finite Groups and Associative Algebras (Interscience, New York, 1962).

[11] P.A.M.Dirac, The quantum theory of the electron, Proc. Roy. Soc. **A117**(1927)610–624.

[12] A.S.Eddington, On sets of anticommuting matrices, J. Lond. Math. Soc. **7**(1932)58–68.

[13] ———, On sets of anticommuting matrices. Part II: the factorisation of the E-numbers, J. Lond. Math. Soc. **8**(1933)142–152.

[14] J.Eve, The evaluation of polynomials, Numer. Math. **6**(1964)17–21.

[15] M.E.Furman, Application of a method of fast multiplication of matrices to the problem of finding the transitive closure of a directed graph, Dokl. Akad. Nauk SSSR **11**(1970)1252.

[16] R.V.Jones, Reflections on Intelligence, (Heinemann, London, 1989).

[17] D.E.Littlewood, Note on the anticommuting matrices of Eddington, J. Lond. Math. Soc. **9**(1934)41–50.

[18] M.H.A.Newman, Note on an algebraic theorem of Eddington, J. Lond. Math. Soc. **7**(1932) 93–99. (Corrigendum p.272.)

[19] V.Y.Pan, New fast algorithms for matrix operations, SIAM J. Comput. **9**(1980)321–342.

[20] ———, Complexity of computations with matrices and polynomials, SIAM Review **34**(1992)225–262.

[21] R.Penrose, The Road to Reality, (Jonathan Cape, London, 2004).

[22] I.R.Porteous, Topological Geometry, (Cambridge University Press, Cambridge, 1981).

[23] J.S.Rose, A Course on Group Theory, (Cambridge University Press, Cambridge, 1978).

[24] A.Schönhage, Partial and total matrix multiplication, SIAM J. Comput. **10**(1981)434–455.

[25] J.-P.Serre, Linear Representations of Finite Groups, (Springer, New York, 1977).

[26] V.Strassen, Gaussian elimination is not optimal, Numer. Math. **13**(1969)354–356.

[27] L.G.Valiant, General context free recognition in less than cubic time, J. Computer and System Sciences **10**(1975)308–315.

[28] J.H.Wilkinson, The Algebraic Eigenvalue Problem, (Oxford University Press, London, 1965).

Notes on the theories of finite groups and their representations

James Eve

May 2, 2008

1 Introduction

The theories of finite groups and of finite group representations do not figure largely in the armoury of numerical analysts. However, this seems to be where a search for efficient algorithms for matrix operations inexorably leads. In that these imply efficient algorithms for operations well beyond the confines of computational linear algebra they may be of interest to a wider audience for which the same is true.

Initially, interest in representation theory sprang from the fact that representations mimic the properties of group elements and group algebras so such properties can be established by proving that representations possess them. Several results have subsequently been proved either initially or, in some cases, solely via representation theory. Later, theoretical physicists saw that this theory provides algebras describing physical systems; this stimulated further interest and development.

Various textbooks cover those parts of finite group theory relevant to the reading of a report on efficient algorithms for matrix operations. These parts do, however, tend to be rather submerged in other material. For representation theory, the choice of texts is very much more restricted since modern textbooks on algebra and even group theory choose to omit treatment of representation theory entirely. A colleague points out that, in the two monographs cited below, even the more elementary account of basic results in Part I of Serre[3], though concise and elegant, is a rather austere introduction.

In these circumstances, there is reason to provide an elementary informal introduction (proofs are omitted) to the concepts and results used in the report.

2 Elements of the theory of finite groups

1. If G is a nonempty finite set of *elements* on which an associative binary operation $\circ$ is defined then G is also a *group* if

(i) for $a, b \in G$, $a \circ b$ (commonly simply written ab) is in G (closure axiom),

(ii) $\exists\ 1 \in G$ such that $1 \circ g = g \circ 1 = g$ for all $g \in G$ (identity element axiom),

(iii) $\forall\ g \in G, \exists\ g^{-1} \in G$ such that $g^{-1} \circ g = g \circ g^{-1} = 1$ (inverse element axiom).

The identity and inverse elements are unique.

2. Any subset of G obeying the three axioms is a *subgroup* of G.

3. Any group G has the trivial subgroups 1 (strictly $\{1\}$) and G.

4. If $gh = hg, \forall\ h, g \in G$ then G is *abelian* or *commutative*.

5. If G has n elements then G is of *order* $|G| = n$.

6. As $|G|$ is finite g, g^2, g^3, ..., $g^{|G|+1}$ cannot all be different; there must be a least integer m in $(1, |G| + 1]$ such that $g^m = g$. But then $g^{m-1} = 1$.

The *order* of an element g is the least integer $n > 0$ such that $g^n = 1$.

7 The *exponent* of G is the least integer $n > 0$ such that $g^n = 1$, $\forall\ g \in G$.

8. If $g, g^2, g^3, \ldots, g^n = 1$ are the elements of G then G is the *cyclic group* of order n (usually denoted by C_n) and g is the *generator* of C_n.

9. If the members of a subset S of G with the binary operation suffice to construct all elements of G then the members of S are *generators* of G.

10. [2, Section 2.31] Let G and H be arbitrary groups with disjoint sets of elements. If g, g' are elements in G and h, h' are elements in H and every element of G commutes with every element of H, the *direct product group* $G \times H$ of groups G and H has elements (g, h) and (g', h') and a binary operation $(g, h)(g', h') = (gg', hh')$. The identity element is $(1, 1)$ and $(g, h)^{-1} = (g^{-1}, h^{-1})$. The definition extends to products of several groups $G_1 \times G_2 \times \ldots \times G_n$, where $(g_1, g_2, \ldots, g_n)$ is customarily written $g_1 g_2 \ldots g_n$.

11. The finite abelian groups are cyclic groups of prime power order, C_{p^r}, or direct products of such cyclic groups [2, Sections 8.26 and 8.27].

12. If H is a subgroup of G and g is in G, the set $gH = \{gh : h \in H\}$ is a *left coset* of H in G. Similarly, $Hg = \{hg : h \in H\}$ is a *right coset* of H in G.

There is an equivalence (i.e. a reflexive, symmetric and transitive) relation $\sim$ on G. For $g_1, g_2 \in G,\ g_1 \sim g_2$ if and only if $g_1 = g_2 h$ for some $h \in H$. Consequently, the left cosets of H are equivalence classes of the relation $\sim$ and partition the elements of G. Since the right cosets similarly partition G, there are as many right cosets as left cosets.

13. There is a *conjugacy* equivalence relation $\overset{*}{\sim}$ on G. For $x, y \in G$, $x \overset{*}{\sim} y$ if and only if, for some $g \in G$, $x = g^{-1} y g$ [2, Exercise 49]; it partitions G into *conjugate classes*.

14. H is a *normal* or *self conjugate* subgroup of G if $g^{-1} h g \in H, \forall\ h \in H$ and $\forall\ g \in G$. This is equivalent to $g^{-1} H g = \{g^{-1} h g : h \in H\} = H$ from which $Hg = gH$ so a normal subgroup is one whose left cosets are also right cosets [2, Section 3.2]. Accordingly, in discussing cosets of normal subgroups the left and right qualifiers are suppressed.

15. If H is a normal subgroup of G then G/H denotes the set of all cosets of H in G. With $xHyH = xyH$ defining the binary operation on the cosets, G/H becomes the *quotient group* of G by H. It is not, in general, a subgroup of G [2, Section 3.20].

16. The *centre* of G is the normal subgroup $Z_G = \{z \in G : zg = gz, \forall\ g \in G\}$ [2, Exercise 117].

17. For $h, g \in G$, $h^{-1} g^{-1} h g$ is the *commutator* of (h, g) and is 1 if and only if h and g commute. The *commutator subgroup*, denoted $[G, G]$, is the normal subgroup generated by the smallest set containing all of the commutators in G [2, Sections 3.46-3.48].

18. The commutator subgroup $[G, G]$ of a group G is the unique smallest normal subgroup of G such that $G/[G, G]$ is abelian [2, Section 3.52]. Equivalently, $G/[G, G]$ is the largest abelian quotient group of G. In fact, G/H is abelian $\Leftrightarrow$ H contains $[G, G]$.

19. A map $m : G \to H$ is a *homomorphism* or *group map* if $\forall\ a, b, c \in G$,

$ab = c \Rightarrow m(a)m(b) = m(c)$.

So a group map also respects the identity element and inverses. If the map is also a bijection then G and H are isomorphic [2, Section 2.6].

The *kernel* of the map m, $\mathrm{Ker}(m) = \{g \in G : m(g) = 1\}$, is a normal subgroup of G [2, Section 3.9].

20. The elements of a group G of order n can be permuted in $n!$ ways. The *symmetric group on the elements of* G, Σ_G, has the $n!$ arrangements of the elements of G as

its elements; the binary operation is the composition of permutations [2, Section 2.7]. (Every finite group of order n is isomorphic to a subgroup of Σ_G.)

21. [2, Sections 2.19-2.21 and exercise 117] For each $g \in G$ there is an automorphism

$$I_g : G \to G;\ h \mapsto g^{-1}hg$$

called the *inner automorphism* of G induced by g. The set of maps $\{I_g : g \in G\}$ form a group, the *group of inner automorphisms* of G, and the injective map

$$I : G \to \Sigma_G;\ g \mapsto I_g$$

has Z_G, the centre of G, as its kernel; G/Z_G is the group of inner automorphisms of G.

3 The classical theory of finite group representations

1. Unitary matrices are used to represent group elements. An n-dimensional representation ρ of a group G contains an $n\times n$ matrix $\rho(g)$ for each g in G such that

(i) for $a, b, c \in G$, if $a = bc$ then $\rho(a) = \rho(b)\rho(c)$,

(ii) $\rho(1) = 1_n$, the $n\times n$ unit matrix (so $\rho(g^{-1}) = [\rho(g)]^{-1}$).

Scalar multiples $\lambda 1_n$ of unit matrices where $\lambda \in \mathbf{C}$ occur frequently; these multiples are called *homotheties*.

2. In a one dimensional representation each group element g is represented by a value λ in $\mathbf{C}$ [3, Section 1.2(a)]. Since $g^n = 1$, for some n, λ is an nth root of unity.

3. Every group has the trivial one dimensional representation $\rho(g) = 1$ for all g in G [3, Section 1.2(a)].

4. A *monomial matrix* has precisely one nonzero element in each row and column; 1_n is monomial. If all nonzero elements in an $n\times n$ monomial matrix P are 1 then P is a *permutation matrix*: so called because $P^{-1}MP = P^{\top}MP$ permutes the rows and columns of an $n\times n$ matrix M.

The *regular representation* $\mathcal{R}$ of a group G is a $|G|$-dimensional representation containing permutation matrices.

The underlying idea is that each element g is associated with a different column $v(g)$ of $1_{|G|}$ and, for all $g_1, g_2, g_3 \in G$ such that $g_1g_2 = g_3$, the representations $\mathcal{R}(g)$ are such that $\mathcal{R}(g_1)v(g_2) = v(g_3)$. But $\mathcal{R}(g)v(1) = v(g)$, for all $g \in G$, implies that the images of $v(1)$ form a basis for a $|G|$ dimensional space and also that $g_1g_2 = g_3$ implies $\mathcal{R}(g_1)\mathcal{R}(g_2)v(1) = \mathcal{R}(g_3)v(1)$. So the regular representation has the required property $\mathcal{R}(g_1)\mathcal{R}(g_2) = \mathcal{R}(g_3)$ [3, Section 1.2(b)].

Example 1. The regular representation of C_3 contains

$$\mathcal{R}(1) = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix},\quad \mathcal{R}(g) = \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix},\quad \mathcal{R}(g^2) = \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}$$

if

$$v(1) = \begin{pmatrix} 1 \\ \\ \end{pmatrix},\qquad v(g) = \begin{pmatrix} \\ 1 \\ \end{pmatrix},\qquad v(g^2) = \begin{pmatrix} \\ \\ 1 \end{pmatrix}.$$ ■

5. The *trace* of a matrix M is $\mathrm{tr}(M) = \sum_i M_{ii}$. If ρ is the matrix representation $\{\rho(g) : g \in G\}$, the *character* χ of ρ is $\{\chi(g) = \mathrm{tr}(\rho(g)) : g \in G\}$ [3, Section 2.1].

(Replacing a matrix representation by its character is a considerable abstraction but many results in representation theory involve characters rather than representations

since general procedures for constructing matrix representations for nonabelian groups are hard to come by. Matrix representations have been constructed for relatively few nonabelian groups using group specific methods.)

6. If T is a unitary $n\times n$ matrix and ρ is n-dimensional, $\{T^{-1}\rho(g)T : g \in G\}$ is also an n-dimensional representation. The trace of a matrix product is invariant under cyclic permutation of the matrices in the product; this property of the trace function is used repeatedly in representation theory. Here, since $\mathrm{tr}(T^{-1}\rho(g)T) = \mathrm{tr}(TT^{-1}\rho(g)) = \mathrm{tr}(\rho(g))$, it shows that representations derived from ρ in this way all have the same character.

7. There is an equivalence relation on representations reminiscent of the conjugacy relation on group elements. Representations U and V are *similar* or *isomorphic* if, for some unitary T, $V = \{T^{-1}U(g)T : g \in G\}$. The equivalence classes of representations so produced all have the same character. Hence the name *character*; two $n\times n$ representations are *distinct* or *non-isomorphic* when their characters differ.

8. [3, Section 1.4] An $n\times n$ representation ρ is *reducible* if there exists a unitary matrix T such that $\{T^{-1}\rho(g)T : g \in G\}$ contains block diagonal matrices with the same block diagonal structure. In this event, a single n-dimensional representation is reduced to a set of matrix representations with smaller dimensions.

A representation is *irreducible* if no such matrix T exists.

9. An abelian group G has $|G|$ (necessarily irreducible) one dimensional representations [3, Theorem 9]. A nonabelian group has at least one irreducible representation ρ of dimension $d_\rho \geq 2$ [3, Section 1.4].

10. Irreducible representations have certain benefits (see 11 below) but again there are no general methods of construction. However, the number of distinct irreducible representations and their dimensions are related to other group properties.

(i) The number of distinct irreducible representations of a group is equal to the number of its conjugate classes [3, Theorem 7].

(ii) If G has distinct irreducible representations ρ_i of dimension d_{ρ_i}, where $1 \leq i \leq n$, then $|G| = \sum_{i=1}^{n} d_{\rho_i}^2$ [3, Proposition 5, Corollary 2(a)].

If the requisite number of representations can be acquired, their characters are distinct and the sum of the squares of their dimensions is equal to the order of the group then this is a complete set of irreducible representations [3, Proposition 5, Remark 1].

11. The regular representation is known to be reducible to irreducible block diagonal form in which each distinct d_ρ-dimensional irreducible representation ρ occurs d_ρ times [3, Proposition 5, Corollary 1].

This result is fundamentally responsible for a Fourier transform algorithm that uses the irreducible representations to multiply elements of a group algebra.

Example 2. Consider the regular representation of C_3 in Example 1. If $\omega^3 = 1$ and

$$T\sqrt{3} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \text{ then } T^{-1}\sqrt{3} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix}$$

so T is unitary and

$$T^{-1}\mathcal{R}(1)T = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \quad T^{-1}\mathcal{R}(g)T = \begin{pmatrix} 1 & & \\ & \omega^2 & \\ & & \omega \end{pmatrix}, \quad T^{-1}\mathcal{R}(g^2)T = \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix}$$

show that T reduces the regular representation to the three one dimensional representations of $1,\ g,\ g^2$, namely, $1,\ 1,\ 1$ followed by $1,\ \omega^2,\ \omega$ followed by $1,\ \omega,\ \omega^2$. ∎

12. [3, Section 2.2] Schur's Lemma implies, *inter alia*, that only homotheties commute with every matrix in an irreducible representation (so elements in the centre must be represented by them). The primary use of Schur's Lemma is in establishing the so called orthogonality relations of the irreducible matrix representations.

If ρ and ξ are distinct irreducible representations of dimension d_ρ and d_ξ the orthogonality relations (on elements of matrices in the representations) state

(i) $\sum_{g\in G} \rho_{ms}(g)\rho_{li}(g^{-1}) = |G|d_\rho^{-1}\delta_{ls}\delta_{mi}$, for all $m, s, l, i \in [0, d_\rho)$,
where $\delta_{xy} = 1$ if $x = y$ and $\delta_{xy} = 0$ if $x \neq y$,

(ii) $\sum_{g\in G} \rho_{ms}(g)\xi_{li}(g^{-1}) = 0$, for all $m, s \in [0, d_\rho)$ and all $l, i \in [0, d_\xi)$.

(There are corresponding orthogonality relations for the characters [3, Section 2.3].)

13. Tensor products of matrices are used in forming matrix representations: for example, in constructing representations of $G \times H$ from representations of G and H.

The *tensor product*, $U \otimes V$, of a $u\times u$ matrix U and a $v\times v$ matrix V, is a $uv\times uv$ matrix with elements $(U\otimes V)_{(u_1,v_1)(u_2,v_2)} = U_{u_1u_2}V_{v_1v_2}$.

Using ordered pairs to label rows and columns leaves a degree of arbitrariness in the actual order of rows and columns. It can be resolved by imposing any convenient ordering on the ordered pairs. For example, the order of rows and columns of $U\otimes V$ can be arranged so that $UV_{v_1v_2}$ is the (v_1, v_2) $u\times u$ submatrix of $U\otimes V$. This merely requires that (u_i, v_i) precedes (u_j, v_j) if $v_i < v_j$ or, when $v_i = v_j$, if $u_i < u_j$.

References

[1] C.W.Curtis and I.R.Reiner, Representation Theory of Finite Groups and Associative Algebras (Interscience, New York, 1962).

[2] J.S.Rose, A Course on Group Theory, (Cambridge University Press, Cambridge, 1978).

[3] J.-P.Serre, Linear Representations of Finite Groups, (Springer, New York, 1977).

A Note by Donald Knuth

Donald E. Knuth
Stanford University

December 2008

Dear Jim,

I ran into a problem understanding your algorithm, so I need your help before I can go further. In this note I'll try to explain exactly where I'm stymied. I shall stick only to the simple case $p = 3$ and $s = 1$ of Proposition 4.10 in your draft of August 25; thus we want to square a 3×3 matrix $M = (m_{ij})$, where the subscripts i and j run through the set $\{0, 1, 2\}$.

Let ω be a primitive cube root of unity, so that $\omega^2 = \bar\omega$ and $1 + \omega + \bar\omega = 0$.

First we express M as a linear combination $\sum_{i,j} z_{i,j} G_{i,j}$, where you have defined nine interesting matrices $G_{ij} = \omega^{ij} X^i (\bar\omega Y)^j$:

$$G_{00} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad G_{01} = \begin{pmatrix} \bar\omega & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix} \quad G_{02} = \begin{pmatrix} \omega & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \bar\omega \end{pmatrix}$$
$$G_{10} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad G_{11} = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & \bar\omega \\ 1 & 0 & 0 \end{pmatrix} \quad G_{12} = \begin{pmatrix} 0 & \bar\omega & 0 \\ 0 & 0 & \omega \\ 1 & 0 & 0 \end{pmatrix}$$
$$G_{20} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad G_{21} = \begin{pmatrix} 0 & 0 & 1 \\ \omega & 0 & 0 \\ 0 & \bar\omega & 0 \end{pmatrix} \quad G_{22} = \begin{pmatrix} 0 & 0 & 1 \\ \bar\omega & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}$$

(Indeed, you have a nice transform that efficiently takes any $3^s \times 3^s$ matrix into a linear combination of 3^{2s} similar G-matrices, for arbitrary s, and back again; hence the general squaring problem is reduced to finding an efficient way to find the square of such a linear combination, as another linear combination of those matrices.)

To square this, you do a discrete Fourier transform of the coefficients z_{ij}, which I shall denote by $Z_{st} = \sum_{i,j} \omega^{is+jt} z_{ij}$. Then you square the transformed coefficients, getting $Z'_{st} = Z_{st}^2$, and untransform to get new coefficients, z'_{ij}. Supposedly we now have $(\sum_{i,j} z_{ij} G_{ij})^2 = \sum_{i,j} z'_{ij} G_{ij}$.

But here's where there either is a mistake or I have gravely misunderstood what you said. For if the original matrix M happens to be, say, $G_{01} + G_{10}$, we get $Z_{st} = \omega^s + \omega^t$, hence $Z'_{st} = \omega^{2s} + 2\omega^{s+t} + \omega^{2t}$, hence $z'_{ij} = \delta_{i2}\delta_{j0} + 2\delta_{i1}\delta_{j1} + \delta_{i0}\delta_{j2}$; you are claiming that $(G_{01} + G_{10})^2 = G_{02} + 2G_{11} + G_{20}$. But in fact, the square is $G_{02} - G_{11} + G_{20}$.

You note correctly that $G_{ij} G_{i'j'} = \omega^{i'j - ij'} G_{(i+i')(j+j')}$, hence the product is one of the G's if and only if G_{ij} commutes with $G_{i'j'}$. And you note that a matrix commutes with its square. But I fail to see why this implies the validity of a commutative-algebra convolution method to compute the square.

As far as I can see, a new kind of "skewed" convolution is needed, instead of the Z_{st} you have used, if we want to square linear combinations of the G matrices efficiently. Perhaps such a convolution exists, but I haven't been able to come up with one.

Best wishes, Don

Jim Eve

An Address given at the Celebration of Dr Jim Eve's life,
Saltwell, Gateshead, 9 March 2009, by Brian Randell

I have known Jim, as a University colleague and close friend, for forty years. But Jim's association with Newcastle University goes back much further. After obtaining an Honours Degree in Physics here in 1954, and then a Ph.D in Theoretical Physics, he was appointed in 1957 as a Research Assistant in the newly-created Computing Laboratory, so bringing its staff complement up to a full half dozen. (It had been set up both to provide a computing service to the University, and to undertake teaching and research in Computing Science.)

Completing this bald summary of Jim's career at Newcastle, in 1960 he was appointed to a Lectureship, and in 1968 to a Senior Lectureship, a post he held with distinction until he retired in 1996.

Two very important years in Jim's life, or rather in Jim and Margaret's lives, were sabbatical years spent in the United States. The first was in 1966-67 at Carnegie-Mellon University. The second was during 1974-75, which he spent partly at another very prestigious CS Department, namely Stanford University, and partly as a Visiting Scientist at the nearby and now legendary Xerox Palo Alto Research Centre, source of so many revolutionary computer developments.

During these two sabbaticals Jim gained the great respect, and he and Margaret the continuing friendship, of a number of eminent computer scientists, including Professor Al Perlis at Carnegie, and Professors Don Knuth and Bob Floyd at Stanford. (I'll return to Bob Floyd in a moment.)

But much earlier there had been two particularly important weeks in his life at Newcastle. Jim was organizing the first computerized registration of students in the University, when he received a visit from the young lady who headed up the admissions office in the Registrar's department.

They had never met before – she had arrived in Newcastle only a week earlier and was the University's only female administrator. Jim acted with a speed and decisiveness that astonished his colleagues, and by the end of those two weeks he and Margaret were engaged. The rest, as they say, is history.

I first got to know Jim when I arrived here from the States in 1969, fresh from the IBM Research Lab – Liz and I will always be grateful for Jim and Margaret's welcome, and for their help with the culture shock they knew we would be suffering.

Jim's research had mainly been on syntax analysis, complexity theory and computer typesetting. (He participated in what was in fact the world's first computer-typesetting project.) However, shortly after I arrived, I received a letter from the Science Research Council, asking why Newcastle had not sought any research funding from them.

I took this letter with me to coffee. By lunchtime Jim and I had planned a large SRC-funded research project on system dependability. Thus started a still-continuing and still-growing programme of system dependability research, a programme of which Newcastle can be justly proud.

For a while Jim was actively involved in this research, and he and I went on a fact-finding trip together to the States. At Stanford University we met Bob Floyd. Subsequently Jim and I often recalled how Bob, when asked how he chose which research topics to work on, replied: "I try to identify some really critical and challenging questions, and then choose one that I don't think anyone else can answer".

This incident may partly explain why Jim took up complexity theory again, and an immensely significant and highly mathematical problem. This became what some might call his continuing obsession (I prefer the term hobby), one that he remained actively engaged in even after he became ill last year.

Over the years, Jim made tremendous progress, though to everyone's regret he did not live to complete the project – our aim now is to see that his work is taken up and brought to a successful conclusion. Meanwhile, the quotation* in your programme from Marcus du Sautoy, Professor of Mathematics at Oxford, might help you gain some understanding of what was driving Jim, and what fulfillment he was getting from his work.

I sought help from several colleagues whilst composing this brief tribute – time does not permit my using much of the material they kindly sent me, but here is one typical quote, from Roy Maxion of Carnegie-Mellon University: "Jim was a delight in so many ways – his keen intellect, his fine sense of humor, his high integrity, his deep warmth and friendliness, and his most excellent judgment in all things, including having chosen Margaret as a life partner". (Another friend Jim first met at CMU, Hugh Lauer, has in fact come over from the States especially for this occasion.)

I'll end with one further quote, from John Rushby, now a leading international expert on formal methods: "It was Jim's lectures on automata and formal languages

---

* *Looking back over the year the problem I have been working on ended up getting more complicated than it was 12 months ago. It will make the final resolution, if it come, more gratifying. What's the satisfaction in solving easy problems? I'm still not even sure what the final answer will be. In mathematics the real prize is not a medal or invitation to the International Congress of Mathematicians but making the breakthrough on the problem to which you've dedicated your life.*

From "Finding Moonshine. A Mathematician's Journey Through Symmetry"
Marcus du Sautoy, 2008.

that first revealed to me that computer science is about more than just techniques of computation – it has its own topics of intrinsic interest and beauty. I don't think it's an exaggeration to say that it changed the course of my life."

Jim, I'm sure, changed many lives – so his own can be truly celebrated.