Group-Theoretic Methods for bounding the exponent of matrix Multiplication

MSc Thesis (*Afstudeerscriptie*)

written by

Sandeep R. Murthy
(born April 4th, 1977 in Hyderabad, India)

under the supervision of **T.H. Koornwinder**, and submitted to the Board of Examiners in partial fulfillment of the requirements for the degree of

MSc in Logic

at the *Universiteit van Amsterdam*.

Date of the public defense:	**Members of the Thesis Committee:**
21st August, 2007	Dick de Jongh
	T.H. Koornwinder
	R. van der Waall
	Peter van Emde Boas

Institute for Logic, Language and Computation

Contents

Acknowledgements

This thesis was completed under the kind supervision of Prof. Tom Koornwinder of the Korteweg de Vries (KdV) Institute for Mathematics.

The author also acknowledges the help of Prof. Peter van Emde Boas of the ILLC in relation to Chapter 2 dealing with the algebraic theory of complexity of matrix multiplication, and of Prof. R. van der Waal of the KdV Institute in relation to Chapter 3 dealing with the representation theory of finite groups.

Acknowledgements are also due to the coauthors of the papers on which the thesis is based, Dr. Chris Umans (Dept. of Computer Science, California Institute of Technology), and Dr. Henry Cohn (Microsoft Research), for some clarifying remarks and comments.

Chapter 1

Introduction

1.1 The Exponent ω of Matrix Multiplication

Matrix multiplication is a fundamental operation in linear algebra. For any given field K, the (asymptotic) complexity of matrix multiplication over K is measured by a real parameter $\omega(K) > 0$, called the *exponent of matrix multiplication* over K, which is defined to be the smallest real number $\omega > 0$ such that for an arbitrary degree of precision $\epsilon > 0$, two $n \times n$ K-matrices can be multiplied using an algorithm using $O(n^{\omega+\epsilon})$ number of non-division arithmetical operations, i.e. less than some constant ≥ 1 multiple of $n^{\omega+\epsilon}$ number of multiplications, additions or subtractions. The notation $\omega(K)$ indicates a dependency on the ground field K, but we usually have in mind the complex field $K = \mathbb{C}$, which is general enough for most purposes. It is proved that ω determines the complexities of many other linear operations, e.g. matrix inversion, determinants, etc., and these are concisely covered by Bürgisser et. al., *Chapter 16* in [BCS1997].

If we denote by $M_K(n)$ the total number of arithmetical operations for performing $n \times n$ matrix multiplication over a field K, then by the standard algorithm, $M_K(n) = 2n^3 - n^2 = O(n^3)$, because one needs to perform n^3 multiplications, and $n^3 - n^2$ additions of the resulting products. This is equivalent to an upper bound of 3 for ω. Since the product of two $n \times n$ matrices consists of n^2 entries, one needs to perform a total number of operations which is *at least* some constant ≥ 1 multiple of the n^2 entries. This is written as $M_K(n) = \Omega(n^2)$, which

is equivalent to a lower bound of 2 for ω. Strassen in 1969 obtained the first important result that $\omega < 2.81$ using his result that 2×2 matrix multiplication could be performed using 7 multiplications, not 8, as in the standard algorithm [STR1969, p. 355]. In 1984, Pan improved this to 2.67, using a variant of Strassen's approach [PAN1984, p. 400]. It has been conjectured for twenty years that $\omega = 2$, but the best known result is that $\omega < 2.38$, due to Coppersmith and Winograd [CW1990, p. 251]. In all these approaches, estimates for ω depend on the number of main running steps in their algorithms.

1.2 Groups and Matrix Multiplication

In a recent series of papers in 2003 and 2005, Cohn and Umans put forward an entirely different approach using fairly elementary methods from group theory to describe the complexity of matrix multiplication.

The approach is based on two important facts.

1.2.1 *Realizing Matrix Multiplications via Finite Groups*

(I) A (nontrivial) finite group G which has a triple of index subsets S, T, $U \subseteq G$ of sizes $|S| = n$, $|T| = m$, $|U| = p$, such that $s^{'}s^{-1}t^{'}t^{-1}u^{'}u^{-1} = 1_G \Longleftrightarrow s^{'}s^{-1} = t^{'}t^{-1} = u^{'}u^{-1} = 1_G$, for all elements $s^{'}, s \in S$, $t^{'}, t \in T$, $u^{'}, u \in U$, *realizes* multiplication of $n \times m$ by $m \times p$ matrices over $\mathbb{C}$, in the sense that the entries of a given $n \times m$ complex matrix $A = (A_{i,j})$ and an $m \times p$ matrix $B = (B_{k,l})$, can be indexed by the subsets S, T, U as $A = (A_{s,t})_{s \epsilon S, t \epsilon T}$ and $B = \left(B_{t',u}\right)_{t' \epsilon T, u \, \epsilon U}$, then injectively embedded in the regular group algebra $\mathbb{C}G$ of G as the elements $\overline{A} = \sum_{s \, \epsilon \, S, \, t \, \epsilon \, T} A_{s,t}s^{-1}t$ and $\overline{B} = \sum_{t' \, \epsilon \, T, \, u \, \epsilon \, U} B_{t',u}t^{'-1}u$, and the matrix product AB can be computed by the rule that the $s^{''}, u^{''}$-th entry $(AB)_{s^{''},u^{''}}$ is the coefficient of the term $s^{''-1}u^{''}$ in the group algebra product $\overline{AB} = \sum_{s \, \epsilon \, S, \, t \, \epsilon \, T} \sum_{t' \, \epsilon \, T, \, u \, \epsilon \, U} A_{s,t}B_{t',u}s^{-1}tt^{'-1}u$ (see *Theorem 4.13*). In this case, by definition, G is said to support $n \times m$ by $m \times p$ matrix multiplication, equivalently, to *realize* the matrix tensor $\langle n, m, p \rangle$, whose size we define as nmp, and the subsets S, T, U

are said to have the *triple product property* (TPP) and be an *index triple* of G corresponding to the tensor $\langle n, m, p \rangle$ (see *Chapter 4*).

1.2.2 *Wedderburn's Theorem*

(II) By Wedderburn's theorem there is an isomorphism $\mathbb{C}G \cong \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathbb{C}^{d_\varrho \times d_\varrho}$ of the regular group algebra $\mathbb{C}G$ of G, where $\bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathbb{C}^{d_\varrho \times d_\varrho}$ is a block-diagonal matrix algebra of dimension $\sum_{\varrho \,\epsilon\, Irrep(G)} d_\varrho^2 = |G|$, and the $\mathbb{C}^{d_\varrho \times d_\varrho}$ are its irreducible subalgebras of dimensions d_ϱ^2, and the d_ϱ are the degrees of the distinct irreducible characters of G, i.e. the dimensions $d_\varrho = Dim\ \varrho$ of the distinct (inequivalent) irreducible representations $\varrho \,\epsilon\, Irrep(G)$ of G. Any such isomorphism constitutes a group discrete Fourier transform (DFT) for G, and, further, we can deduce that $|G| \leq \mathfrak{R}(\mathfrak{m}_{\mathbb{C}G}) \leq \sum_{\varrho \,\epsilon\, Irrep(G)} \mathfrak{R}\left(\langle d_\varrho, d_\varrho, d_\varrho \rangle\right)$, where $\mathfrak{R}(\mathfrak{m}_{\mathbb{C}G})$ and $\mathfrak{R}\left(\langle d_\varrho, d_\varrho, d_\varrho \rangle\right)$ are the ranks of the bilinear multiplication maps $\mathfrak{m}_{\mathbb{C}G}$ and $\langle d_\varrho, d_\varrho, d_\varrho \rangle$ in $\mathbb{C}G$ and $\mathbb{C}^{d_\varrho \times d_\varrho}$, respectively.

1.2.3 *A Group-theoretic DFT Algorithm for Matrix Multiplication*

This suggests the following group-theoretic DFT algorithm for $n \times n$ matrix multiplication via a finite group G realizing $n \times n$ matrix multiplication via subsets S, T, $U \subseteq G$ having the triple product property.

1. Injectively embed $n \times n$ complex matrices $A = (A_{i,j})_{1 \leqslant i,j \leqslant n}$ and $B = \left(B_{j',k}\right)_{1 \leqslant j',k \leqslant n}$ into $\mathbb{C}G$ as elements $\overline{A} = \sum_{s \,\epsilon\, S,\ t \,\epsilon\, T} A_{s,t} s^{-1} t$ and $\overline{B} = \sum_{t' \,\epsilon\, T,\ u \,\epsilon\, U} B_{t',u} t'^{-1} u$ via S, T, U (as described in (I)).

2. Use a discrete group Fourier transform (DFT) for G, $DFT : \mathbb{C}G \cong \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathbb{C}^{d_\varrho \times d_\varrho}$ to compute the transforms $\widehat{A} = DFT(\overline{A})$ and $\widehat{B} = DFT(\overline{B})$.

3. Compute the block-diagonal matrix product of transforms, $\widehat{C} = \widehat{A}\widehat{B}$.

4. Recover the vector $\overline{AB} = \overline{C} = DFT^{-1}\left(\widehat{C}\right)$ from its transform by the inverse group DFT.

5. Fill the matrix AB from $\overline{AB} = \sum_{s \,\epsilon\, S,\, t \,\epsilon\, T} \sum_{t' \,\epsilon\, T,\, u \,\epsilon\, U} A_{s,t} B_{t',u} s^{-1} t t'^{-1} u$ by the rule that for each $s'' \,\epsilon\, S$, $u'' \,\epsilon\, U$, the s'', u''-th entry $(AB)_{s'',u''} =$ coefficient $\sum_{t,\, t' \,\epsilon\, T} A_{s,t} B_{t',u}$ of the term $s^{-1} t t'^{-1} u$ in $\overline{AB}$ for which $s = s''$, $t = t'$, $u = u''$.

1.2.4 *The Complexity of Matrix Multiplications Realized by Groups*

In the approach we describe, estimates for ω can be derived from certain numerical parameters relating to the efficiency with which groups realize matrix multiplications, and also to the degrees of their irreducible characters.

(1) *Pseudoexponents* $\alpha(G)$, defined by $\alpha(G) := \log_{z'(G)^{1/3}} |G|$, where $\left\langle n', m', p' \right\rangle$ is a matrix tensor of maximal size $z'(G) = n'm'p' > 1$ realized by G, and uniquely determining $\alpha(G)$. We prove that $|G| \leq z'(G) < |G|^{\frac{3}{2}}$, which is equivalent to $2 < \alpha(G) \leq 3$, and that $\alpha(G) = 3$ whenever G is Abelian. The $\alpha(G)$ are measures of the efficiency with which the groups G realize or embed matrix multiplication, and the closer $\alpha(G)$ is to 2 the higher the embedding efficiency (section *4.2.1*).

(2) *Parameters* $\gamma(G)$, defined by $\gamma(G) := \inf_{\gamma > 0} |G|^{\frac{1}{\gamma}} = d'(G)$, where $d'(G)$ is any maximal irreducible character degree of G, for which we can easily prove that $2 < 2\frac{\log|G|}{\log(|G|-1)} \leq \gamma(G) \leq 2\frac{\log|G|}{\log(|G|-c(G))}$, where $c(G)$ is the class number of G, and that $2 < 2\frac{\log|G|}{\log(|G|-1)} < \gamma(G) < 2\frac{\log|G|}{\log(|G|-c(G))}$, iff G is non-Abelian ((section *4.2.2*))

(3) Sums of powers of irreducible character degrees, $D_r(G) = \sum_{\varrho \,\epsilon\, Irrep(G)} d_\varrho^r$, $r \geq 0$. Facts from representation theory are that $D_0(G) = c(G)$, and $D_2(G) = |G|$ (section *3.2.*).

1.2.5 *Relations and Results for the Exponent* ω

The four most important relations which we prove using single groups G are the following.

(1.1) $\quad |G|^{\frac{\omega}{\alpha(G)}} \leqslant D_{\omega}(G)$	this is equivalent to $2 \leqslant \omega \leqslant \alpha(G) \log_{|G|} D_{\omega}(G)$
(1.2) $\quad D_r(G) \leq |G|^{\frac{(r-2)}{\gamma(G)}+1}$	real $r \geq 2$
(1.3) $\quad (nmp)^{\frac{1}{3}} \leq d^{'}(G)^{1-\frac{2}{\omega}} \, |G|^{\frac{1}{\omega}}$	if G realizes a tensor $\langle n, m, p \rangle$
(1.4) $\quad \omega \leq \alpha(G) \left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)} \right)$	if $\alpha(G) < \gamma(G)$

By applying these relations, we have also been able to derive a number of results about how to prove estimates for ω using non-Abelian groups. These are listed below.

Proposition 1.1 *$\omega \leq t < 3$ for some $t > 2$, if there is a non-Abelian finite group G with pseudoexponent $\alpha(G)$ and parameter $\gamma(G)$ such that $\alpha(G) < \gamma(G)$ and $\alpha(G) \left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)} \right) \leq t$. An equivalent, but more precise statement is that $\omega \leq t < 3$, for some $t > 2$, if there is a non-Abelian finite group G realizing matrix multiplication of maximal size $z^{'}(G)$ and with a maximal irreducible character degree $d^{'}(G)$ such that $z^{'}(G)^{\frac{1}{3}} > d^{'}(G)$ and $|G| \leq \frac{z^{'}(G)^{\frac{t}{3}}}{d^{'}(G)^{(t-2)}}$. (Corollary 4.28)*

Proposition 1.2 *If $\{G_k\}$ is a family of non-Abelian groups such that $\alpha(G_k) \equiv \alpha_k = 2 + o(1)$, and $\gamma(G_k) \equiv \gamma_k = 2 + o(1)$, and $\alpha_k - 2 = o(\gamma_k - 2)$, as $k \longrightarrow \infty$, then $\omega = 2$. (Corollary 4.29)*

Proposition 1.3 *Let $\{G_k\}$ be a family of non-Abelian groups G_k realizing matrix multiplications of largest sizes $z_k^{'} \equiv z^{'}(G_k)$ and with largest irreducible character degrees $d_k^{'} \equiv d_k^{'}(G)$. Then, (1) $\omega = 2$ if $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$ and $(|G_k| - 1)^{\frac{1}{2}} - d_k^{'} = o(1)$ such that $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o\left((|G_k| - 1)^{\frac{1}{2}} - d_k^{'} \right)$ as $k \longrightarrow \infty$. And more generally, (2) $\omega = 2$ if $|G_k| \longrightarrow \infty$ as $k \longrightarrow \infty$ and there exists a sequence $\{C_k\}$ of constants C_k for the G_k such that $2 \leq C_k \leq |G_k| - 1$, $|G_k| \geq C_k \left(1 + \frac{1}{C_k - 1} \right)$, $C_k \longrightarrow \infty$, $C_k = o(|G_k|)$, $(|G_k| - C_k)^{\frac{1}{2}} - d_k^{'} = o(1)$, $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$ and $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o\left((|G_k| - C_k)^{\frac{1}{2}} - d_k^{'} \right)$, as $k \longrightarrow \infty$. (Theorem 4.30)*

1.2.6 *Realizing Simultaneous, Independent Matrix Multiplications via Groups*

In *Chapter 5*, we introduce a more general concept of *simultaneous triple product property* (STPP) (also due to Cohn and Umans, [CUKS2005]). To be more precise, a collection

$\{(S_i, T_i, U_i)\}_{i\,\epsilon\,I}$ of triples (S_i, T_i, U_i) of subsets $S_i, T_i, U_i \subseteq G$, of sizes $|S_i| = m_i$, $|T_i| = p_i$, $|U_i| = q_i$ respectively, is said to satisfy the *simultaneous triple product property* (STPP) iff it is the case that each triple (S_i, T_i, U_i) satisfies the TPP and $s_i' s_j^{-1} t_j' t_k^{-1} u_k' u_i^{-1} = 1_G \Longrightarrow i = j = k$, for all $s_i' s_j^{-1} \,\epsilon\, Q(S_i, S_j)$, $t_j' t_k^{-1} \,\epsilon\, Q(T_j, T_k)$, $u_k' u_i^{-1} \,\epsilon\, Q(U_k, U_i)$, $i, j, k \,\epsilon\, I$. In this case, G is said to *simultaneously realize* the corresponding collection $\{\langle m_i, p_i, q_i\rangle\}_{i\,\epsilon\,I}$ of tensors through a corresponding collection $\{(S_i, T_i, U_i)\}_{i\,\epsilon\,I}$, which is called a *collection of simultaneous index triples*. The importance of STPP is that it describes how a finite group may realize several independent matrix multiplications simultaneously such that the total complexity of these several matrix multiplications cannot exceed the complexity of one multiplication in its regular group algebra. The first set of important results about ω relating to the STPP are summarised by the following proposition.

Proposition 1.4 *If $\{\langle m_i, p_i, q_i\rangle\}_{i=1}^{r}$ is a collection of r tensors simultaneously realized by a group G then*

$$(1) \sum_{i=1}^{r} (m_i p_i q_i)^{\frac{\omega}{3}} \leq D_\omega(G) \qquad \textit{(part (1) of Corollary 5.2)}$$

and if these tensors are all identical, say, $\langle m_i, p_i, q_i\rangle = \langle n, n, n\rangle$, for all $1 \leq i \leq r$, then

$$(2)\ \omega \leq \frac{\log |G| - \log r}{\log n}. \qquad \textit{(Corollary 5.3)}$$

The most useful types of groups for estimates for ω using the STPP seem to be wreath product groups $H \wr Sym_n$, for which we prove that $D_\omega(H \wr Sym_n) \leq (n!)^{\omega-1} |H|^n$ (*Lemma 5.7*). Using the latter result, the most general result which we've obtained (*Proposition 5.10*) in this regard involves the wreath product groups $H \wr Sym_n$ where H is Abelian.

Proposition 1.5 *For any n triples $S_i, T_i, U_i \subseteq H$ of sizes $|S_i| = m_i, |T_i| = p_i, |U_i| = q_i$, $1 \leq i \leq n$ satisfy the STPP in an Abelian group H, there is a unique number $1 \leq k_n \leq (n!)^3$ of triples of permutations, $\sigma_j, \tau_j, \upsilon_j \,\epsilon\, Sym_n$, $1 \leq j \leq k_n$, such that the k_n permuted product triples $\prod_{i=1}^{n} S_{\sigma_j(i)} \wr Sym_n$, $\prod_{i=1}^{n} T_{\tau_j(i)} \wr Sym_n$, $\prod_{i=1}^{n} U_{\upsilon_j(i)} \wr Sym_n$, $1 \leq j \leq k_n$, satisfy the STPP in $H \wr Sym_n$,*

and such that $H \wr Sym_n$ *realizes the square product tensor* $\left\langle n! \prod_{i=1}^{n} m_i, n! \prod_{i=1}^{n} p_i, n! \prod_{i=1}^{n} q_i \right\rangle$ k_n *times simultaneously, such that*

$$\omega \leq \frac{n \log |H| - \log n! - \log k_n}{\log \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i}}.$$

1.2.7 *Estimates for the Exponent* ω

In *Chapter 6*, we give several estimates for ω using Abelian groups H or wreath products involving them, $H \wr Sym_n$.

$\omega <$	*Group*	*Reference*
2.93	$Cyc_{41}^{\times 3} \wr Sym_2$	section *6.2.2*
2.82	$\left(Cyc_m^{\times 3}\right)^{\times m} \wr Sym_{2^m}$	section *6.2.3*
2.82	$Cyc_{16}^{\times 3}$	section *6.2.1*

We conclude with the observation that $\left(Cyc_n^{\times 3}\right)^{\times n} \wr Sym_{2^n}$ (i.e. $\left(\left(Cyc_n^{\times 3}\right)^{\times n}\right)^{\times 2^n} \rtimes Sym_{2^n}$) realizes the product tensor $\left\langle 2^n! \left(n-1\right)^{n2^n}, 2^n! \left(n-1\right)^{n2^n}, 2^n! \left(n-1\right)^{n2^n} \right\rangle$ some $1 \leq k_{2^n} \leq \left(2^n!\right)^3$ times simultaneously such that

$$\omega \leq \frac{2^n \log n^{3n} - \log 2^n! - \log k_{2^n}}{2^n n \log\left(n-1\right)}.$$

For example, if $k_{2^n} = \left(2^n!\right)^3$ then $\omega \leq \frac{2^n \log n^{3n} - 4 \log 2^n!}{2^n n \log(n-1)}$, the latter achieving a minimum of 2.012 for $n = 6$. In general, for the groups $\left(Cyc_n^{\times 3}\right)^{\times n} \wr Sym_{2^n}$ the closer k_{2^n} is to $\left(2^n!\right)^3$, the closer ω is to 2.012 (from the upper side).

It is one of the original suggestions in the thesis that given an Abelian group H with a given STPP family $\{(S_i, T_i, U_i)\}_{i=1}^{n}$ it is therefore useful to know the how to choose triples of permutations $\sigma_j, \tau_j, \upsilon_j \in Sym_n$ in order that a maximum number $1 \leq k_n \leq (n!)^3$ of triples $\prod_{i=1}^{n} S_{\sigma_j(i)} \wr Sym_n, \prod_{i=1}^{n} T_{\tau_j(i)} \wr Sym_n, \prod_{i=1}^{n} U_{\upsilon_j(i)} \wr Sym_n$, $1 \leq j \leq k_n$, satisfy the STPP in $H \wr Sym_n$. Using such groups and their triples in this way, the sharpest upper bounds for ω will occur where the ratio $k_n / \left(n!\right)^3$ is highest.

Chapter 2

Algebraic Complexity of Matrix Multiplication

In section *2.1* we describe matrix multiplication as a bilinear map describing multiplication in matrix algebras, and introduce a certain measure of the complexity of matrix multiplication defined in terms of the concept of rank of bilinear map. Then, in section *2.2* we introduce the exponent ω as an asymptotic, real-valued measure of complexity, and conclude by describing the fundamental relations between the bilinear and the asymptotic measures.

2.1 Bilinear Complexity of Matrix Multiplication

2.1.1 *Matrix Multiplication as a Bilinear Map*

If U and V are two K-spaces of dimensions n and m, respectively, with bases $\{u_i\}_{1\leq i\leq n}$ and $\{v_j\}_{1\leq j\leq m}$ respectively, then for any third space W, a map $\phi : U \times V \longrightarrow W$ which satisfies the condition

$$\begin{aligned} & \phi\left(\kappa_1 u_1 + \kappa_2 v_1, \kappa_3 u_2 + \kappa_4 v_2\right) \\ = \; & \kappa_1\kappa_3\phi\left(u_1, u_2\right) + \kappa_1\kappa_4\phi\left(u_1, v_2\right) + \kappa_2\kappa_3\phi\left(v_1, u_2\right) + \kappa_2\kappa_4\phi\left(v_1, v_2\right) \end{aligned}$$

for all scalars $\kappa_1, \kappa_2, \kappa_3, \kappa_4 \in K$ and vectors $u_1, u_2 \in U$, $v_1, v_2 \in V$, is called a *K-bilinear map*, or simply, a *bilinear map*, on U and V. The map $K^{n\times m} \times K^{m\times p} \longrightarrow K^{n\times p}$ describing multiplication of $n \times m$ by $m \times p$ matrices over K is such a bilinear map, which we denote by $\langle n, m, p\rangle_K$. We call the integers n, m, p the *components* of the map $\langle n, m, p\rangle$, which is also called a tensor, ([BCS1997, p. 361].

For a K-space U, the set of all linear forms (functionals) $f : U \longrightarrow K$ on U, i.e linear maps of U into its ground field, forms a K-space U^*, equidimensional with U, called its *dual space*. The matrix vector space $K^{n\times m}$ has the basis $\{E_{ij}\}_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$, where E_{ij} is the $n \times m$ matrix with a 1 in its $(i, j)^{th}$ entry and a 0 everywhere else, and the dual space $K^{n\times m^*}$ has the dual basis $\left\{e^*_{ij}\right\}_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$ where e^*_{ij} is a map $K^{n\times m} \longrightarrow K$ which sends any $n \times m$ matrix A over K to its $(i, j)^{th}$ entry $(A)_{ij}$. We denote the zero $n \times m$ matrix of $K^{n\times m}$ by $\mathbf{O}_{n\times m}$.

2.1.2 *Rank of Matrix Multiplication*

The set $Bil_K(U, V; W)$ of all bilinear maps on two K-spaces U and V into a third space W also forms a K-space, e.g. $\langle n, m, p\rangle_K \in Bil_K(K^{n\times m}, K^{m\times p}; K^{n\times p})$. If $U = V = W$, we write $Bil_K(U)$ for $Bil_K(U, V; W)$. For any $\phi \in Bil_K(U, V; W)$, there is a smallest positive integer r such that for every pair $(u, v) \in U \times V$, $\phi(u, v)$ has the bilinear representation

$$\phi(u, v) = \sum_{i=1}^{r} f_i^*(u)\, g_i^*(v)\, w_i$$

where $f_i^* \in U^*, g_i^* \in V^*, w_i \in W$ correspond to ϕ, and the sequence of r triples, f_1^*, g_1^*, w_1; f_2^*, g_2^*, w_2; .... ; f_r^*, g_r^*, w_r is called a *bilinear computation* for ϕ of length r [BCS1997, p. 354]. The *bilinear complexity* or *rank* $\mathfrak{R}(\phi)$ of ϕ is defined by

$$\mathfrak{R}(\phi) := \min\left\{ r \in \mathbb{Z}^+ \mid \phi(u, v) = \sum_{i=1}^{r} f_i^*(u)\, g_i^*(v)\, w_i,\ \ (u, v) \in U \times V \right\}.$$

where $f_i^* \in U^*, g_i^* \in V^*, w_i \in W$ uniquely correspond to ϕ, i.e. $\mathfrak{R}(\phi)$ is length r of the shortest bilinear computation for ϕ [BCS1997, p. 354]. For example, if $U = V = W = K^{n\times n}_{Diag}$, where $K^{n\times n}_{Diag}$ is the space of all $n \times n$ diagonal matrices over K with pointwise multiplication, then

$f_i^* = g_i^* = e_{ii}^*$, $w_i = E_{ii}$, $1 \leq i \leq r$, and $r = n$. In the same way, the rank $\mathfrak{R}(\langle n,m,p\rangle)$ of the tensor $\langle n,m,p\rangle$, i.e. the rank of $n \times m$ by $m \times p$ matrix multiplication, is the smallest positive integer r such that every product $AB \in K^{n\times p}$ of an $n \times m$ matrix $A \in K^{n\times m}$ and an $m \times p$ matrix $B \in K^{m\times p}$ has the bilinear representation

$$\langle n,m,p\rangle(A,B) = AB = \sum_{i=1}^{r} f_i^*(A)\, g_i^*(B)\, C_i$$

where $f_i^* \in K^{n\times m^*}$, $g_i^* \in K^{m\times p^*}$, $C_i \in K^{n\times p}$, $1 \leq i \leq r$. For example, $\mathfrak{R}(\phi) = n$ for any $\phi \in Bil_K\left(K_{Diag}^{n\times n}\right)$, e.g. $\mathfrak{R}\left(\langle n,n,n\rangle_{Diag}\right) = n$, where $\langle n,n,n\rangle_{Diag}$ is the multiplication map of $n \times n$ diagonal matrices.. For example, if K^n is the n dimensional space of all n-tuples over K, with a pointwise multiplication map $\langle n\rangle : K^n \times K^n \longrightarrow K^n$ of rank $\mathfrak{R}(\langle n\rangle) = \langle n\rangle$ then $\mathfrak{R}(\phi) = n$ for any $\phi \in Bil_K(K^n)$ if $\phi \cong_K \langle n\rangle$. This shows that $\mathfrak{R}(\langle n,n,n\rangle) \geq n$, because $K^n \cong_K K_{Diag}^{n\times n} \leq_K K^{n\times n}$. Another property of tensors $\langle n,m,p\rangle$ is invariance under permutations of their components, [BCS1997, pp. 358-359].

Proposition 2.1 $\mathfrak{R}(\langle n,m,p\rangle) = \mathfrak{R}(\langle \mu(n), \mu(m), \mu(p)\rangle)$, *for any permutation* $\mu \in Sym_3$.

For bilinear maps $\phi \in Bil_K(U,V;W)$ and $\phi' \in Bil_K\left(U',V';W'\right)$, ϕ is said to be a *restriction* of ϕ', and we write $\phi \leq_K \phi'$, if there exist linear maps (K-space homomorphisms) $\alpha : U \longrightarrow U', \beta : V \longrightarrow V', \gamma' : W' \longrightarrow W$ such that $\phi(u,v) = \gamma' \circ \phi' \circ (\alpha \times \beta)(u,v)$, for all $(u,v) \in U \times V$. In this regard, a basic result is the following.

Proposition 2.2 *For any bilinear maps* $\phi \in Bil_K(U,V;W)$ *and* $\phi' \in Bil_K\left(U',V';W'\right)$, $\phi \leq_K \phi'$ *implies* $\mathfrak{R}(\phi) \leq \mathfrak{R}\left(\phi'\right)$.

Proof. For bilinear maps $\phi \in Bil_K(U,V;W)$ and $\phi' \in Bil_K\left(U',V';W'\right)$ with ranks $\mathfrak{R}(\phi) = r$ and $\mathfrak{R}\left(\phi'\right) = r'$, respectively, the assumption that $\phi \leq_K \phi'$, by definition, implies there are linear maps $\alpha : U \longrightarrow U', \beta : V \longrightarrow V', \gamma' : W' \longrightarrow W$ such that $\phi(u,v) = \gamma' \circ \phi' \circ (\alpha \times \beta)(u,v)$,

for all $(u,v) \epsilon U \times V$. By these maps, for an arbitrary $(u,v) \epsilon U \times V$

$$\begin{aligned}
& \gamma^{'} \circ \phi^{'} \circ (\alpha \times \beta)(u,v) \\
= \; & \gamma^{'} \left(\phi^{'} \left((\alpha \times \beta)(u,v) \right) \right) \\
= \; & \gamma^{'} \left(\phi^{'} \left(\alpha(u), \beta(v) \right) \right) \\
= \; & \gamma \left(\sum_{j=1}^{r^{'}} f_j^{'*}(\alpha(u)) \, g_j^{'*}(\beta(v)) \, w_j^{'} \right) \\
= \; & \sum_{j=1}^{r^{'}} \gamma \left(f_j^{'*}(\alpha(u)) \, g_j^{'*}(\beta(v)) \, w_j^{'} \right) \\
= \; & \sum_{j=1}^{r^{'}} f_{j^{'}*}(u) \, g_{j^{'}*}(v) \, w_{j^{'}} \qquad (+) \\
= \; & \phi(u,v),
\end{aligned}$$

where $f_{j^{'}*} \epsilon U^*$, $g_{j^{'}*} \epsilon V^*$, $w_{j^{'}} \epsilon W$, $1 \leq j \leq r^{'}$, and $f_j^{'*}, g_j^{'*}, w_j$; $f_j^{'*} \epsilon U^{'*}, g_j^{'*} \epsilon V^{'*}, w_j^{'} \epsilon W^{'}$, $1 \leq j \leq r^{'}$ is the minimal bilinear computation for $\phi^{'}$. Since we must have $\phi(u,v) = \sum_{i=1}^{r} f_i^*(u) \, g_i^*(v) \, w_i$, where f_i^*, g_i^*, w_i; $f_i^* \epsilon U^*, g_i^* \epsilon V^*, w_i \epsilon W$, $1 \leq i \leq r$ is the minimal bilinear computation for ϕ, the minimum number r of terms which can occur in sums of the type $(+)$ must be $\leq r^{'}$, i.e. $r \leq r^{'}$. ■

Two bilinear maps $\phi \epsilon Bil_K(U,V;W)$ and $\phi^{'} \epsilon Bil_K\left(U^{'},V^{'};W^{'}\right)$ are said to be isomorphic if there exist isomorphisms $\alpha : U \longrightarrow U^{'}$, $\beta : V \longrightarrow V^{'}$, and $\gamma : W \longrightarrow W^{'}$ such that $\gamma \circ \phi = \phi^{'} \circ (\alpha \times \beta)$, [BCS1997, p. 355]. The following proposition is a basic result for isomorphism of bilinear maps.

Corollary 2.3 *For any bilinear maps $\phi \epsilon Bil_K(U,V;W)$ and $\phi^{'} \epsilon Bil_K\left(U^{'},V^{'};W^{'}\right)$, $\phi \cong_K \phi^{'}$ implies $\phi \leq_K \phi^{'}$ and $\phi^{'} \leq_K \phi$, in which case also $\mathfrak{R}(\phi) = \mathfrak{R}\left(\phi^{'}\right)$.*

Proof. Consequence of *Proposition 2.2.* ■

As an example of restrictions, consider the matrix spaces $U = K^{n \times m}$, $V = K^{m \times p}$, $W = K^{n \times p}$ and $U^{'} = K^{n^{'} \times m^{'}}$, $V^{'} = K^{m^{'} \times p^{'}}$, $W^{'} = K^{n^{'} \times p^{'}}$, where $n \leq n^{'}$, $m \leq m^{'}$, $p \leq p^{'}$,

and $\phi = \langle n, m, p \rangle$ and $\phi^{'} = \left\langle n^{'}, m^{'}, p^{'} \right\rangle$. Then, there is a natural, injective linear map $\alpha : K^{n \times m} \longrightarrow K^{n^{'} \times m^{'}}$ which embeds an $n \times m$ matrix A into $K^{n^{'} \times m^{'}}$ as an $n^{'} \times m^{'}$ matrix $A^{'}$ having A as an $n \times m$ block in its top-left corner and 0's everywhere else. There are analogous injective linear embedding maps $\beta : K^{m \times p} \longrightarrow K^{m^{'} \times p^{'}}$ and $\gamma : K^{n \times p} \longrightarrow K^{n^{'} \times p^{'}}$ for $K^{m \times p}$ and $K^{n \times p}$, respectively. The product map $\alpha \times \beta : K^{n \times m} \times K^{m \times p} \longrightarrow K^{n^{'} \times m^{'}} \times K^{m^{'} \times p^{'}}$ will be injective and there will be a natural surjective linear map $\gamma^{'} : K^{n^{'} \times p^{'}} \longrightarrow K^{n \times p}$ which is the identity map on left upper $n \times p$ blocks of $n^{'} \times p^{'}$ matrices. Hence we have a restriction $\langle n, m, p \rangle = \gamma^{'} \circ \left\langle n^{'}, m^{'}, p^{'} \right\rangle \circ (\alpha \times \beta)$ of $\left\langle n^{'}, m^{'}, p^{'} \right\rangle$ to $\langle n, m, p \rangle$. Informally, we have proved the following [BCS1997, p. 357 & 362].

Proposition 2.4 *If* $n \leq n^{'}, m \leq m^{'}, p \leq p^{'}$ *then* $\langle n, m, p \rangle \leq_K \left\langle n^{'}, m^{'}, p^{'} \right\rangle$, *and* $\mathfrak{R}(\langle n, m, p \rangle) \leq \mathfrak{R}\left(\left\langle n^{'}, m^{'}, p^{'} \right\rangle\right)$.

If U and V are two algebras of dimensions n and m, respectively, then their direct sum $U \oplus V$ is an $n + m$ dimensional K-space which has as a basis the union of the bases $\{(u_i, 0)\}_{1 \leq i \leq n}$ and $\{(0, v_j)\}_{1 \leq j \leq m}$ where $\{u_i\}_{1 \leq i \leq n}$ and $\{v_j\}_{1 \leq j \leq m}$ are the bases of U and V respectively, and their Kronecker product $U \otimes V$ is an nm dimensional K-space of sums of *dyads* $u \otimes v$, $u \in U$, $v \in V$, which has as a basis $\{u_i \otimes v_j\}_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$. If U and V are two algebras of dimensions n and m, respectively, then $U \otimes V$ becomes an nm-dimensional algebra with multiplication with the property that $(u \otimes v)\left(u^{'} \otimes v^{'}\right) = \left(uu^{'} \otimes vv^{'}\right)$ for any pair of elements $u \otimes v$, $u^{'} \otimes v^{'} \in U \otimes V$. For bilinear maps $\phi \in Bil_K(U, V; W)$ and $\phi^{'} \in Bil_K\left(U^{'}, V^{'}; W^{'}\right)$, their direct sum $\phi \oplus \phi^{'} \in Bil_K\left(U \oplus U^{'}, V \oplus V^{'}; W \oplus W^{'}\right)$ and Kronecker product $\phi \otimes \phi^{'} \in Bil_K\left(U \otimes U^{'}, V \otimes V^{'}; W \otimes W^{'}\right)$ can be defined and satisfy $\mathfrak{R}\left(\phi \oplus \phi^{'}\right) \leq \mathfrak{R}(\phi) + \mathfrak{R}\left(\phi^{'}\right)$ and $\mathfrak{R}\left(\phi \otimes \phi^{'}\right) \leq \mathfrak{R}(\phi)\mathfrak{R}\left(\phi^{'}\right)$ [BCS1997, p. 360]. An important fact here is that to each bilinear map $\phi \in Bil(U, V; W)$ there exists one and only one unique tensor $t_\phi \in U^* \otimes V^* \otimes W$, called the *structural tensor* of ϕ, [BCS1997, p. 358], i.e. $Bil(U, V; W) \cong_K U^* \otimes V^* \otimes W$. Therefore, the isomorphism of two bilinear maps, as described before *Corollary 2.3*, is equivalent to the isomorphism of their corresponding structural tensors, and therefore, the rank of a bilinear map is equal to the rank of its structural tensor.

For tensors we have an important but easily provable result [BCS1997, pp. 360-361].

Proposition 2.5 *For tensors* $\langle n, m, p \rangle$ *and* $\left\langle n^{'}, m^{'}, p^{'} \right\rangle$,

$$(1)\ \ \langle n, m, p \rangle \oplus \left\langle n^{'}, m^{'}, p^{'} \right\rangle \leq_K \left\langle n + n^{'}, m + m^{'}, p + p^{'} \right\rangle$$

and

$$(2)\ \ \langle n, m, p \rangle \otimes \left\langle n^{'}, m^{'}, p^{'} \right\rangle \cong_K \left\langle nn^{'}, mm^{'}, pp^{'} \right\rangle.$$

Direct sums of matrix tensors describe block diagonal matrix multiplication, and Kronecker products of tensors describe block matrix multiplication. A basic result which we will use is the following, as defined in [BCS1997] just before Def. (14.18).

Proposition 2.6 *For tensors* $\langle n, m, p \rangle$ *and* $\left\langle n^{'}, m^{'}, p^{'} \right\rangle$,

$$(1)\ \mathfrak{R}\left(\langle n, m, p \rangle \oplus \left\langle n^{'}, m^{'}, p^{'} \right\rangle\right) \leq \mathfrak{R}\left(\langle n, m, p \rangle\right) + \mathfrak{R}\left(\left\langle n^{'}, m^{'}, p^{'} \right\rangle\right)$$

and

$$(2)\ \mathfrak{R}\left(\langle n, m, p \rangle \otimes \left\langle n^{'}, m^{'}, p^{'} \right\rangle\right) \leq \mathfrak{R}\left(\langle n, m, p \rangle\right) \cdot \mathfrak{R}\left(\left\langle n^{'}, m^{'}, p^{'} \right\rangle\right).$$

2.1.3 *Matrix Algebras*

A K-algebra A is a vector space A defined over a field K, together with a vector multiplication map $\phi_A : A \times A \longrightarrow A$ which is bilinear on A, in the sense described above, with a unique unit 1_A which coincides with the unit of A as a multiplicative monoid. (Here, by definition an algebra A has a unit.) The dimension of the algebra A is defined to be its dimension as a vector space. We denote the unit of A by 1_A. A is called *associative* iff ϕ_A is associative, and *commutative* iff ϕ_A is commutative. The rank $\mathfrak{R}(A)$ of A is defined to be the rank $\mathfrak{R}(\phi_A)$ of ϕ_A, and is a bilinear measure of the multiplicative complexity in A. For example, the matrix space $K^{n \times m}$ is a matrix K-algebra iff $n = m$. $K^{n \times n}$ is an n^2 dimensional matrix K-algebra with a bilinear map $\langle n, n, n \rangle$ describing multiplication of $n \times n$ by $n \times n$ matrices. We say that n is the *order* of the algebra $K^{n \times n}$.

If A and B are two K-algebras then a linear map $\varphi : A \longrightarrow B$ which carries vector multiplication in A onto vector multiplication in B is called an *algebra homomorphism*, or simply, an *algebra morphism*, between A and B, i.e. if for any $a, a^{'} \epsilon A$, $\varphi(a, a^{'}) = \varphi(a)\,\varphi\left(a^{'}\right)$, and $\varphi(1_A) = 1_B$. A simple example is the inclusion homomorphism $\varkappa_2$ of the algebra $K^{2\times 2}_{Diag}$ of all diagonal 2×2 matrices over K into the algebra $K^{2\times 2}$ of all 2×2 matrices. φ is an algebra isomorphism $A \cong_K B$ iff $\phi_A \cong_K \phi_B$ ($\Longrightarrow \mathfrak{R}(\phi_A) = \mathfrak{R}(\phi_B)$), [BCS1997, p. 356]. For example, $\langle 2,2,2\rangle_{Diag} \leq_K \langle 2,2,2\rangle$ and $\mathfrak{R}\left(\langle 2,2,2\rangle_{Diag}\right) = 2 \leq \mathfrak{R}(\langle 2,2,2\rangle)$, and $\mathfrak{R}\left(\langle 2,2,2\rangle_{Diag}\right) = 2 = \mathfrak{R}(\langle 2\rangle)$ because $K^{2\times 2}_{Diag} \cong_K K^2$, where $K^2 \leq_K K^{2\times 2}$. In general, for any n-dimensional algebra A it is the case that $\mathfrak{R}(\phi_A) = n$ iff $A \cong_K K^n$, or equivalently iff $\phi_A \cong_K \langle n\rangle$, [BCS1997, p. 364].

The following is a general result for matrix algebras.

Proposition 2.7 *For positive integers n, $n^{'}$,*

$$(1)\ \textit{if } n \leq n^{'} \textit{ then } \langle n,n,n\rangle \leq_K \left\langle n^{'}, n^{'}, n^{'}\right\rangle \textit{ and } \mathfrak{R}(\langle n,n,n\rangle) \leq \mathfrak{R}\left(\left\langle n^{'}, n^{'}, n^{'}\right\rangle\right)$$

and

$$(2)\ \langle n,n,n\rangle \cong_K \left\langle n^{'}, n^{'}, n^{'}\right\rangle \textit{ and } \mathfrak{R}(\langle n,n,n\rangle) = \mathfrak{R}\left(\left\langle n^{'}, n^{'}, n^{'}\right\rangle\right) \textit{ iff } n = n^{'}.$$

If $\{K^{n_i\times n_i}\}$ is a finite collection of matrix algebras $K^{n_i\times n_i}$ of orders n_i, then $\underset{i}{\oplus} K^{n_i\times n_i}$ is a direct sum matrix algebra of order $\sum\limits_i n_i$, in which multiplication is block diagonal and is described by the direct sum tensor $\underset{i}{\oplus}\langle n_i, n_i, n_i\rangle \cong \left\langle \sum\limits_i n_i, \sum\limits_i n_i, \sum\limits_i n_i\right\rangle$; and $\underset{i}{\otimes} K^{n_i\times n_i}$ is a Kronecker product matrix algebra of order $\prod\limits_i n_i$, in which multiplication is described by the Kronecker product tensor $\underset{i}{\otimes}\langle n_i, n_i, n_i\rangle \cong \left\langle \prod\limits_i n_i, \prod\limits_i n_i, \prod\limits_i n_i\right\rangle$. Using *Proposition 2.6*, we have the following result.

Proposition 2.8 *For a finite set of positive integers n_i*

$$(1)\ \mathfrak{R}\left(\underset{i}{\oplus}\langle n_i, n_i, n_i\rangle\right) \leq \sum_i \mathfrak{R}(\langle n_i, n_i, n_i\rangle)$$

and

$$(2)\ \mathfrak{R}\left(\bigotimes_i \langle n_i, n_i, n_i\rangle\right) \leq \prod_i \mathfrak{R}\left(\langle n_i, n_i, n_i\rangle\right).$$

When $n_i = n$, for $1 \leq i \leq r$, we shall denote by $\langle n, n, n\rangle^{\otimes r}$ the r-fold Kronecker product $\bigotimes_{1\leq i\leq r} \langle n, n, n\rangle$. By part (2) of *Proposition 2.5* $\langle n, n, n\rangle^{\otimes r} \cong \langle n^r, n^r, n^r\rangle$ and $\mathfrak{R}\left(\langle n, n, n\rangle^{\otimes r}\right) = \mathfrak{R}\left(\langle n^r, n^r, n^r\rangle\right)$. The following is a relevant proposition.

Proposition 2.9 *For positive integers* r, n, $\mathfrak{R}\left(\langle n^r, n^r, n^r\rangle\right) \leq \mathfrak{R}\left(\langle n, n, n\rangle\right)^r$.

2.1.4 *The Rank of* 2×2 *Matrix Multiplication is at most* 7

We explain here Strassen's result that the rank of 2×2 matrix multiplication is at most 7. If $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ and $B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$ are given 2×2 matrices, then by the formulas

$$\begin{aligned}
P_1 &= (A_{11} + A_{22})(B_{11} + B_{22}), \\
P_2 &= (A_{21} + A_{22})B_{11}, \\
P_3 &= A_{11}(B_{12} - B_{22}), \\
P_4 &= (-A_{11} + A_{21})(B_{11} + B_{12}), \\
P_5 &= (A_{11} + A_{12})B_{22}, \\
P_6 &= A_{22}(-B_{11} + B_{21}), \\
P_7 &= (A_{12} - A_{22})(B_{21} + B_{22})
\end{aligned}$$

we will be able to recover their product $AB = C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$ by the formulas

$$\begin{aligned}
C_{11} &= P_1 + P_6 - P_5 + P_7, \\
C_{12} &= P_3 + P_5, \\
C_{21} &= P_2 + P_6, \\
C_{22} &= P_1 - P_2 + P_3 + P_4,
\end{aligned}$$

using a total of $7 = \#\{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$ multiplications and 18 additions/subtractions [PAN1984, p. 394].

If we then define 7 paired linear forms $f_i^*, g_i^* \in K^{2\times 2^*}$, $1 \leq i \leq 7$, by

$$\begin{aligned}
f_1^*(A) &= A_{11} + A_{22} & g_1^*(B) &= B_{11} + B_{22} \\
f_2^*(A) &= A_{21} + A_{22} & g_2^*(B) &= B_{11} \\
f_3^*(A) &= A_{11} & g_3^*(B) &= B_{12} - B_{22} \\
f_4^*(A) &= -A_{11} + A_{21} & g_4^*(B) &= B_{11} + B_{12} \\
f_5^*(A) &= A_{11} + A_{12} & g_5^*(B) &= B_{22} \\
f_6^*(A) &= A_{22} & g_6^*(B) &= -B_{11} + B_{21} \\
f_7^*(A) &= A_{12} - A_{22} & g_7^*(B) &= B_{21} + B_{22}
\end{aligned}$$

then there are matrices $C_i \in K^{2\times 2}$, $1 \leq i \leq 7$, such that

$$AB = \sum_{i=1}^{7} f_i^*(A) g_i^*(B) C_i$$

hence $\mathfrak{R}(\langle 2, 2, 2, \rangle) \leq 7$ [BCS1997, pp. 10-13]. We state this formally, for future reference.

Proposition 2.10 $\mathfrak{R}(\langle 2, 2, 2, \rangle) \leq 7$.

In general, if $n = 2m$, this algorithm allows us to multiply $2m \times 2m$ matrices with 7 multiplications and 18 additions/subtractions of $m \times m$ matrices, for $m \geq 1$. We define an integer function $T_K(n)$ by

(2.1) $T_K(n) := \min_{t \in \mathbb{Z}^+}$ *two $n \times n$ matrices can be multiplied using t multiplications, additions, or subtractions.*

If n is some power 2^m of 2, then we can partition two $2^m \times 2^m$ matrices into four $2^{m-1} \times 2^{m-1}$ blocks each, and view these blocks as inputs to the original algorithm, and by a recursive application of this procedure we obtain for $T_K(n)$ the following recursion formula [BCS1997, pp. 12-13].

(2.2) $T_K(n) \leq 7T_K\left(\frac{1}{2}n\right) + 18\left(\frac{1}{2}n\right)^2$.

In 1971, Winograd proved a stronger result that $\mathfrak{R}(\langle 2,2,2,\rangle) = 7$, [WIN1971].

2.2 Asymptotic Complexity of Matrix Multiplication

Here we introduce the exponent ω describing the asymptotic complexity of matrix multiplication, including Strassen's estimate of $\omega < 2.81$, and conclude with some fundamental relations between ω and the ranks of matrix tensors, which we shall use later in our analysis and estimates of ω in *Chapter 6*.

2.2.1 *The Exponent of Matrix Multiplication*

We denote by $M_K(n)$ the total number of arithmetical operations $\{\times, +, -\}$ needed to multiply $n \times n$ matrices over K. This is defined more formally as:

(2.3) $$M_K(n) := L^{tot}_{K[X,Y]}(n) := L^{tot}_{K[X,Y]}\left(\left\{\sum_{1\leq j\leq n} X_{ij}Y_{jk};\ 1 \leq i,k \leq n\right\}\right),$$

where $K[X,Y]$ is the ring of bivariate polynomials over K, and the expression on the right is an *exact* measure of the total number *tot* of arithmetical operations $\{\times, +, -\}$ needed to multiply two $n \times n$ matrices of a given set of indeterminates X_{ij}, $Y_{jk} \in K$, $1 \leq i,j,k \leq n$, over K without divisions [BCS1997, p. 108, p. 126, p. 375].

The *exponent of matrix multiplication over* K is the real number $\omega(K) > 0$ defined by

(2.4) $$\omega(K) := \inf\left\{h \in \mathbb{R}^+ \mid M_K(n) = O\left(n^h\right),\ n \longrightarrow \infty\right\}.$$

The notation $\omega(K)$ is intended to indicate a possible dependency on the ground field K. It has been proved that $\omega(K)$ is unchanged if we replace K by any algebraic extension $\overline{K}$

[BCS1997, p. 383]. It has also been proved that $\omega(K)$ is determined only by the characteristic $Char\ K$ of K, such that $\omega(K) = \omega(\mathbb{Q})$ if $Char\ K = 0$, and $\omega(K) = \omega(\mathbb{Z}_p)$ otherwise, where $\mathbb{Z}_p$ is the finite field of integers modulo a prime p, of characteristic p, [PAN1984].. Since $Char\ \mathbb{C} = Char\ \mathbb{R} = Char\ \mathbb{Q} = 0$, this means that $\omega(\mathbb{C}) = \omega(\mathbb{R}) = \omega(\mathbb{Q})$. In this chapter, we shall continue to indicate the ground field dependency in writing $\omega(K)$, but in later chapters we shall drop this formalism and simply write ω, since our concern will be with complex matrix multiplication, which is general enough for most purposes.

Returning to $M_K(n)$, by the standard algorithm for $n \times n$ matrix multiplication, the n^2 entries C_{ik} of an $n \times n$ matrix product $C = AB$ are given by the formula $C_{ik} = \sum_{1 \leq j \leq n} A_{ij}B_{jk}$, for all $1 \leq i, k \leq n$. In using the standard algorithm, we will be using n^3 multiplications, and $n^3 - n^2$ additions of the resulting products, which yields an upper estimate $M_K(n) = 2n^3 - n^2 < 2n^3 = O(n^3)$, i.e. $M_K(n) < C' n^3$ for the constant $C' = 2$, and implies an upper bound of 3 for ω [BCS1997, p. 375]. For the lower bound, we note that since the product of two $n \times n$ matrices consists of n^2 entries, one needs to perform a total number of operations which is *at least* some constant $C \geq 1$ multiple of the n^2 entries, which we denote by $M_K(n) = \Omega(n^2)$, and is equivalent to a lower bound of 2 for ω [BCS1997, p. 375]. (Our focus will be on the upper bounds for $M_K(n)$ since we are interested in worst case complexity.) Informally, we have proved the following elementary result.

Proposition 2.11 *For every field K, (1) $2 \leq \omega(K) \leq 3$, and (2) $\omega(K) = h\ \epsilon\ [2,3]$ iff $\Omega(n^{h+\epsilon}) = M_K(n) = O\left(n^{h+\varepsilon}\right)$, where h is uniquely minimal for any given degree of precision $\varepsilon > 0$.*

The connection between the exponent ω and the concept of bilinear rank is established by the following important proposition, [BCS1997, pp. 376-377].

Proposition 2.12 *For every field K*

$$\omega(K) = \inf\left\{h\ \epsilon\ \mathbb{R}^+ \mid \mathfrak{R}(\langle n, n, n\rangle) = O\left(n^h\right),\ n \longrightarrow \infty\right\}.$$

This means for any given degree of precision $\varepsilon > 0$, with respect to a given field K, there exists a constant $C_{K,\varepsilon} \geq 1$, independent of n, such that $\mathfrak{R}(\langle n, n, n\rangle) \leq C_{K,\varepsilon} n^{\omega(K)+\varepsilon}$ for all n. It is conjectured that $\omega(\mathbb{C}) = 2$, [CU2003]. Henceforth, ω shall denote $\omega(\mathbb{C})$ and in the concluding sections we shall describe some important relations between ω and the concept of tensor rank, introduced earlier, which describe the conditions for realizing estimates of ω of varying degrees of sharpness.

2.2.2 *Relations between the Rank of Matrix Multiplication and the Exponent* ω

Taking tensor product powers in the estimate $\mathfrak{R}(\langle 2, 2, 2\rangle) \leq 7$ (*Proposition 2.10*) we have, by part (2) of *Proposition 2.9*,

$$\mathfrak{R}(\langle 2^n, 2^n, 2^n\rangle) = \mathfrak{R}\left(\langle 2, 2, 2\rangle^{\otimes n}\right) \leq \mathfrak{R}(\langle 2, 2, 2\rangle)^n \leq 7^n.$$

Since for all positive integers $n \geq 2$, $n \leq 2^{\lceil \log_2 n \rceil} = n + \varepsilon_n$, where $\varepsilon_n > 0$ is a residual depending on n, and $\lceil \cdot \rceil$ denotes the ceiling function for real numbers, using *Proposition 2.9* again we have

$$\begin{aligned}
\mathfrak{R}(\langle n, n, n\rangle) &\leq \mathfrak{R}\left(\left\langle 2^{\lceil \log_2 n \rceil}, 2^{\lceil \log_2 n \rceil}, 2^{\lceil \log_2 n \rceil}\right\rangle\right) \\
&\leq \mathfrak{R}(\langle 2, 2, 2\rangle)^{\lceil \log_2 n \rceil} \\
&\leq 7^{\lceil \log_2 n \rceil} \\
&\leq 7n^{\log_2 7} \approx 7n^{2.807}.
\end{aligned}$$

By *Proposition 2.12* this gives Strassen's estimate $\omega < 2.81$ [STR1969, pp. 354-356]. The best estimate of ω is Coppersmith and Winograd's result that $\omega < 2.38$ [CW1990, p. 251].

Assume that $\mathfrak{R}(\langle n, m, p\rangle) \leq s$ for positive integers n, m, p, and s. By *Proposition 2.1* and part (2) of *Proposition 2.5*, $\langle nmp, nmp, nmp\rangle \cong \langle n, m, p\rangle \otimes \langle m, p, n\rangle \otimes \langle p, n, m\rangle$. Then, we see

that

$$\begin{aligned} & \mathfrak{R}\left(\langle nmp, nmp, nmp\rangle\right) \\ = \; & \mathfrak{R}\left(\langle n,m,p\rangle \otimes \langle m,p,n\rangle \otimes \langle p,n,m\rangle\right) \\ \leq \; & \mathfrak{R}\left(\langle n,m,p\rangle^{\otimes 3}\right) \\ \leq \; & \mathfrak{R}\left(\langle n,m,p\rangle\right)^3 \\ \leq \; & s^3. \end{aligned}$$

i.e. that $(nmp)^{\omega} \leq s^3$, which is equivalent to $(nmp)^{\frac{\omega}{3}} \leq s$. We have proved the following result, which we shall repeatedly use later [BCS1997, p. 380]. Since $\mathfrak{R}\left(\langle n,m,p\rangle\right)$ is, by definition, a positive integer, and $\mathfrak{R}\left(\langle n,m,p\rangle\right) \leq \mathfrak{R}\left(\langle n,m,p\rangle\right)$, we have proved the following.

Proposition 2.13 $(nmp)^{\frac{\omega}{3}} \leq \mathfrak{R}\left(\langle n,m,p\rangle\right)$ *for any positive integers* n, m, p.

This is equivalent to $\omega \leq \frac{\log \mathfrak{R}(\langle n,m,p\rangle)}{\log(nmp)^{1/3}}$, for any positive integers n, m, p, a consequence which occurs in a group-theoretic context as shown in *Chapter 4*. Informally, we can understand nmp to be "size" of $n \times m$ by $m \times p$ matrix multiplication, and $(nmp)^{\frac{1}{3}}$ to be the (geometric) mean of this size. The above proposition has as a generalization the following statement.

Proposition 2.14 $\sum\limits_i \left(n_i m_i p_i\right)^{\frac{\omega}{3}} \leq \mathfrak{R}\left(\bigoplus\limits_i \langle n_i, m_i, p_i\rangle\right)$, *for any finite set of positive integer triples* n_i, m_i, p_i.

This is a formulation in terms of ordinary rank $\mathfrak{R}$ of Schönhage's asymptotic direct sum inequality involving the related but approximative concept of border rank $\underline{\mathfrak{R}}$, which we shall not discuss further [BCS1997, p. 380]. In essence, *Proposition 2.14* means that the complexity of several, simultaneous independent matrix multiplications is at least the sum of the mean sizes of the multiplications to the power ω, a consequence which occurs in a group-theoretic context as shown in *Chapter 5*.

Chapter 3

Basic Representation Theory

We start with some basic theory of representations and character theory of finite groups, focusing in particular on various relations and estimates for sums of powers of the distinct irreducible group character degrees, which will be important in the central analysis in *Chapter 4*. Then we proceed to describe basic facts about multiplicative complexity in regular group algebras, and conclude with an outline of the discrete Fourier transforms for groups and their computational complexities.

3.1 Basic Representation Theory and Character Theory of Finite Groups

3.1.1 *Representations, $\mathbb{C}G$-Modules and Characters*

In this thesis, a (finite-dimensional) *representation* π of a finite group G is defined as a group homomorphism $\pi : G \longrightarrow GL(V)$, where V is a finite-dimensional, complex vector space, and where $GL(V)$ is the group of all linear operators mapping V to itself. In particular, when $V = \mathbb{C}^n$ then $GL(V) = GL(n, \mathbb{C})$, the group of all invertible $n \times n$ complex matrices, and π is called a *matrix representation* of G. For example, G always has the trivial representation ι on V, defined by $g \longrightarrow 1_{GL(V)}$, whenever $g \in G$, where $1_{GL(V)}$ is the identity automorphism of V. If π is a representation of G we will call V the *target space* of π, and define the *dimension of*

π to be the dimension of V, i.e. $Dim\ \pi := Dim\ V$. For each $g \epsilon G$, $\pi(g)$ is an automorphism $V \longrightarrow V$ of V, and we note that π satisfies $\pi(gh) = \pi(g)\pi(h)$, $\pi(g^{-1}) = (\pi(g))^{-1}$, for all $g, h \epsilon G$, and that in particular, $\pi(1_G) = 1_{GL(V)}$, the trivial automorphism of V. A representation of G, the so-called (*right*) *regular representation*, exists when $V = \mathbb{C}^G = \{f \mid f : G \longrightarrow \mathbb{C}\}$, the $|G|$-dimensional, associative $\mathbb{C}$-algebra of all complex-valued maps $f : G \longrightarrow \mathbb{C}$ on G, with standard basis $\mathcal{B}_G = \left\{e_g \mid e_g \epsilon \mathbb{C}^G,\ e_g(h) = \delta_{g,h},\ h \epsilon G\right\}$ of the $|G|$ indicator maps $e_g \longleftrightarrow g \epsilon G$. $\mathbb{C}^G$ can be identified with the set $\mathbb{C}G = \left\{\sum\limits_{g\ \epsilon\ G} f_g g \mid f \epsilon \mathbb{C}^G, f(g) \equiv f_g\right\}$ of all formal linear sums of group elements with coefficients as their f-values, for each $f \epsilon \mathbb{C}^G$. $\mathbb{C}G$ constitutes a $|G|$-dimensional vector space over $\mathbb{C}$ and it is a $\mathbb{C}$-algebra called the *regular group algebra of* G, admitting as basis elements the elements of G itself, yielding the *regular basis*. The endomorphisms $f = \sum\limits_{g'\ \epsilon\ G} f_{g'} g' \mapsto gf := \sum\limits_{g'\ \epsilon\ G} f_{g'} \left(gg'\right)$, $f \epsilon \mathbb{C}G$, arbitrary fixed $g \epsilon G$, describe permutation left-actions on regular basis components of $f \epsilon \mathbb{C}G$ for elements $g \epsilon G$ via their uniquely associated permutations $\mu_g \epsilon Sym_{|G|}$, and have unique associated permutation matrices $[g]_G \epsilon GL(|G|, \mathbb{C})$. The regular representation of G, denoted by $\rho_{\mathbb{C}G}$, is the mapping $g \longmapsto [g]_G = \rho_{\mathbb{C}G}(g)$, $g \epsilon G$.

Let π be a representation of G on a vector space V. If W is a subspace of V which is invariant under the automorphisms $\pi(g)$, i.e. $\pi(g)(W) \subseteq W$, for all $g \epsilon G$, then W is called π-*invariant*. The restriction $\pi \downarrow W$ of π to a π-invariant subspace W of V produces a representation ρ of G on W called a *subrepresentation* of π, which can be called a *component* (representation) of π, and conversely, every subrepresentation ρ of a representation π of G on V is the restriction $\pi \downarrow W$ of π to some π-invariant subspace W of V depending on ρ: ρ is given by $\rho(g)(w) = \pi(g)(w)$, for all $g \epsilon G$, $w \epsilon W$. It follows that the dimension of a subrepresentation of a representation of G cannot exceed the dimension of the representation. π is called *irreducible* iff it contains no nontrivial subrepresentations, otherwise it is called *reducible*. G admits always has the trivial 1-dimensional irreducible representation ι_1, as defined by $g \longrightarrow (1)$, and conversely any 1-dimensional representation is irreducible; equivalently, the dimension of a reducible representation is at least 2. If ρ is any other representation of G on a vector space W, then π and ρ are called *equivalent* (notation $\pi \sim \rho$) iff there is a vector space isomorphism $T : V \cong W$ such that $T(gv) := T(\pi(g)(v)) = \rho(g)T(v) =: gT(v)$, for all $g \epsilon G$, $v \epsilon V$. Otherwise, i.e. if such a T does not exist for π and ρ, they are called *inequivalent*, and we denote this by

$\pi \nsim \rho$. Equivalence of representations is an equivalence relation. If ϱ and ς are two irreducible representations of G then we define the delta quantity $\delta_{\varrho,\varsigma}$ as $\delta_{\varrho,\varsigma} = 1$ iff $\varrho \sim \varsigma$ and $\delta_{\varrho,\varsigma} = 0$ iff $\varrho \nsim \varsigma$.

Given a representation π of G on a vector space V, there is a naturally defined multiplication map $G \times V \longrightarrow V$ describing left-action $(g, v) \longmapsto gv := \pi(g)\, v$ of G on V, which is associative: $(gh)(v) = g(hv)$; has a natural identity: $1_G v = v$ for all $v \in V$; is invertible: $v = g^{-1}(gv) = g(g^{-1}v)$; is homogenous with respect to scalar multiples of vectors: $g(\lambda v) = \lambda(gv)$; and is right-linear with respect to $\mathbb{C}G$-multiplication: $g(v + v') = gv + gv'$; for all elements $g, h \in G$, vectors v, $v' \in V$, scalars $\lambda \in \mathbb{C}$. The space V under this multiplication is called a $\mathbb{C}G$-*module*, and its dimension is its dimension as a vector space. A special kind of $\mathbb{C}G$-module, called the *regular* $\mathbb{C}G$-module, occurs when $V = \mathbb{C}G = \left\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in \mathbb{C} \right\}$, the regular group algebra of G, discussed above. A subspace W of V is called a $\mathbb{C}G$-*submodule* of V iff it is closed under the map $G \times V \longrightarrow V$ via π. A $\mathbb{C}G$-submodule W of V under the representation π always corresponds to some subrepresentation ρ of π. V and the zero subspace $\{\mathbf{O}_V\}$ always form trivial $\mathbb{C}G$-submodules of V, and V is an *irreducible* $\mathbb{C}G$-*module* iff it contains no nontrivial $\mathbb{C}G$-submodules. Two $\mathbb{C}G$-modules V and W, corresponding to representations π and ρ, respectively, of G, are called equivalent iff π is equivalent to ρ, otherwise they are called inequivalent.

Given a representation π of G on a space V, the *character* χ_π of π (also, the character of V as a $\mathbb{C}G$-module) stands for the map $G \longrightarrow \mathbb{C}$ defined by $\chi_\pi(g) := Tr(\pi(g))$, $g \in G$, where $Tr(\cdot)$ is the trace map for operators. The *degree* d_π of the character χ_π is defined to be the dimension of its underlying representation π, i.e. $d_\pi := \chi_\pi(1_G) = Tr(\pi(1_G)) = Tr(1_{GL(V)}) = Dim\ \pi = Dim\ V$. For example, the character χ_{ι_1} of the trivial irreducible representation ι_1 is defined by $g \longmapsto 1$, $g \in G$. The set of all characters χ_π of G is denoted by $\widehat{G}$. Characters of degree 1 are called linear. A character χ_π is said to be irreducible iff its underlying representation π is irreducible, otherwise it is said to be reducible. All linear characters are irreducible. The characters χ_π and χ_ρ of equivalent representations π and ρ, respectively, are the same, and, conversely, π and ρ are equivalent if $\chi_\pi = \chi_\rho$. The character of the regular representation $\rho_{\mathbb{C}G}$ of G, called the *regular character* of G, denoted by $\chi_{\mathbb{C}G}$, is the map $G \longrightarrow \mathbb{C}$ defined by

$g \longmapsto Tr(\chi_{\mathbb{C}G}(g))$, $g \in G$. Observe that $\chi_{\mathbb{C}G}$ takes the value $|G|$ if $g = 1_G$, and 0 otherwise. It holds that $d_{\chi_{\mathbb{C}G}} = |G|$. We define the *inner product* of two characters χ_π and χ_ρ of G by $\langle \chi_\pi, \chi_\rho \rangle = |G|^{-1} \sum_{g \in G} \chi_\pi(g) \overline{\chi_\rho(g)}$.

3.1.2 *Canonical Decompositions for Regular Representations, $\mathbb{C}G$-Modules, and Characters*

A representation π of G is called *completely reducible* iff its target $\mathbb{C}G$-module V is the direct sum $V = \bigoplus_{\varrho_\pi \text{ irreducible}} R_{\varrho_\pi}$ of a finite number of irreducible $\mathbb{C}G$-modules R_{ϱ_π}, in which case π is the direct sum of a finite number of irreducible representations ϱ_π of G, occuring with multiplicity $l_{\pi,\varrho} = \langle \chi_\pi, \varrho_\pi \rangle > 0$, called the *irreducible components* of π, of dimensions d_{ϱ_π}. The following is a fundamental theorem in this regard [SER1977].

Theorem 3.1 *(Maschke) Every finite-dimensional representation of a finite group is completely reducible.*

The character χ_π of π is said to completely reducible iff π is completely reducible, and will take the form $\chi_\pi = \sum_{\varrho_\pi \text{ irreducible}} \chi_{\varrho_\pi}$, and will have degree $d_\pi = \sum_{\varrho_\pi \text{ irreducible}} d_{\varrho_\pi}$, which is, by definition, the dimension of π and of V.

The following theorem is crucial here [HUP1998], [SER1977].

Theorem 3.2 *(Frobenius) If G is a finite group then* (1) *the number of its distinct irreducible representations ϱ is equal to the number of its distinct conjugacy classes, denoted by $c(G)$, which is called its class number.* (2) *The characters χ_ϱ of the irreducible representations ϱ form an orthonormal basis of $\mathbb{C}G$, i.e. $\langle \chi_\varrho, \chi_\varsigma \rangle = \delta_{\varrho,\varsigma}$, for distinct irreducible representations ϱ and ς.* (3) *An arbitrary representation π of G, or its target $\mathbb{C}G$-module V_π, is irreducible iff its character χ_π satisfies $\langle \chi_\pi, \chi_\pi \rangle = 1$.* (4) *$\left|\chi_\varrho(g)\right| \leq \left|\chi_\varrho(1_G)\right| = d_\varrho$, $g \in G$, for any irreducible character χ_ϱ of G.*

There are exactly $c(G)$ distinct irreducible representations ϱ upto equivalence, $c(G)$ distinct irreducible $\mathbb{C}G$-modules R_ϱ upto equivalence, and $c(G)$ distinct irreducible characters of G upto equivalence. The collections of these are denoted by $Irrep(G)$, $Irr_{\mathbb{C}G}(G)$, $Irr(G)$, respectively. It holds that for any $\varrho, \varsigma \in Irrep(G)$, $\langle \chi_\varrho, \chi_\varsigma \rangle = \delta_{\varrho,\varsigma}$. We note the following result, [HUP1998].

Theorem 3.3 $\quad \langle \chi_{\mathbb{C}G}, \chi_\varrho \rangle = \chi_\varrho(1_G) = d_\varrho$, *for each* $\chi_\varrho \in Irr(G)$.

$\langle \chi_{\mathbb{C}G}, \chi_\varrho \rangle$ is the multiplicity of an $\varrho \in Irrep(G)$ in $\rho_{\mathbb{C}G}$, which we denote by $l_{\mathbb{C}G,\varrho}$, the above result states that every $\varrho \in Irrep(G)$ occurs in the regular representation $\rho_{\mathbb{C}G}$ exactly $l_{\mathbb{C}G,\varrho} = Dim\ \varrho = d_\varrho$ number of times, where $l_{\mathbb{C}G,\varrho} \geq 1$, since $d_\varrho \geq 1$. This means, equivalently, that every distinct irreducible $\mathbb{C}G$-module $R_\varrho \in Irr_{\mathbb{C}G}(G)$, and distinct irreducible character $\chi_\varrho \in Irr(G)$, occur in $\mathbb{C}G$ and $\chi_{\mathbb{C}G}$, respectively, all occur with positive multiplicity equal to $l_{\mathbb{C}G,\varrho} = d_\varrho$. The $\rho_{\mathbb{C}G}$, $\mathbb{C}G$, and $\chi_{\mathbb{C}G}$ decompose into a direct sum of *isotypic components* $\left\{ \bigoplus_{i_\varrho=1}^{d_\varrho} \varrho \mid \varrho \in Irrep(G) \right\}$, $\left\{ \bigoplus_{i_\varrho=1}^{d_\varrho} R_\varrho \mid \varrho \in Irrep(G) \right\}$, and $\left\{ \bigoplus_{i_\varrho=1}^{d_\varrho} \chi_\varrho \mid \varrho \in Irrep(G) \right\}$ respectively, in the following way:

(3.1) $\rho_{\mathbb{C}G} = \bigoplus_{\varrho \in Irrep(G)} d_\varrho \varrho = \bigoplus_{\varrho \in Irrep(G)} \bigoplus_{i_\varrho=1}^{d_\varrho} \varrho,$

(3.2) $\mathbb{C}G = \bigoplus_{\varrho \in Irrep(G)} d_\varrho R_\varrho = \bigoplus_{\varrho \in Irrep(G)} \bigoplus_{i_\varrho=1}^{d_\varrho} R_\varrho,$

(3.3) $\chi_{\mathbb{C}G} = \sum_{\varrho \in Irrep(G)} d_\varrho \chi_\varrho = \sum_{\varrho \in Irrep(G)} \sum_{i_\varrho=1}^{d_\varrho} \chi_\varrho.$

If we put $d_{\mathbb{C}G} = Dim\ \rho_{\mathbb{C}G} = Dim\ \mathbb{C}G = \chi_{\mathbb{C}G}(1_G)$, then we get:

(3.4) $d_{\mathbb{C}G} = |G| = \sum_{d_\varrho \in cd(G)} l_{\mathbb{C}G,\varrho} d_\varrho = \sum_{d_\varrho \in cd(G)} d_\varrho^2.$

This shows that $d_\varrho^2 \leq |G|$, for any $\varrho \in Irrep(G)$.

3.1.3 *Induced and Restricted Representations, $\mathbb{C}G$-Modules, and Characters*

A representation π of a group G, with target $\mathbb{C}G$-module V_π and character χ_π, is said to be an *induction* of a representation θ of a subgroup $H \leq G$ if $V_\pi = \underset{\kappa \,\epsilon\, G/H}{\oplus} W_\kappa$, where G/H stands for the set of $[G:H] = \frac{|G|}{|H|}$ distinct left G-cosets $\kappa = s_\kappa H$ of H with the $s_\kappa \,\epsilon\, G$ being their distinct coset representatives, $W_{1_G} \equiv W$ is a $Res^G_H\pi$-invariant subspace of V such that θ is the representation $\theta : H \longrightarrow GL(Dim\ W, \mathbb{C})$; $\{W_\kappa\}_{\kappa\,\epsilon\,G/H}$ is the set of $[G:H]$ distinct, $Dim\ W$-dimensional subspaces of V_π given by $W_\kappa = \pi(s_\kappa)(W)$, $\kappa \,\epsilon\, G/H$ [SER1977]. In this case, every $v \,\epsilon\, V_\pi$ has the form $\sum\limits_{\kappa\,\epsilon\,G/H,\ w_\kappa\,\epsilon\,W_\kappa} w_\kappa$; π is the direct sum $\pi = \underset{\kappa\,\epsilon\,G/H}{\oplus} \theta_\kappa$ of the subrepresentations θ_κ of G on the components W_κ of V_π of the form $g \longmapsto [g]_\kappa(w_\kappa)$, $\kappa \,\epsilon\, G/H$, $[g]_\kappa \,\epsilon\, GL(Dim\ W_\kappa, \mathbb{C})$; π is said to be induced by θ and denoted by $\pi = Ind^G_H\theta$; W becomes a $\mathbb{C}G$-module W_θ and a $\mathbb{C}G$-submodule of V_π; V_π is of dimension $[G:H] \cdot Dim\ W_\theta$ and is said to be induced by W_θ and denoted by $V_\pi = Ind^G_H W_\theta$. $Ind^G_H\theta$ will have the canonical decomposition $\underset{\varrho\,\epsilon\,Irrep(G)}{\oplus} l_{Ind^G_H\theta,\varrho}\varrho$, its character $\chi_{Ind^G_H\theta}$ will have the decomposition $\chi_{Ind^G_H\theta} = \sum\limits_{\varrho\,\epsilon\,Irrep(G)} l_{Ind^G_H\theta,\varrho}\chi_\varrho$, and dimension $d_{Ind^G_H\theta} = \sum\limits_{\varrho\,\epsilon\,Irrep(G)} l_{Ind^G_H\theta,\varrho} d_\varrho = [G:H] \cdot Dim\ W_\theta = \frac{|G|}{|H|} d_\theta$, where $l_{Ind^G_H\theta,\varrho} = \left\langle \chi_{Ind^G_H\theta}, \chi_\varrho \right\rangle$ are the multiplicities of the $\varrho \,\epsilon\, Irrep(G)$ in $Ind^G_H\theta$, not all simultaneously equal to 0 [SER1977]. The following proposition summarizes some elementary properties of dimensions of induced representations.

Proposition 3.4 *For any representation θ of a subgroup $H \leq G$: (1) $d_{Ind^G_H\theta} = \frac{|G|}{|H|} d_\theta$; for any $\varrho \,\epsilon\, Irrep(G)$, (2) $d_\varrho \mid d_{Ind^G_H\theta}$; (3) $d_\varrho = d_{Ind^G_H\theta}$ iff $l_{Ind^G_H\theta,\varsigma} = \delta_{\varsigma,\varrho}$ for all $\varsigma \,\epsilon\, Irrep(G)$, i.e. iff $Ind^G_H\theta$ is an irreducible representation of G equivalent to (or coinciding with) exactly one $\varrho \,\epsilon\, Irrep(G)$.*

A representation ξ of a subgroup $H \leq G$ is said to be the *restriction* of a representation π of G if $\xi(h) = \pi(h)$ for all $h \,\epsilon\, H$, and this is denoted by $\xi = Res^G_H\pi$, in which case the target $\mathbb{C}G$-module U_ξ of ξ is said to be a restriction of the $\mathbb{C}G$-module V_π of π denoted by $U_\xi = Res^G_H V_\pi$ [SER1977]. $Res^G_H\pi$ will have the canonical decomposition $\underset{\vartheta\,\epsilon\,Irrep(H)}{\oplus} l_{Res^G_H\pi,\vartheta}\vartheta$,

its character $\chi_{Res^G_H \pi}$ will have the decomposition $\chi_{Res^G_H \pi} = \sum_{\vartheta \,\epsilon\, Irrep(H)} l_{Res^G_H \pi, \vartheta} \chi_\vartheta$, and it will have the dimension $d_{Res^G_H \pi} = d_\pi = \sum_{\vartheta \,\epsilon\, Irrep(H)} l_{Res^G_H \pi, \vartheta} d_\vartheta$, where $l_{Res^G_H \pi, \vartheta} = \left\langle \chi_{Res^G_H \pi}, \chi_\vartheta \right\rangle$ are the nonnegative multiplicities of the $\vartheta \,\epsilon\, Irrep(H)$ in $Res^G_H \pi$, not all simultaneously equal to 0. The following proposition summarizes some elementary properties of dimensions of restricted representations.

Proposition 3.5 *For any representation π of $G \geq H$, (1) $d_\pi = d_{Res^G_H \pi}$; for any $\vartheta \,\epsilon\, Irrep(H)$, (2) $d_\vartheta \leq d_\pi$ if $l_{Res^G_H \pi, \vartheta} > 0$; (3) $d_\vartheta = d_\pi$ iff $l_{Res^G_H \pi, \varphi} = \delta_{\varphi, \vartheta}$ for all $\varphi \,\epsilon\, Irrep(H)$, i.e. iff $Res^G_H \pi$ is an irreducible representation of H equivalent to (coinciding with) exactly one $\vartheta \,\epsilon\, Irrep(H)$.*

The following is a famous theorem of Frobenius describing a reciprocity between induction and restriction of irreducible representations.

Theorem 3.6 *(Frobenius) For a subgroup $H \leq G$, and any $\vartheta \,\epsilon\, Irrep(H)$ and $\varrho \,\epsilon\, Irrep(G)$, $l_{Res^G_H \varrho, \vartheta} = l_{\varrho, Ind^G_H \vartheta}$.*

This is called the *Frobenius reciprocity law*, and in this thesis is useful in deriving information about size estimates relating to the dimensions of the distinct irreducible representations of groups.

3.1.4 *Irreducible Character Degrees*

Henceforth, let us denote by $cd(G)$ the set of degrees of the distinct irreducible characters of a finite group G. Formally:

(3.5) $cd(G) := \left\{ d_\varrho = \chi_\varrho(1_G) \mid \chi_\varrho \,\epsilon\, Irr(G),\, \varrho \,\epsilon\, Irrep(G) \right\}$.

We call $cd(G)$ the *character degree set* of G, where we know $|cd(G)| = |Irrep(G)| = c(G)$ holds. The following is a fundamental theorem about irreducible character degrees [HUP1998].

Theorem 3.7 *For any $d_\varrho \in cd(G)$, (1) d_ϱ divides $[G:A]$ where $[G:A]$ is the index of any maximal Abelian normal subgroup A of G (Itô), (2) d_ϱ divides $[G:Z(G)]$, where $Z(G)$ is the centre of G, and (3) d_ϱ divides $|G|$.*

(2) is a consequence of (1) since if ϱ is irreducible, then d_ϱ must divide $[G:Z(G)]$ where $Z(G) \leq A$ for some maximal Abelian normal subgroup A of G. (3) is a consequence of (2) since if ϱ is irreducible then $d_\varrho \mid [G:Z(G)]$ by (2) and therefore $d_\varrho \mid |G| = [G:Z(G)]\ [Z(G):1_G]$.

Let us consider the irreducible character degrees of finite Abelian groups. Until section *3.1.5* G will be a finite Abelian group. Then every conjugacy class g^G of every element $g \in G$ contains only g as its element, and therefore, there are in G exactly as many distinct conjugacy classes as there are elements, i.e. $|cd(G)| = c(G) = |G|$. Also, $Z(G) = G$, $[G:Z(G)] = 1$, and by *Theorem 3.7*, for any $d_\varrho \in cd(G)$, $d_\varrho \mid [G:G] = 1$, which means that $d_\varrho = 1$, i.e. the dimension of every irreducible representation and every irreducible $\mathbb{C}G$-module, and the degree of every irreducible character, of a finite Abelian group G is 1. Thus, the dimension d_π of an arbitrary representation π of G, and of its target $\mathbb{C}G$-module V_π, is given by $d_\pi = \sum_{\varrho \in Irrep(G)} \langle \chi_\pi, \chi_\varrho \rangle\, d_\varrho = \sum_{\varrho \in Irrep(G)} \langle \chi_\pi, \chi_\varrho \rangle = \sum_{\varrho \in Irrep(G)} l_{\pi,\varrho}$, i.e. the sum of the multiplicities of the irreducible components of π. For each $\varrho \in Irrep(G)$, and a given $g \in G$, the matrix $\varrho(g)$ of ϱ at g will be a 1×1 matrix given by $\big(\chi_\varrho(g)\big)$, and its character $\chi_\varrho \in Irr(G)$ will have an inverse χ_ϱ^{-1}, defined by $\chi_\varrho^{-1}(g) = \chi_\varrho\left(g^{-1}\right) = \overline{\chi_\varrho(g)}$, so that $\chi_\varrho^{-1} = \overline{\chi_\varrho}$; the character set $\widehat{G}$ will then form, under pointwise multiplication, a multiplicative Abelian group isomorphic to G, called its *dual* or *character group*.

3.1.5 *Estimates for Sums of Powers of Irreducible Character Degrees*

We derive here a number of estimates relating to sums of powers of irreducible character degrees of a finite group G, for which we introduce a map $D_r(G) : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ defined by:

(3.6) $$D_r(G) = \sum_{d_\varrho \in cd(G)} d_\varrho^r = \sum_{\varrho \in Irrep(G)} d_\varrho^r = \sum_{\chi_\varrho \in Irr(G)} \chi_\varrho(1_G)^r, \qquad r \geq 1.$$

$D_r(G)$ records the sum of the r^{th} powers of the distinct irreducible character degrees of G. For $r = 0$, $D_0(G) = c(G)$. For $t > 0$ the t^{th} power of $D_r(G)$ is given by $D_r(G)^t = \left(\sum_{d_\varrho \,\epsilon\, cd(G)} d_\varrho^r \right)^t$, $r \geq 1$, and we define $D_r(G)^0 := 1$. For $r = 2$, $t = 1$, *(3.6)* occurs as the case:

(3.7) $D_2(G) = \sum_{d_\varrho \,\epsilon\, cd(G)} d_\varrho^2 = |G| = \chi_{\mathbb{C}G}(1)$.

Every nontrivial group G has at least two distinct irreducible characters, each of degree ≥ 1, and there is always at least one $d_\varrho \,\epsilon\, cd(G)$ such that $d_\varrho = 1$, e.g. if $\varrho = \iota_1$. Therefore, $D_1(G)^r = \left(\sum_{d_\varrho \,\epsilon\, cd(G)} d_\varrho \right)^r$ contains all terms d_ϱ^r of $D_r(G)$ besides other cross-product terms ≥ 1. Therefore:

(3.8) $D_r(G) \leq D_1(G)^r, \qquad r \geq 1.$

Similarly the sum product $D_r(G)D_s(G) = \sum_{d_\varrho \,\epsilon\, cd(G)} d_\varrho^r \sum_{d_\varsigma \,\epsilon\, cd(G)} d_\varsigma^s$ contains all terms d_ϱ^r and d_ς^s of $D_r(G)$ and $D_s(G)$ respectively, besides other cross-product terms ≥ 1, and therefore

(3.9) $D_{r+s}(G) \leq D_r(G)D_s(G), \qquad r, s \geq 1.$

From *(3.9)* we can write the following.

(3.10) $D_r(G) \leq D_2(G)D_{r-2}(G) = |G|\, D_{r-2}(G), \qquad r \geq 2.$

For a fixed group G, $D_r(G)$ is a convex function of the inverse $\frac{1}{r}$ of the index $r \geq 1$, meaning that:

(3.11) $D_s(G)^{1/s} \leq D_r(G)^{1/r}, \qquad 1 \leq r \leq s.$

There is a useful monotonicity result for sums of powers of irreducible character degrees of subgroups.

Lemma 3.8 *For any subgroup $H \leq G$, $D_r(H) \leq D_r(G)$, and $D_r(H) < D_r(G)$ iff $H < G$, for all real $r \geq 1$.*

Proof. For any $\varrho \in Irrep(G)$ and $\vartheta \in Irrep(H)$, by Frobenius reciprocity (*Theorem 3.6*), $l_{Ind_H^G \vartheta,\varrho} = l_{Res_H^G \varrho,\vartheta}$, and, further, by *Proposition 3.5*, $d_\vartheta \leq d_\varrho$ if $l_{Ind_H^G \vartheta,\varrho} = l_{Res_H^G \varrho,\vartheta} > 0$. Fixing a $\varrho \in Irrep(G)$, we have:

$$\sum_{\vartheta \in Irrep(H),\, l_{Ind_H^G \vartheta,\varrho}>0} d_\vartheta = \sum_{\vartheta \in Irrep(H),\, l_{Res_H^G \varrho,\vartheta}>0} d_\vartheta \leq \sum_{\vartheta \in Irrep(H)} l_{Res_H^G \varrho,\vartheta} d_\vartheta = d_{Res_H^G \varrho} = d_\varrho.$$

Taking r^{th} powers in the above estimate, for $r \geq 1$, by the reasoning in *(3.11),* we obtain:

$$\sum_{\vartheta \in Irrep(H),\, l_{Res_H^G \varrho,\vartheta}>0} d_\vartheta^r \leq \left(\sum_{\vartheta \in Irrep(H),\, l_{Res_H^G \varrho,\vartheta}>0} d_\vartheta \right)^r \leq \left(\sum_{\vartheta \in Irrep(H)} l_{Res_H^G \varrho,\vartheta} d_\vartheta \right)^r = d_\varrho^r.$$

If, in the above estimate, we sum over all $\varrho \in Irrep(G)$ and omit the intermediate sums, we obtain:

$$\sum_{\varrho \in Irrep(G)} \sum_{\vartheta \in Irrep(H),\, l_{Res_H^G \varrho,\vartheta}>0} d_\vartheta^r \leq \sum_{\varrho \in Irrep(G)} d_\varrho^r = D_r(G).$$

Since $\sum_{\vartheta \in Irrep(H)} d_\vartheta^r \leq \sum_{\varrho \in Irrep(G)} \sum_{\vartheta \in Irrep(H),\, l_{Res_H^G \varrho,\vartheta}>0} d_\vartheta^r$, we obtain the estimate:

$$D_r(H) = \sum_{\vartheta \in Irrep(H)} d_\vartheta^r \leq \sum_{\varrho \in Irrep(G)} \sum_{\vartheta \in Irrep(H),\, l_{Res_H^G \varrho,\vartheta}>0} d_\vartheta^r \leq \sum_{\varrho \in Irrep(G)} d_\varrho^r = D_r(G).$$

This proves the first part of our claim. For the second part, we note that $H = G$ implies that $D_r(H) = D_r(G)$. If $H < G$, i.e. is a proper subgroup of G, then $H \subset G$ and $|H| < |G|$, and $D_1(H) < D_1(G)$ (proof left to the reader), and using the first part, it can easily be seen that $D_r(H) < D_r(G)$ for all $r > 1$. ■

3.1.6 *Estimates for Maximal Irreducible Character Degrees*

Here, we derive lower and upper estimates for the maximal irreducible character degree d' of a finite group G with character degree set $cd(G)$. First, we note that *(3.10)* may be

sharpened further using $d^{'}$. By definition, $d \leq d^{'}$ for all $d \epsilon cd(G)$, so that for $r \geq 2$, $D_r(G) = \sum_{d_\varrho \epsilon cd(G)} d_\varrho^r = \sum_{d_\varrho \epsilon cd(G)} d_\varrho^{r-2} d_\varrho^2 \leq d^{'r-2} \cdot \sum_{d_\varrho \epsilon cd(G)} d_\varrho^2 = d^{'r-2} D_2(G) = d^{'r-2} |G|$. We record this for later use:

(3.12) $D_r(G) \leq d^{'r-2} D_2(G) = d^{'r-2} |G|, \qquad r \geq 2.$

For convenience, we denote $c(G)$ by c. For each $d_\varrho \epsilon cd(G)$ we know that $d_\varrho \mid |G|$ and $1 \leq d_\varrho^2 \leq |G|$, and therefore, that there is an integer $0 \leq e_\varrho = |G| - d_\varrho^2$ such that $d_\varrho^2 + e_\varrho = |G|$, i.e. that $d_\varrho = (|G| - e_\varrho)^{1/2}$. We denote by ι_1 the trivial irreducible representation of G of dimension $d_{\iota_1} = 1$, so that $e_{\iota_1} = |G| - d_{\iota_1}^2 = |G| - 1$. If $e_\varrho = |G| - d_\varrho^2 = 0$ for any $d_\varrho \epsilon cd(G)$ then $|G| = d_\varrho^2$ and G has only the one irreducible representation $\varrho = \iota_1$, which is true iff G is trivial. Thus G is nontrivial iff all the $e_\varrho \geq 1$. If we let $e^{'} = |G| - d^{'2}$ then $1 \leq d^{'} = \left(|G| - e^{'}\right)^{1/2} \leq (|G| - 1)^{1/2}$. The case $d^{'} = 1$ means that $d_\varrho = 1$ for all $d_\varrho \epsilon cd(G)$, which is true iff G is Abelian. We have $d^{'} \geq 2$ whenever G is non-Abelian. The case $e^{'} = 1 \Longleftrightarrow d^{'} = (|G| - 1)^{1/2} \geq 1$, is exceptional: this forces $|G| = \sum_{d_\varrho \epsilon cd(G)} d_\varrho^2$ to be the sum $|G| = d^{'2} + d_{\iota_1}^2 = d^{'2} + 1$, where $d^{'} = Dim\ \varrho^{'}$ for some $\varrho^{'} \epsilon Irrep(G)$ of maximal dimension. However, since $d^{'} \mid |G|$, it must be that $d^{'} \mid 1$, which means that $d^{'} = 1$, $|G| = 2$, G must be a cyclic group of order 2. Thus, $d^{'} = (|G| - 1)^{1/2} \geq 1$ can occur only for $d^{'} = 1$ with G cyclic of order 2. Thus, the case $2 \leq d^{'} < (|G| - 1)^{1/2}$ holds iff G is a non-Abelian group, which shows that $e^{'} = 2 \leq d^{'} < (|G| - 1)^{1/2}$ implies that $|G| \geq 6$. The case $1 = d^{'} < (|G| - 1)^{1/2}$ is true iff G is an Abelian group of order > 2.

Now we turn to the lower estimate for $d^{'}$, for which 1 is always a trivial value. A tighter lower bound may easily be obtained as follows. By definition, $d_\varrho \leq d^{'}$ for all $d_\varrho \epsilon cd(G)$. Then, since $|G| = D_2(G) = \sum_{d_\varrho \epsilon cd(G)} d_\varrho^2 \leq \sum_{d_\varrho \epsilon cd(G)} d^{'2} = d^{'2} \cdot \sum_{d_\varrho \epsilon cd(G)} 1 = cd^{'2}$, we have that $d^{'} \geq \left(\frac{|G|}{c}\right)^{1/2}$, where $1 \leq c \leq |G|$. We consider necessary and sufficient conditions for G such that $d^{'}$ reaches the lower bound $\left(\frac{|G|}{c}\right)^{1/2}$ exactly. The case $d^{'} = \left(\frac{|G|}{c}\right)^{1/2}$ is equivalent to the case $|G| = \sum_{d_\varrho \epsilon cd(G)} d_\varrho^2 = cd^{'2}$, and since $1 \leq c \leq |G|$, this can only occur iff all $d_\varrho = d^{'} = 1$, which is true iff G is Abelian. Thus, when G is Abelian, $\left(\frac{|G|}{c}\right)^{1/2} = 1 = d^{'} \leq (|G| - 1)^{1/2}$, with

an additional equality on the right iff G is cyclic of order 2. This shows that $\left(\frac{|G|}{c}\right)^{1/2} = 1 = d^{'} < (|G|-1)^{1/2}$ iff G is Abelian of order > 2. The case $d^{'} = \left(\frac{|G|}{c}\right)^{1/2} \geq 2$, with G Abelian, is impossible, since G always has the trivial irreducible character χ_{ι_1} of degree $d_{\iota_1} = 1$, so that $|G| = d_{\iota_1}^2 + \sum_{d_\varrho \,\epsilon\, cd(G)\setminus d_{\iota_1}} d_\varrho^2 \neq cd^{'2}$. Thus, $\left(\frac{|G|}{c}\right)^{1/2} < d^{'}$ iff G is non-Abelian, which is true iff $d^{'} \geq 2$, in which case $1 < c < |G|$ and $1 < \left(\frac{|G|}{c}\right)^{1/2}$ also. Thus, $1 < \left(\frac{|G|}{c}\right)^{1/2} < d^{'} < (|G|-1)^{1/2}$ holds iff G is non-Abelian, and implies that $|G| \geq 6$. Thus, we have proved the following result.

Theorem 3.9 *For a nontrivial finite group G with a maximal irreducible character degree $d^{'}(G)$ and class number $c(G)$ it holds that*

(1) $\quad 1 \leq \left(\frac{\lvert G\rvert}{c(G)}\right)^{1/2} \leq d^{'}(G) \leq (\lvert G\rvert - 1)^{1/2}$	*general case*
(2) $\quad 1 = \left(\frac{\lvert G\rvert}{c(G)}\right)^{1/2} = d^{'}(G) \leq (\lvert G\rvert - 1)^{1/2}$	*iff G is Abelian*
(3) $\quad 1 = \left(\frac{\lvert G\rvert}{c(G)}\right)^{1/2} = d^{'}(G) = (\lvert G\rvert - 1)^{1/2}$	*iff G is cyclic of order $\lvert G\rvert = 2$*
(4) $\quad 1 = \left(\frac{\lvert G\rvert}{c(G)}\right)^{1/2} = d^{'}(G) < (\lvert G\rvert - 1)^{1/2}$	*iff G is Abelian of order $\lvert G\rvert > 2$*
(5) $\quad 1 < \left(\frac{\lvert G\rvert}{c(G)}\right)^{1/2} < d^{'}(G) < (\lvert G\rvert - 1)^{1/2}$	*iff G is non-Abelian ($\Longrightarrow \lvert G\rvert \geq 6$)*

(Note: (2) − (4) are trivial.)

From the upper bound for $d^{'}(G)$ and the estimate *(3.12)*, we obtain the estimate:

(3.13) $D_r(G) \leq |G|\,(|G|-1)^{\frac{r-2}{2}}$, for all $r \geq 2$.

3.2 Regular Group Algebras

3.2.1 *Canonical Decomposition*

Our main reference here is [BCS1997]. The $\varrho \,\epsilon\, Irrep(G)$ linearly extend to injective ($\mathbb{C}$-algebra) homomorphisms $\mathcal{F}_\varrho : \mathbb{C}G \longrightarrow \mathbb{C}^{d_\varrho \times d_\varrho}$ of dimensions $Dim\ \mathcal{F}_\varrho = d_\varrho$ defined by:

(3.14) $f \equiv \sum_{g \,\epsilon\, G} f(g)g \longmapsto \mathcal{F}_\varrho(f) = \sum_{g \,\epsilon\, G} f(g)\varrho(g) \equiv \widehat{f}(\varrho), \qquad f \,\epsilon\, \mathbb{C}G,\ \varrho \,\epsilon\, Irrep(G).$

By the irreducibility of the $\varrho \,\epsilon\, Irrep(G)$ the $\mathcal{F}_\varrho$ define distinct irreducible matrix representations of $\mathbb{C}G$, and form a complete set $Irrep(\mathbb{C}G)$ of such representations. The direct sum homomorphism $\mathcal{F} = \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathcal{F}_\varrho : \mathbb{C}G \longrightarrow \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathbb{C}^{d_\varrho \times d_\varrho}$ of dimension $|G| = \sum_{\varrho \,\epsilon\, Irrep(G)} d_\varrho^2$ defined by:

(3.15) $f \equiv \sum_{g \,\epsilon\, G} f(g)g \longmapsto \widehat{f} \equiv \mathcal{F}(f) = \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \sum_{g \,\epsilon\, G} f(g)\varrho(g) = \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \widehat{f}(\varrho), \qquad f \,\epsilon\, \mathbb{C}G,$

is injective and surjective, and, therefore, the isomorphism:

(3.16) $\mathcal{F} = \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathcal{F}_\varrho : \mathbb{C}G \cong_{\mathbb{C}} \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \mathbb{C}^{d_\varrho \times d_\varrho}.$

This results in Wedderburn's theorem about the canonical decomposition of $\mathbb{C}G$ as an isomorphic direct sum of $c(G)$ complex matrix algebras of orders the $c(G)$ distinct irreducible character degrees d_ϱ of G. Taking dimensions on both sides of *(3.16)* this gives us another version of *(3.4)*. The matrix algebra on the right of *(3.16)*, whose elements are block-diagonal matrices, is called the *target algebra* of $\mathbb{C}G$. Iff G is Abelian all its irreducible character degrees will be of size 1, the matrices of the target algebra of its regular algebra $\mathbb{C}G$ will be diagonal of order $|G|$, and multiplication in $\mathbb{C}G$ will be pointwise and equal in complexity to that of diagonal matrix multiplication of order $|G|$.

3.2.2 *Multiplicative Complexity and Rank*

The (bilinear) multiplication maps of isomorphic $\mathbb{C}$-algebras are isomorphic, in the sense of *Corollary 2.3*, which is also true for algebras, and by *(3.16)*, we have:

(3.17) $\mathfrak{m}_{\mathbb{C}G} \cong_{\mathbb{C}} \bigoplus_{\varrho \,\epsilon\, Irrep(G)} \langle d_\varrho, d_\varrho, d_\varrho \rangle\,,$

where these are the multiplication maps of $\mathbb{C}G$ and its target algebra, respectively. The rank of $\mathbb{C}G$ is defined to be rank $\mathfrak{R}(\mathfrak{m}_{\mathbb{C}G})$ of its bilinear multiplication map $\mathfrak{m}_{\mathbb{C}G} : \mathbb{C}G \times \mathbb{C}G \longrightarrow \mathbb{C}G$, which is defined to be the length of the minimal bilinear computation needed to express the product of any two elements of $\mathbb{C}G$ (see section *2.1.2* in *Chapter 2*), and, therefore, cannot be less than $Dim\ \mathbb{C}G = |G|$. But, $|G|$ is also simultaneously the rank $\mathfrak{R}_{|G|}$ and the dimension of the vector space $\mathbb{C}^{|G|}$ which forms an algebra under pointwise vector multiplication. Thus, we have the relation:

(3.18) $$\mathfrak{R}_{|G|} = |G| \leq \mathfrak{R}(\mathfrak{m}_{\mathbb{C}G}) = \mathfrak{R}\left(\bigoplus_{\varrho\ \epsilon\ Irrep(G)} \langle d_\varrho, d_\varrho, d_\varrho \rangle\right) \leq \sum_{\varrho\ \epsilon\ Irrep(G)} \mathfrak{R}\left(\langle d_\varrho, d_\varrho, d_\varrho \rangle\right).$$

Equality above holds as $|G| = \mathfrak{R}(\mathfrak{m}_{\mathbb{C}G}) = \sum_{\varrho\ \epsilon\ Irrep(G)} \mathfrak{R}\left(\langle 1, 1, 1 \rangle\right) = \sum_{\varrho\ \epsilon\ Irrep(G)} \mathfrak{R}\left(\langle d_\varrho, d_\varrho, d_\varrho \rangle\right)$ iff G is Abelian.

3.3 Generalized Group Discrete Fourier Transforms

3.3.1 *Generalized Group Discrete Fourier Transforms*

Any $\mathbb{C}$-algebra isomorphism $\mathcal{F}$ of the form *(3.16)* is called a *generalized discrete Fourier transform* (DFT) on $\mathbb{C}G$, equivalently, a *generalized group discrete Fourier transform* on G, and defines a $|G|$-dimensional matrix representation of $\mathbb{C}G$ on its target algebra also of dimension $|G|$, where $\mathbb{C}G$ is called the *time domain* of $\mathcal{F}$ and the target algebra $\bigoplus_{\varrho\ \epsilon\ Irrep(G)} \mathbb{C}^{d_\varrho \times d_\varrho}$ is called its *frequency space* or *Fourier domain* [BCS1997, p. 327]. $\mathcal{F}$ is of dimension $Dim\ \mathcal{F} = |G|$, and has an invertible $|G| \times |G|$ block-diagonal matrix of full rank $|G|$ denoted by $[\mathcal{F}]$, called a DFT matrix for $\mathbb{C}G$, w.r.t. any fixed bases of $\mathbb{C}G$ - e.g. its regular basis G - and of its target algebra. Every choice of such distinct basis pairs yields a distinct DFT and a DFT matrix for $\mathbb{C}G$. Any DFT $\mathcal{F}$ on $\mathbb{C}G$ has a unique direct sum decomposition $\bigoplus_{\varrho\ \epsilon\ Irrep(G)} \mathcal{F}_\varrho$, where the $\mathcal{F}_\varrho$ are the irreducible components of $\mathcal{F}$ in *(3.16)*, with each $\mathcal{F}_\varrho$ faithfully mapping $\mathbb{C}G$ onto $\mathbb{C}^{d_\varrho \times d_\varrho}$. Given a DFT $\mathcal{F}$ on $\mathbb{C}G$, for an $f\ \epsilon\ \mathbb{C}G$, $\mathcal{F}(f) \equiv \widehat{f}$ is called the Fourier transform of f, for a fixed $\varrho\ \epsilon\ Irrep(G)$, $\widehat{f}(\varrho)$ defined by the formula *(3.14)* is called the Fourier transform of f

at ϱ, and the elements of $\left\{\widehat{f}(\varrho)\right\}_{\varrho \epsilon Irrep(G)}$ are called the Fourier coefficients of f which define $\widehat{f}$. There is an inversion formula for recovering f from its transform [SER1977].

(3.19) $f(g) = |G|^{-1} \sum_{\varrho \epsilon Irrep(G)} d_\varrho \cdot Tr\left[\widehat{f}(\varrho)\varrho(g^{-1})\right], \qquad g \epsilon G.$

This formula defines the inverse DFT of an $f \epsilon \mathbb{C}G$. If G is Abelian all the $d_\varrho = 1$, so that the 1-dimensional $\varrho \epsilon Irrep(G)$ may be replaced, in *(3.14)* and *(3.21)*, by their irreducible characters χ_ϱ, all of degree 1. This yields the familiar Fourier transform and inverse transform formulas for finite Abelian groups [SER1977].

(3.20) $\widehat{f}(\chi_\varrho) = \sum_{g \epsilon G} f(g)\chi_\varrho(g), \qquad \varrho \epsilon Irrep(G),$

(3.21) $f(g) = |G|^{-1} \sum_{\varrho \epsilon Irrep(G)} \widehat{f}(\chi_\varrho)\overline{\chi_\varrho(g)}, \qquad g \epsilon G.$

A DFT $\mathcal{F}$ on $\mathbb{C}G$ has an invertible matrix $[\mathcal{F}]$ of order $|G|$, whose columns correspond to the group elements $g \epsilon G$, and whose rows correspond to the distinct irreducible representations $\varrho \epsilon Irrep(G)$. For any $g \epsilon G$ and any $\varrho \epsilon Irrep(G)$, $\varrho(g)$ is an invertible matrix of order d_ϱ indexed by $1 \leq k_\varrho, l_\varrho \leq d_\varrho$, whose d_ϱ^2 number of entries $\varrho(g)_{k_\varrho, l_\varrho}$ occur in $[\mathcal{F}]$ by the following formula [SER1977].

(3.22) $[\mathcal{F}]_{\varrho, k_\varrho, l_\varrho; g} = \varrho(g)_{k_\varrho, l_\varrho}.$

Every choice of basis pairs in $\mathbb{C}G$ and its target algebra yields a distinct DFT $\mathcal{F}$ and a DFT matrix $[\mathcal{F}]$ for $\mathbb{C}G$, and the class $\{[\mathcal{F}]\}$ of all DFT matrices $[\mathcal{F}]$ for $\mathbb{C}G$ is determined uniquely by the $\varrho \epsilon Irrep(G)$.

3.3.2 *Discrete Fourier Transform on* Sym_3

Here we present the example of [BCS1997, pp. 329-330]. Consider Sym_3, the symmetric group of all permutations of 3 symbols. The 6 permutation elements of Sym_3 are the identity permutation (1), the three transpositions (12), (13), and (23), and the two cycles (123) and (132), and these three subsets of elements form the three distinct conjugacy classes C_e, C_t, and C_c, respectively, of D_3, where e denotes the no-change permutation, t denotes a transposition, and c a 3-cycle. Sym_3 has the trivial 1-dimensional irreducible representation ι corresponding to e, which is defined by $g \longmapsto (1)$, the nontrivial 1-dimensional irreducible representation σ corresponding to t, which is defined by $g \longmapsto sgn(g)$, and the 2-dimensional irreducible representation Δ which is defined explicitly by the mappings: $(1) \longmapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $(12) \longmapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $(13) \longmapsto \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}$, $(23) \longmapsto \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}$, $(123) \longmapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$, $(132) \longmapsto \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$. The distinct irreducible character degrees of Sym_3 are $d_\iota = 1$, $d_\sigma = 1$, and $d_\Delta = 2$, such that $d_\iota^2 + d_\sigma^2 + d_\Delta^2 = 6$. By *(3.16)* the regular group algebra $\mathbb{C}Sym_3$ of Sym_3 then has the canonical decomposition $\mathbb{C}Sym_3 \cong_{\mathbb{C}} \mathbb{C}^{d_\iota \times d_\iota} \oplus \mathbb{C}^{d_\sigma \times d_\sigma} \oplus \mathbb{C}^{d_\Delta \times d_\Delta} = \mathbb{C}^{1\times 1} \oplus \mathbb{C}^{1\times 1} \oplus \mathbb{C}^{2\times 2}$. The DFT matrix $[\mathcal{F}]$ for $\mathbb{C}Sym_3$, w.r.t. canonical bases in the components of its target algebra, by formula *(3.24)*, will be the 6×6 matrix:

$$\begin{array}{c} \\ \iota_{1,1} \\ \sigma_{1,1} \\ \Delta_{1,1} \\ \Delta_{1,2} \\ \Delta_{2,1} \\ \Delta_{2,2} \end{array} \begin{array}{c} \begin{array}{cccccc} (1) & (12) & (13) & (23) & (123) & (132) \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 0 & -1 & 0 & 1 & -1 \\ 0 & -1 & 1 & 1 & -1 & 0 \\ 1 & 1 & -1 & 1 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 & 1 \end{bmatrix} \end{array}.$$

We see that formula *(3.24)* prescribes that the entries of the column corresponding to a $g \in Sym_3$ are the coefficients of the linear forms obtained from the entries of the matrices $\iota(g)$, $\sigma(g)$, and $\Delta(g)$.

3.3.3 *Complexity and Fast Fourier Transform (FFT) Algorithms*

For a given finite group G with regular group algebra $\mathbb{C}G$, we can think about *a* discrete Fourier transform $\mathcal{F}$ on G as a linear transformation defined by $DFT(f) = \widehat{f}$ for any given $f \in \mathbb{C}G$, where $\widehat{f}$ is a matrix valued function on $Irrep(G)$, e.g. $\widehat{f}(\varrho) \in \mathbb{C}^{d_\varrho \times d_\varrho}$ for any $\varrho \in Irrep(G)$. We see that a DFT on G is described by the product of a $|G| \times |G|$ matrix by a vector of length $|G|$. If we write $M_{\mathcal{F}}(G)$ as the total number of arithmetical operations $\{\times, +, -\}$ required to implement a given group DFT $\mathcal{F}$ on G, then we see that

(3.23) $|G| \leq M_{\mathcal{F}}(G) \leq 2|G|^2$.

An *efficient* group DFT algorithm, also called a *fast Fourier transform* (FFT), is one which minimizes $M_{\mathcal{F}}(G)$ for *any* given Fourier transform $\mathcal{F}$, i.e. by reducing the upper limit $2|G|^2$. The famous Cooley-Tukey algorithm is an FFT to compute the DFT on the cyclic group $\mathbb{Z}/n\mathbb{Z}$ in $M_{\mathcal{F}}(\mathbb{Z}/n\mathbb{Z}) = O(n \log n)$ operations [MR2003, p. 283]. It is out of the scope of this thesis to discuss the FFTs on groups further, but we will conclude by noting that according to Maslen and Rockmore, who present an up-to-date survey of the field, $M_{\mathcal{F}}(G) \leq O(|G| \log |G|)$ holds for all Abelian groups G, and for arbitrary groups G they conjecture that there are constants C_1 and C_2 such that $M_{\mathcal{F}}(G) \leq C_1 |G| \log^{C_2} |G|$, [MR2003, p. 286]. This was perhaps suggested by the discovery for symmetric groups Sym_n that $M_{\mathcal{F}}(Sym_n) = O\left(n! \log^2 n!\right)$ [MR2003, p. 286].

Chapter 4

Groups and Matrix Multiplication I

Here we introduce the basic group-theoretic approach of embedding matrices into group algebras via triples of subsets of the groups having the so-called triple product property, and studying the complexity of matrix multiplication in terms of certain numerical parameters relating to the size of groups, the degrees of their irreducible characters, and the sizes of the matrix multiplications realized by them. The methods discussed here pertain to the group algebra embedding of a *single* arbitrary pair of matrices, and the recovery of their product via multiplication in the group algebra, while in the sequel to this chapter, *Chapter 5*, we describe methods for the *simultaneous* embedding into a group algebra of several pairs of matrices, and recovering their independent products simultaneously via a single multiplication in the algebra. In the concluding part *4.3* of the chapter, we describe a number of ways of proving estimates for ω using the methods outlined earlier.

4.1 Realizing Matrix Multiplication via Groups

4.1.1 *Groups and Index Triples*

Henceforth, G shall always denote a *nontrivial*, *finite* group. For any nonempty subset $S \subseteq G$ its right-quotient set, denoted by $Q(S)$, is defined as:

(4.1) $Q(S) := \Big\{ s's^{-1} \mid s, s' \in S \Big\}$.

By the definition above, $1_G \epsilon Q(S)$ necessarily for all right-quotient sets of subsets S of G. The relation

(4.2) $|Q(S)| \geq |S|$

is a simple consequence of *(4.1)* since a fixed $s \epsilon S$ the elements $s^{'}s^{-1}$, for arbitrary $s^{'} \epsilon S$, are distinct elements of S. Equality in *(4.2)* always holds for any subgroup $S \leq G$.

A triple (S, T, U) of nonempty subsets $S, T, U \subseteq G$ is said to have the *triple product property* (TPP) if the following condition holds.

(4.3) $s^{'}s^{-1}t^{'}t^{-1}u^{'}u^{-1} = 1_G \Longleftrightarrow s^{'}s^{-1} = t^{'}t^{-1} = u^{'}u^{-1} = 1_G, \qquad s^{'}s^{-1} \epsilon Q(S),\ t^{'}t^{-1} \epsilon Q(T),$
$u^{'}u^{-1} \epsilon Q(U).$

A subset triple (S, T, U) of G which has the triple product property is called an *index triple* of G, for which we can derive an elementary property.

Corollary 4.1 *If (S, T, U) is an index triple of G then the mapping $(x, y) \longmapsto x^{-1}y$ on any distinct pair $X, Y \epsilon \{S,\ T,\ U\}$ is injective.*

Proof. Since $S, T, U \subseteq G$, by assumption, satisfy the triple product property, for arbitrary $s, s^{'} \epsilon S$, $t, t^{'} \epsilon T$, $u, u^{'} \epsilon U$, it is the case that $s^{'}s^{-1}t^{'}t^{-1}u^{'}u^{-1} = 1_G \Longleftrightarrow s^{'} = s,\ t^{'} = t,\ u^{'} = u$. Then for arbitrary elements $s, s^{'} \epsilon S$ and $t, t^{'} \epsilon T$, $u, u^{'} \epsilon U$, we see that

$$\begin{aligned} s^{-1}t \quad &= \quad s^{'-1}t^{'} \\ &\Longrightarrow \quad s^{'}s^{-1}tt^{'-1}uu^{'-1} = 1 \\ &\Longrightarrow \quad s^{'} = s,\ t^{'} = t. \end{aligned}$$

We can prove, in the same way, the injectivity of this mapping for all other distinct pairs in $\{S,\ T,\ U\}$. ■

For any triple of subgroups S, T, $U \leq G$ the triple product property condition may be expressed as: $stu = 1_G$ iff $s = t = u = 1_G$, $s \in S$, $t \in T$, $u \in U$, since $Q(S) = S$, $Q(T) = T$, $Q(U) = U$ iff $S, T, U \leq G$.

The following is a trivial result.

Lemma 4.2 *If G is any group then* (1) $G, \{1_G\}, \{1_G\}$ *is a triple of subroups having the triple product property, and* (2) $G \times \{1_G\} \times \{1_G\}, \{1_G\} \times G \times \{1_G\}, \{1_G\} \times \{1_G\} \times G$ *is a triple of subgroups having the triple product property in $G^{\times 3}$.*

For Abelian groups there is an equivalent characterization of the triple product property by maps, as expressed in the following lemma.

Lemma 4.3 *If G is Abelian, then (S, T, U) is an index triple of G iff the triple product map $\psi : S \times T \times U \longrightarrow G$, defined by $(s, t, u) \longmapsto stu$, is injective.*

Proof. Let G be Abelian. If subsets S, T, $U \subseteq G$ satisfy the triple product property, then for any two elements (s, t, u), $(s', t', u') \in S \times T \times U$:

$$\begin{aligned} \psi(s', t', u') &= s't'u' = stu = \psi(s, t, u) \\ &\Longrightarrow s's^{-1}t't^{-1}u'u^{-1} = 1_G \\ &\Longleftrightarrow s's^{-1} = 1_G,\ t't^{-1} = 1_G,\ u'u^{-1} = 1_G \\ &\Longrightarrow (s', t', u') = (s, t, u). \end{aligned}$$

The converse is also true. If ψ is injective on $S \times T \times U$ then for any two elements (s, t, u), $(s', t', u') \in S \times T \times U$:

$$\begin{aligned} s's^{-1}t't^{-1}u'u^{-1} &= 1_G \\ &\Longrightarrow s't'u' = stu \\ &\Longleftrightarrow \left(s', t', u'\right) = (s, t, u) \\ &\Longrightarrow s's^{-1} = 1_G,\ t't^{-1} = 1_G,\ u'u^{-1} = 1_G. \end{aligned}$$

■

The following is an elementary corollary:

Corollary 4.4 *If G is Abelian and (S,T,U) is an index triple of G, then $|S|\,|T|\,|U| \leq |G|$. Equivalently, if (S,T,U) is an index triple of G such that $|S|\,|T|\,|U| > |G|$ then G is non-Abelian.*

Proof. By *Lemma 4.3,* the triple product map ψ on an index triple (S,T,U) of an Abelian group G is necessarily injective and, therefore, $S \times T \times U \cong \operatorname{Im}\psi \subseteq G$. Taking cardinalities on either side, we have that $|S \times T \times U| = |S|\,|T|\,|U| \leq |G|$. The equivalent statement follows from the negation of the previous statement. ■

The property of G having an index triple is invariant under permutations of the components of the triple.

Lemma 4.5 *A subset triple (S,T,U) is an index triple of G iff any permuted triple $(\mu(S),\mu(T),\mu(U))$ is an index triple of G, for a permutation $\mu \in Sym\{S,T,U\}$.*

Proof. Assume (S,T,U) has the triple product property. Then, for all $s's^{-1} \in Q(S)$, $t't^{-1} \in Q(T)$, $u'u^{-1} \in Q(U)$

$$\begin{aligned} t't^{-1}s's^{-1}u'u^{-1} &= 1_G \\ &\Longrightarrow\ s's^{-1}t't^{-1}u'u^{-1} = 1_G \\ &\Longrightarrow\ s's^{-1} = t't^{-1} = u'u^{-1} = 1_G. \end{aligned}$$

This shows that (T,S,U) has the triple product property if (S,T,U) does, and in the same way, we can show that (S,U,T) has the triple product property, and so do all other permuted triples (T,U,S), (U,S,T), (U,T,S), because (T,S,U) and (S,U,T) generate the permutation group $Sym\{S,T,U\}$. ■

4.1.2 *Extension Results for Index Triples*

We start with a basic statement about index triples of subgroups.

Proposition 4.6 *If (S,T,U) is an index triple of a subgroup $H \leq G$ then (S,T,U) is an index triple of G.*

This follows from the definition *(4.3)* of an index triple of G. Index triples of groups can also be obtained as extensions of index triples.of normal subgroups and of their corresponding factor groups.

Lemma 4.7 *If (S_1,S_2,S_3) is an index triple of $H \lhd G$ and (U_1,U_2,U_3) is an index triple of G/H, then there exists a subset triple (T_1,T_2,T_3) of G, corresponding to (U_1,U_2,U_3), such that the pointwise product triple (S_1T_1, S_2T_2, S_3T_3) is an index triple of G, where the $T_i \subseteq G$ are lifts to G of the U_i.*

Proof. Elements of G/H are left-cosets gH of H in G, the subsets U_1, U_2, $U_3 \subseteq G/H$ are of form

$$U_i = \{u_i = v_iH \mid v_i \,\epsilon\, G\}, \qquad 1 \leq i \leq 3.$$

We define *lift* subsets $T_i \subseteq G$ of the U_i by

$$T_i = \{t_i \,\epsilon\, G |\ t_i = v_ih_i, \text{ some } h_i \,\epsilon\, H, \text{ and } u_i = v_iH \,\epsilon\, U_i, \text{ some } v_i \,\epsilon\, G\}, \qquad 1 \leq i \leq 3.$$

The T_i, which are not necessarily unique for the U_i, have the properties that (1) $t_iH = u_i$, for all $t_i \,\epsilon\, T_i$ and $u_i \,\epsilon\, U_i$, (2) $U_i \cong T_i$, and (3) $t \,\epsilon\, T_i$ implies $T_i \cap tH = \{t\}$, $1 \leq i \leq 3$. Let $s_1, s_1^{'} \,\epsilon\, S_1, t_1, t_1^{'} \,\epsilon\, T_1, u_1, u_1^{'} \,\epsilon\, U_1$, and $s_2, s_2^{'} \,\epsilon\, S_2, t_2, t_2^{'} \,\epsilon\, T_2, u_2, u_2^{'} \,\epsilon\, U_2$, and $s_3, s_3^{'} \,\epsilon\, S_3, t_3, t_3^{'} \,\epsilon\, T_3, u_3, u_3^{'} \,\epsilon\, U_3$ be arbitrary elements. Then $s_1^{'}t_1^{'}t_1^{-1}s_1^{-1}s_2^{'}t_2^{'}t_2^{-1}s_2^{-1}s_3^{'}t_3^{'}t_3^{-1}s_3^{-1} = 1_G$ implies $s_1^{'}t_1^{'}t_1^{-1}s_1^{-1}s_2^{'}t_2^{'}t_2^{-1}s_2^{-1}s_3^{'}t_3^{'}t_3^{-1}s_3^{-1}H = H$, which implies $t_1^{'}H\,(t_1H)^{-1}\,t_2^{'}H\,(t_2H)^{-1}\,t_3^{'}H\,(t_3H)^{-1} = H$, which implies $u_1^{'}u_1^{-1}u_2^{'}u_2^{-1}u_3^{'}u_3^{-1} = 1_{G/H}$, which implies $u_i^{'} = u_i$ (assumption of TPP for the U_i in G/H) which implies $t_i^{'}H = t_iH$, which implies $t_i^{'} = t_i$, which implies, by the first

inequality, $s_1' s_1^{-1} s_2' s_2^{-1} s_3' s_3^{-1} = 1_H$, which implies $s_i' = s_i$ (assumption of TPP for the S_i in $H \lhd G$). ■

In general, the pointwise product of two index triples of G is not necessarily an index triple of G.

We define the set $\mathfrak{I}(G)$ to be the collection of all index triples of G. Formally:

(4.4) $\mathfrak{I}(G) := \{(S,T,U) \mid S,\ T,\ U \subseteq G$ satisfy the triple product property *(4.3)*$\}$.

By *Proposition 4.5* we have:

(4.5) $\mathfrak{I}(H) \subseteq \mathfrak{I}(G), \qquad H \leq G,$

and:

(4.6) $|\mathfrak{I}(H)| \leq |\mathfrak{I}(G)|, \qquad H \leq G.$

Now we have an important extension result for the index triples of direct product groups.

Lemma 4.8 *If groups G_1 and G_2 have index triples (S_1,T_1,U_1) and (S_2,T_2,U_2) respectively then the direct product of these triples, $(S_1 \times S_2, T_1 \times T_2, U_1 \times U_2)$, is an index triple of $G_1 \times G_2$.*

Proof. For any subsets $S_1,T_1,U_1 \subseteq G_1$ and $S_2,T_2,U_2 \subseteq G_2$, we define for $G_1 \times G_2$ the subsets $S_1 \times S_2 = \{(s_1,s_2) \mid s_1 \in S_1,\ s_2 \in S_2\}$, $T_1 \times T_2 = \{(t_1,t_2) \mid t_1 \in T_1,\ t_2 \in T_2\}$, $U_1 \times U_2 = \{(u_1,u_2) \mid u_1 \in U_1,\ u_2 \in U_2\} \subseteq G_1 \times G_2$. We call $(S_1 \times S_2, T_1 \times T_2, U_1 \times U_2)$ the direct product $(S_1,T_1,U_1) \times (S_2,T_2,U_2)$ of the triples (S_1,T_1,U_1) and (S_2,T_2,U_2). It is sufficient simply to assume the triple product property for the triples (S_1,T_1,U_1) and (S_2,T_2,U_2), and

then, for arbitrary $s_1, s_1^{'} \epsilon S_1$, $t_1, t_1^{'} \epsilon T_1$, $u_1, u_1^{'} \epsilon U_1$, $s_2, s_2^{'} \epsilon S_2$, $t_2, t_2^{'} \epsilon T_2$, $u_2, u_2^{'} \epsilon U_2$, we see that:

$$
\begin{aligned}
& s_1^{'} s_1^{-1} t_1^{'} t_1^{-1} u_1^{'} u_1^{-1} = 1_{G_1},\ s_2^{'} s_2^{-1} t_2^{'} t_2^{-1} u_2^{'} u_2^{-1} = 1_{G_2} \\
\iff\ & s_1^{'} s_1^{-1} = t_1^{'} t_1^{-1} = u_1^{'} u_1^{-1} = 1_{G_1},\ s_2^{'} s_2^{-1} = t_2^{'} t_2^{-1} = u_2^{'} u_2^{-1} = 1_{G_2} \\
\iff\ & s_1^{'} = s_1,\ t_1^{'} = t_1,\ u_1^{'} = u_1,\ s_2^{'} = s_2,\ t_2^{'} = t_2,\ u_2^{'} = u_2 \\
\iff\ & \left(s_1^{'}, s_2^{'}\right)(s_1, s_2)^{-1} = \left(t_1^{'}, t_2^{'}\right)(t_1, t_2)^{-1} = \left(u_1^{'}, u_2^{'}\right)(u_1, u_2)^{-1} \\
=\ & (1_{G_1}, 1_{G_2}) \\
=\ & \left(s_1^{'} s_1^{-1} t_1^{'} t_1^{-1} u_1^{'} u_1^{-1}, s_2^{'} s_2^{-1} t_2^{'} t_2^{-1} u_2^{'} u_2^{-1}\right) \\
=\ & \left(s_1^{'}, s_2^{'}\right)(s_1, s_2)^{-1} \left(t_1^{'}, t_2^{'}\right)(t_1, t_2)^{-1} \left(u_1^{'}, u_2^{'}\right)(u_1, u_2)^{-1}.
\end{aligned}
$$

■

If we denote by $\mathfrak{I}(G_1 \times G_2)$ the set of index triples of $G_1 \times G_2$, by *Lemma 4.8* we have the following.

(4.7) $\mathfrak{I}(G_1 \times G_2) \supseteq \mathfrak{I}(G_1) \times \mathfrak{I}(G_2)$.

(4.8) $|\mathfrak{I}(G_1 \times G_2)| \geq |\mathfrak{I}(G_1)|\,|\mathfrak{I}(G_2)|$.

4.1.3 *Groups and Matrix Tensors*

From *Chapter 2*, we recall the definition of the stuctural tensor, or simply, the matrix tensor $\langle n, m, p\rangle_K$ as the K-bilinear map $\langle n, m, p\rangle_K : K^{n\times m} \times K^{m\times p} \longrightarrow K^{n\times p}$, which describes the multiplication of $n \times m$ matrices by $m \times p$ matrices over K, with resulting product matrices in the matrix vector space $K^{n\times p}$. We omit the subscript K and say that G *realizes* a tensor $\langle n, m, p\rangle$ via an index triple (S, T, U), iff $|S| = n$, $|T| = m$, $|U| = p$, where these are positive integers, and, by definition, (S, T, U) has the triple product property. In this case, the index triple (S, T, U) said to correspond to the tensor $\langle n, m, p\rangle$. Loosely speaking, as will become clear later, this means that G "supports" the multiplication of $n \times m$ by $m \times p$ matrices indexed

by subsets S, T, $U \subseteq G$, in the sense of fact (I), section 1.3, *Chapter 1.* By assumption G is nontrivial, so that by *Lemma 4.2*, G always realizes the tensors $\langle 1,1,1\rangle$ and $\langle 2 \leq |G|, 1, 1\rangle$, and $G^{\times 3}$ always realizes the tensor $\langle |G|, |G|, |G|\rangle$. The following describes an elementary property for tensors of subgroups.

Proposition 4.9 *If $\langle n,m,p\rangle$ is a tensor realized by a subgroup $H \leq G$, then $\langle n,m,p\rangle$ is also realized by G.*

For G we define the set $\mathfrak{S}(G)$ as:

(4.9) $\mathfrak{S}(G) := \{\langle n,m,p\rangle \mid G \text{ realizes the tensor } \langle n,m,p\rangle\}$.

$\mathfrak{S}(G)$ is the set of all tensors $\langle n,m,p\rangle$ realized by G. By *(4.5)-(4.6)* we have the following results.

(4.10) $\mathfrak{S}(H) \subseteq \mathfrak{S}(G), \qquad H \leq G,$

and:

(4.11) $|\mathfrak{S}(H)| \leq |\mathfrak{S}(G)|, \qquad H \leq G.$

$\mathfrak{S}(G)$ is necessarily finite by the finiteness of $\mathfrak{J}(G)$.

For arbitrary tensors $\langle n,m,p\rangle$ and permutations $\mu \in Sym_3$ we denote by $\mu(\langle n,m,p\rangle)$ the permuted tensor $\langle \mu(n), \mu(m), \mu(p)\rangle$. Then we have an elementary result.

Lemma 4.10 *A group G realizes a tensor $\langle n,m,p\rangle$ iff it realizes any permuted tensor $\mu(\langle n,m,p\rangle) = \langle \mu(n), \mu(m), \mu(p)\rangle$, where $\mu \in Sym_3$.*

Proof. *A consequence of Lemma 4.5. (The reader will note the similarity between this lemma and Proposition 2.1. It will be shown that this is, in fact, a group-theoretic version of Proposition 2.1.)* ■

This means that if G supports multiplication of $n \times m$ by $m \times p$ matrices over K it simultaneously supports multiplication of matrices, over K, of all possible permutations of the dimensions $n \times m$ and $m \times p$, i.e. it also supports multiplication of $n \times p$ by $p \times m$ matrices, of $m \times n$ by $n \times p$ of matrices, of $m \times p$ by $p \times n$ matrices, of $p \times n$ by $n \times m$ matrices, of $p \times m$ by $m \times p$ matrices. As an example, we note that by *Lemma 4.1*, any group G realizes the tensors $\langle |G|, 1, 1\rangle$, $\langle 1, |G|, 1\rangle$, $\langle 1, 1, |G|\rangle$. We denote $M(\langle n, m, p\rangle)$ to be the set $\{\mu(\langle n, m, p\rangle) \mid \mu \in Sym_3\}$ of all permutations of a given tensor $\langle n, m, p\rangle$. If we write a tensor $\langle n, m, p\rangle$ in a "normal" form, where $n \leqslant m \leqslant p$, then $\langle n, m, p\rangle$ can be taken to be the representative of the set $M(\langle n, m, p\rangle)$. Thus, $\langle n, m, p\rangle \in \mathfrak{S}(G)$ implies that $M(\langle n, m, p\rangle) \subseteq \mathfrak{S}(G)$, and therefore $\mathfrak{S}(G)$ can be rewritten as:

$$\textit{(4.12)}\quad \mathfrak{S}(G) := \bigcup_{G \text{ realizes } \langle n,m,p\rangle,\ n \leq m \leq p} M(\langle n, m, p\rangle).$$

For arbitrary tensors $\langle n_1, m_1, p_1\rangle$ and $\langle n_2, m_2, p_2\rangle$ we define a pointwise multiplication operation $\cdot$ defined by $\langle n_1, m_1, p_1\rangle \cdot \langle n_2, m_2, p_2\rangle := \langle n_1 n_1, m_1 m_2, p_1 p_2\rangle$, which is associative, commutative, and has the unit $\langle 1, 1, 1\rangle$. $\mathfrak{S}(G)$ need not be closed under pointwise products. This operation allows us to characterize certain important extension results about tensors.

4.1.4 *Extension Results for Matrix Tensors*

Lemma 4.11 *If a normal subgroup $H \lhd G$ and the corresponding factor group G/H realize the tensors $\langle n_1, n_2, n_3\rangle$ and $\langle m_1, m_2, m_3\rangle$, respectively, then G realizes the tensor $\langle n_1, n_2, n_3\rangle \cdot \langle m_1, m_2, m_3\rangle = \langle n_1 m_1, n_2 m_2, n_3 m_3\rangle$, where $\langle n_1, n_2, n_3\rangle$ and $\langle m_1, m_2, m_3\rangle$ correspond to certain representative index triples of H and G/H resp., and $\langle n_1, n_2, n_3\rangle \cdot \langle m_1, m_2, m_3\rangle$ corresponds to the pointwise product of these index triples.*

Proof. A consequence of *Lemma 4.7*. ■

An analogous result applies to direct product groups.

Lemma 4.12 *If groups G_1 and G_2 realize tensors $\langle n_1, m_1, p_1\rangle$ and $\langle n_2, m_2, p_2\rangle$, respectively, then their direct product $G_1 \times G_2$ realizes the pointwise product tensor $\langle n_1, m_1, p_1\rangle \cdot \langle n_2, m_2, p_2\rangle = \langle n_1 n_2, m_1 m_2, p_1 p_2\rangle$, where $\langle n_1, m_1, p_1\rangle$ and $\langle n_2, m_2, p_2\rangle$ correspond to certain representative index triples of G_1 and G_2 resp. and $\langle n_1, m_1, p_1\rangle$ and $\langle n_2, m_2, p_2\rangle$ corresponds to the direct product of these index triples.*

Proof. A consequence of *Lemma 4.8.* ■

Thus:

(4.13) $\mathfrak{S}(G_1 \times G_2) \supseteq \mathfrak{S}(G_1) \cdot \mathfrak{S}(G_2)$.

4.1.5 *Group-Algebra Embedding and Complexity of Matrix Multiplication*

The following is a fundamental result describing the embedding of matrix multiplication into group algebras via the triple product property.

Theorem 4.13 *If $\langle n, m, p\rangle \in \mathfrak{S}(G)$ then (1) $\langle n, m, p\rangle \leq_K \mathfrak{m}_{KG}$ and (2) $\Re(\langle n, m, p\rangle) \leq \Re(\mathfrak{m}_{KG})$.*

Proof. Assume that G realizes $\langle n, m, p\rangle$ through an index triple (S, T, U), i.e. subsets $S, T, U \subseteq G$ have the triple product property, and $|S| = n$, $|T| = m$, $|U| = p$. First we prove that there exists a restriction of $\mathfrak{m}_{KG}$ to $\langle n, m, p\rangle$, where $\mathfrak{m}_{KG}$ is the (K-bilinear) multiplication map of the group K-algebra KG of G. Let $A = (A_{ij}) \in K^{n\times m}$ and $B = \left(B_{j'k}\right) \in K^{m\times p}$ be arbitrary $n \times m$ and $m \times p$ K-matrices respectively. The product of A and B is the $n \times p$ K-matrix $AB = C = (C_{ik})$ with entries C_{ik} determined by the formula $C_{ik} = \sum_{j=j'} A_{ij}B_{jk}$, $1 \leq i \leq n$, $1 \leq k \leq p$. We index the entries of A by S and T, and of B by T and U as follows:

$$\begin{aligned} A_{ij} &= A_{s,t}, & s = s(i), t = t(j); 1 \leq i \leq n, 1 \leq j \leq m; \\ B_{j'k} &= B_{t',u}, & t' = t'(j'), u = u(k); 1 \leq j' \leq m, 1 \leq k \leq p. \end{aligned}$$

We define linear maps $\mathfrak{a} : K^{n\times m} \longrightarrow KG$ and $\mathfrak{b} : K^{m\times p} \longrightarrow KG$ for embedding the matrices $A = (A_{s,t})$ and $B = \left(B_{t',u}\right)$ into the group K-algebra KG of G as follows:

$$\begin{aligned}\mathfrak{a}(A) &= \overline{A} = \sum_{s\,\epsilon\,S,\ t\,\epsilon\,T} A_{s,t}s^{-1}t;\\ \mathfrak{b}(B) &= \overline{B} = \sum_{t'\,\epsilon\,T,\ u\,\epsilon\,U} B_{t',u}t'^{-1}u.\end{aligned}$$

The injectivity of the mappings $(s,t) \longmapsto s^{-1}t$ and $(t,u) \longmapsto t^{-1}u$ on $S \times T$ and $T \times U$ respectively, proved in *Lemma 4.1*, means that $Ker\ \mathfrak{a} = \{\mathbf{O}_{n\times m}\}$ and $Ker\ \mathfrak{b} = \{\mathbf{O}_{m\times p}\}$, where $\mathbf{O}_{n\times m}$ and $\mathbf{O}_{m\times p}$ are zero matrices of dimensions $n \times m$ and $m \times p$ respectively, which proves the injectivity of $\mathfrak{a}$ and $\mathfrak{b}$. We index the $n \times p$ matrix product $AB = C = (C_{ik})$ by S and U as follows:

$$C_{ik} = C_{s,u}, \qquad s = s(i), u = u(k); 1 \le i \le n, 1 \le k \le p$$

We define an injective linear embedding map $\mathfrak{c} : K^{n\times p} \longrightarrow KG$ as follows:

$$\mathfrak{c}(C) = \overline{C} = \sum_{s\,\epsilon\,S,\ u\,\epsilon\,U} C_{s,u}s^{-1}u.$$

The product of $\overline{A}$ and $\overline{B}$ in KG is given by:

$$\begin{aligned}\overline{AB} &= \sum_{s\,\epsilon\,S,\ t\,\epsilon\,T} A_{s,t}s^{-1}t \cdot \sum_{t'\,\epsilon\,T,\ u\,\epsilon\,U} B_{t',u}t'^{-1}u\\ &= \sum_{s\,\epsilon\,S,\ t\,\epsilon\,T}\ \sum_{t'\,\epsilon\,T,\ u\,\epsilon\,U} A_{s,t}B_{t',u}s^{-1}tt'^{-1}u\\ &= \sum_{s\,\epsilon\,S,\ u\,\epsilon\,U} \left(\sum_{t,t'\,\epsilon\,T} A_{s,t}B_{t',u}tt'^{-1}\right) s^{-1}u.\end{aligned}$$

Clearly, for each distinct pair $s\ \epsilon\ S$, $u\ \epsilon\ U$, $C_{s,u} = \sum\limits_{t=t'\,\epsilon\,T} A_{s,t}B_{t,u}$. By assumption, (S,T,U) is an index triple of G, which means that for arbitrary elements $s'\ \epsilon\ S$, $u'\ \epsilon\ U$, $s'^{-1}u' = s^{-1}tt'^{-1}u \iff s's^{-1}tt'^{-1}uu'^{-1} = 1_G$ is true iff $s' = s$, $t' = t$, $u' = u$. But the sum of those terms of $\overline{AB}$ for which $t' = t$ all have the group term $s'^{-1}u'$ and the coefficient $\sum\limits_{t=t'\,\epsilon\,T} A_{s',t}B_{t,u'}$

corresponds 1-to-1 with the $(i,k)^{th}$ entry C_{ik} of C in $K^{n\times p}$ as given above. Thus,

$$\mathfrak{c}(C) = \overline{C} = \overline{AB} = \mathfrak{a}(A)\mathfrak{b}(B).$$

Then, we define an extraction map $\mathfrak{x} : K^{n\times p} \longleftarrow KG$ by:

$$\mathfrak{x}(\overline{AB}) = C = (C_{ik})$$

where the $C_{i'k'}$ are coefficients of the terms $s^{'-1}u^{'}$ in $\overline{AB}$, for $1 \leq i^{'} = i^{'}(s^{'}) \leq n$, $1 \leq k^{'} = k^{'}(t^{'}) \leq p$, $s^{'} \epsilon\, S$, $t^{'} \epsilon\, T$. Clearly $\mathfrak{x} = \mathfrak{a}^{-1} \cdot \mathfrak{b}^{-1}$, and by $\mathfrak{x}$ we will recover the desired matrix product $C = AB$ from $\overline{AB}$. By the injectivity of the maps $\mathfrak{a}$ and $\mathfrak{b}$ it follows that $\mathfrak{x} = \mathfrak{a}^{-1} \cdot \mathfrak{b}^{-1} = \mathfrak{c}^{-1}$. Since, for each $(A,B)\ \epsilon\ K^{n\times m} \times K^{m\times p}$, we have the composition $\mathfrak{x} \circ \mathfrak{m}_{KG} \circ (\mathfrak{a} \times \mathfrak{b})\,(A,B) = C$ $\epsilon\ K^{n\times p}$, it follows that:

$$\mathfrak{x} \circ \mathfrak{m}_{KG} \circ (\mathfrak{a} \times \mathfrak{b}) = \langle n,m,p \rangle\,.$$

i.e. $\langle n,m,p \rangle \leq_K \mathfrak{m}_{KG}$, which proves (1). (2) follows from applying *Proposition 2.2* to (1). ■

If $K = \mathbb{C}$ then we have an elementary corollary.

Corollary 4.14 *If* $\langle n,m,p \rangle\ \epsilon\ \mathfrak{S}(G)$ *then* (1) $\langle n,m,p \rangle \leq_{\mathbb{C}} \mathfrak{m}_{\mathbb{C}G} \cong_{\mathbb{C}} \bigoplus\limits_{\varrho\ \epsilon\ Irrep(G)} \langle d_\varrho, d_\varrho, d_\varrho \rangle$, (2) $(nmp)^{\frac{\omega}{3}} \leq \Re(\langle n,m,p \rangle) \leq \Re(\mathfrak{m}_{\mathbb{C}G}) \leq \sum\limits_{\varrho\ \epsilon\ Irrep(G)} \Re\left(\langle d_\varrho, d_\varrho, d_\varrho \rangle\right)$, *and* (3) $(nmp)^{\frac{\omega}{3}} \leq \Re(\langle n,m,p \rangle) \leq |G|$ *if* G *is Abelian.*

Proof. For (1) we apply *(3.17)* to part (1) of *Theorem 4.13*. For (2) we apply *(3.18)*, *Proposition 2.6*, and *Proposition 2.13* to part (2) of *Theorem 4.13*. For (3) we note that if G is Abelian then $\Re(\mathfrak{m}_{\mathbb{C}G}) = |G|$. From the latter case, we can also deduce that $\omega \leq \frac{\log|G|}{\log(nmp)^{1/3}}$ if G is Abelian and $\langle n,m,p \rangle\ \epsilon\ \mathfrak{S}(G)$. ■

4.2 The Complexity of Matrix Multiplication Realized by Groups

4.2.1 *Pseudoexponents*

For tensors $\langle n,m,p\rangle$ we define their *size* or *order* by $z(\langle n,m,p\rangle) = nmp$, and we write for their t^{th} powers $(nmp)^t$, where $t > 0$ is any real number. If $t = \frac{1}{3}$ then $(nmp)^{1/3}$ is just the geometric mean of the components of $\langle n,m,p\rangle$, i.e. the *mean size* or *mean order* of $\langle n,m,p\rangle$. We define by $\mathfrak{S}'(G)$ the set of all tensors of size > 1 realized by a nontrivial group G, i.e. $\mathfrak{S}'(G) = \mathfrak{S}(G)\backslash\{\langle 1,1,1\rangle\}$, and for any tensor $\langle n,m,p\rangle \epsilon\, \mathfrak{S}'(G)$, $nmp \geq 2$. Since G is nontrivial, by *Lemma 4.1*, G always realizes the tensor $\langle 2 \leq |G|, 1, 1\rangle$ and $\left|\mathfrak{S}'(G)\right| \geq 1$.

We define for G a number called its *pseudoexponent* $\alpha(G)$ by:

(4.14) $$\alpha(G) := \min_{\langle n,m,p\rangle\, \epsilon\, \mathfrak{S}'(G)} \left(\log_{(nmp)^{1/3}} |G|\right) \equiv \log_{\max_{\langle n,m,p\rangle\, \epsilon\, \mathfrak{S}'(G)} (nmp)^{1/3}} |G|.$$

By the definition and finiteness of $\mathfrak{S}'(G)$, $\alpha(G)$ necessarily exists. From above, we see that $\alpha(G)$ is uniquely determined by a *maximal* tensor $\left\langle n', m', p'\right\rangle \neq \langle 1,1,1\rangle$ realized by G, i.e. a tensor $\left\langle n', m', p'\right\rangle \epsilon\, \mathfrak{S}'(G)$ such that $n'm'p' \geq nmp$ for all other tensors $\langle n,m,p\rangle \epsilon\, \mathfrak{S}'(G)$. Formally:

(4.15) $$z'(G) := z\left(\left\langle n', m', p'\right\rangle\right) := \max_{\langle n,m,p\rangle\, \epsilon\, \mathfrak{S}'(G)} nmp.$$

It follows that:

(4.16) $$1 < nmp \leq n'm'p', \qquad \langle n,m,p\rangle \epsilon\, \mathfrak{S}(G).$$

The components of $\left\langle n', m', p'\right\rangle$ are the sizes $\left|S'\right| = n'$, $\left|T'\right| = m'$, $\left|U'\right| = p'$ of a maximal index triple $\left(S', T', U'\right)$ of G, which need not be unique. $\alpha(G)$ can be redefined as:

(4.17) $$\alpha(G) := \log_{z'(G)^{1/3}} |G|.$$

This is equivalent to:

(4.18) $z^{'}(G) = |G|^{\frac{3}{\alpha(G)}}$.

We note that $z^{'}(G)$ can be understood as the maximal size of matrix multiplication supported by G, and $z^{'}(G)^{\frac{1}{3}}$ is the geometric mean of this maximal size.

It follows from *Proposition 4.9* that:

(4.19) $z^{'}(H) \leq z^{'}(G), \qquad H \leq G.$

The following is an immediate consequence of *Lemma 4.11.*

(4.20) $z^{'}(G_1)z^{'}(G_2) \leq z^{'}(G), \qquad G = G_1 \times G_2.$

It follows from *(4.14)* that:

(4.21) $\alpha(G) \leqslant \log_{(nmp)^{1/3}} |G|, \qquad \langle n, m, p\rangle \, \epsilon \, \mathfrak{S}(G).$

For any positive integer n it follows that:

(4.22) $\alpha(G) \leqslant \log_n |G|, \qquad \langle n, n, n\rangle \, \epsilon \, \mathfrak{S}(G).$

The lower and upper bounds for $\alpha(G)$ are determined by the following fundamental lemma.

Lemma 4.15 *For any group G, $2 < \alpha(G) \leq 3$. If G is Abelian then $\alpha(G) = 3$.*

Proof. By *Lemma 4.2* G realizes the tensor $\langle 1, 1, |G| \rangle$ of size $|G|$, which shows that $\alpha(G) \leq 3$ by *(4.21)*. For the lower bound, we note first that, for any index triple $(S, T, U) \epsilon \mathfrak{I}(G)$ with associated tensor $\langle n, m, p \rangle \epsilon \mathfrak{S}(G)$, by *Lemma 4.1*, the mappings $(s, t) \longmapsto s^{-1}t$, $(s, u) \longmapsto s^{-1}u$, $(t, u) \longmapsto t^{-1}u$ on $S \times T$, $S \times U$, and $T \times U$ respectively, are injective, which means that $nm \leq |G|$, $np \leq |G|$, and $mp \leq |G|$. We now prove that if equalities hold in these inequalities then $p = 1$, or $m = 1$, or $n = 1$, respectively, starting with $nm \leq |G|$. Assume that $nm = |G| \Longleftrightarrow S^{-1}T = G$. Then, for arbitrary elements u, $u^{'} \epsilon U$ and $s^{'} \epsilon S$ and $t \epsilon T$, there exist unique $s \epsilon S$ and $t^{'} \epsilon T$ such that $s^{-1}t^{'} = s^{'-1}uu^{'-1}t$, which implies $s^{'}s^{-1}t^{'}t^{-1}u^{'}u^{-1} = s^{'}s^{'-1}uu^{'-1}tt^{-1}u^{'}u^{-1} = uu^{'-1}u^{'}u^{-1} = 1_G$. Hence, $u^{'}u^{-1} = 1_G$, and $u^{'} = u$, i.e. $|U| = p = 1$. In the same way we can prove that $np = |G| \Longrightarrow m = 1$, and $mp = |G| \Longrightarrow n = 1$. Hence, if $\langle n, m, p \rangle \epsilon \mathfrak{S}(G)$ then *not* all of n, m, $p = 1$, so that *not* all of nm, np, $mp = |G|$, i.e. if G realizes an index triple (S, T, U) corresponding to a tensor $\langle n, m, p \rangle$ then $(nmp)^2 < |G|^3$ and, therefore, $nmp < |G|^{\frac{3}{2}}$. Therefore, $z^{'}(G) < |G|^{\frac{3}{2}}$ maximally, and $\alpha(G) = \log_{z^{'}(G)^{1/3}} |G| > \log_{\left(|G|^{3/2}\right)^{1/3}} |G| = 2$.

Finally, if G is Abelian and has the maximal matrix tensor $\left\langle n^{'}, m^{'}, p^{'} \right\rangle$ of size $z^{'}(G) = n^{'}m^{'}p^{'}$ then, by the *Corollary 4.4* to *Lemma 4.3*, $z^{'}(G) \leq |G|$. This implies that $\log_{|G|^{1/3}} |G| = 3 \leq \log_{z^{'}(G)^{1/3}} |G| = \alpha(G)$, i.e. $\alpha(G) = 3$. The negation of the preceding statement is that $\alpha(G) < 3$ implies that G is non-Abelian. ■

This leads to an elementary corollary.

Corollary 4.16 *If* $\langle n, m, p \rangle \epsilon \mathfrak{S}(G)$, $(nmp)^{\frac{1}{3}} < |G|^{\frac{1}{2}}$.

By *Lemma 4.15*:

(4.23) $|G| \leq z^{'}(G) < |G|^{3/2}$.

The following is another elementary result.

Corollary 4.17 $\alpha(G) < 3$ *iff* $z^{'}(G) > |G|$. *Equivalently,* $\alpha(G) < 3$ *iff* $nmp > |G|$, *for some tensor* $\langle n, m, p \rangle \epsilon \mathfrak{S}(G)$.

Thus, the closer $z^{'}(G)$ is to $|G|$, the closer $\alpha(G)$ is to 3 and G is close to being the 3^{rd} power of the maximal mean order of matrix multiplication that it supports. The closer $z^{'}(G)$ is to $|G|^{3/2}$, the closer $\alpha(G)$ is close to 2 and G is close to being the 2^{nd} power of maximal mean order of matrix multiplication it supports. For example, if G_1 and G_2 are two finite groups such that $\alpha(G_1) \leq \alpha(G_2)$, then G_1 is at least as "efficient" in supporting matrix multiplication as G_2, or more efficient if $\alpha(G_1) < \alpha(G_2)$.

For subgroups we have an easy result.

Lemma 4.18 *For any nontrivial subgroup $H \leq G$, $\alpha(G) \leq \log_{z^{'}(H)^{1/3}}[G:H] + \alpha(H)$.*

Proof. $|G| = [G:H]\,|H|$, and from *(4.19)* $z^{'}(H) \leq z^{'}(G)$. Therefore,

$$\begin{aligned}
\alpha(G) &= \frac{\log|G|}{\log z^{'}(G)^{1/3}} \\
&= \frac{\log[G:H]}{\log z^{'}(G)^{1/3}} + \frac{\log|H|}{\log z^{'}(G)^{1/3}} \\
&\leq \frac{\log[G:H]}{\log z^{'}(H)^{1/3}} + \frac{\log|H|}{\log z^{'}(H)^{1/3}} \\
&= \frac{\log[G:H]}{\log z^{'}(H)^{1/3}} + \alpha(H).
\end{aligned}$$

■

For normal subgroups we have the following basic result.

Lemma 4.19 *For any nontrivial normal subgroup $H \lhd G$ and corresponding factor group G/H, $\alpha(G) \leq \max(\alpha(H), \alpha(G/H))$.*

Proof. Let $\left\langle m_1^{'}, m_2^{'}, m_3^{'} \right\rangle \epsilon\ \mathfrak{S}(H)$ and $\left\langle p_1^{'}, p_2^{'}, p_3^{'} \right\rangle \epsilon\ \mathfrak{S}(G/H)$ be the maximal tensors realized by $H \lhd G$ and its factor group G/H, respectively, and let $\left\langle n_1^{'}, n_2^{'}, n_3^{'} \right\rangle \epsilon\ \mathfrak{S}(G)$ be the maximal tensor realized by G. Then, by *(4.18)*, we have the identities:

$$z^{'}(H)^{\alpha(H)} = |H|^3,\ z^{'}(G/H)^{\alpha(G/H)} = |G/H|^3,\ z^{'}(G)^{\alpha(G)} = |G|^3.$$

By *Lemma 4.11* $\left\langle m_1^{'}p_1^{'}, m_2^{'}p_2^{'}, m_3^{'}p_3^{'}\right\rangle = \left\langle m_1^{'}, m_2^{'}, m_3^{'}\right\rangle \cdot \left\langle p_1^{'}, p_2^{'}, p_3^{'}\right\rangle \epsilon\, \mathfrak{S}(G)$, and therefore:

$$\begin{aligned} & z^{'}(H)z^{'}(G/H) \\ = \;& z\left(\left\langle m_1^{'}, m_2^{'}, m_3^{'}\right\rangle \cdot \left\langle p_1^{'}, p_2^{'}, p_3^{'}\right\rangle\right) \\ = \;& z\left(\left\langle m_1^{'}p_1^{'}, m_2^{'}p_2^{'}, m_3^{'}p_3^{'}\right\rangle\right) \\ = \;& m_1^{'}p_1^{'}m_2^{'}p_2^{'}m_3^{'}p_3^{'} \\ \leq \;& n_1^{'}n_2^{'}n_3^{'} \\ = \;& z^{'}(G) \end{aligned}$$

by the maximality of $\left\langle n_1^{'}, n_2^{'}, n_3^{'}\right\rangle$ for G. Then also

$$\left(z^{'}(H)z^{'}(G/H)\right)^{\alpha(G)} = z^{'}(H)^{\alpha(G)}z^{'}(G/H)^{\alpha(G)} \leq z^{'}(G)^{\alpha(G)}.$$

Using the identities $|H|\,|G/H| = |G|$, and $|H|^3\,|G/H|^3 = |G|^3$, we see that:

$$z^{'}(G)^{\alpha(G)} = z^{'}(H)^{\alpha(H)}z^{'}(G/H)^{\alpha(G/H)}.$$

If $\max(\alpha(H), \alpha(G/H)) = \alpha(H)$ and $\alpha(G) > \alpha(H)$ then:

$$\begin{aligned} \left(z^{'}(H)z^{'}(G/H)\right)^{\alpha(G)} &= z^{'}(H)^{\alpha(G)}z^{'}(G/H)^{\alpha(G)} \\ &> z^{'}(H)^{\alpha(H)}z^{'}(G/H)^{\alpha(H)} \\ &\geq z^{'}(H)^{\alpha(H)}z^{'}(G/H)^{\alpha(G/H)} \\ &= z^{'}(G)^{\alpha(G)} \end{aligned}$$

i.e. a contradiction. Similarly, if $\max(\alpha(H), \alpha(G/H)) = \alpha(G/H)$ and $\alpha(G) > \alpha(G/H)$ then:

$$\begin{aligned} \left(z^{'}(H)z^{'}(G/H)\right)^{\alpha(G)} &= z^{'}(H)^{\alpha(G)}z^{'}(G/H)^{\alpha(G)} \\ &> z^{'}(H)^{\alpha(G/H)}z^{'}(G/H)^{\alpha(G/H)} \\ &\geq z^{'}(H)^{\alpha(H)}z^{'}(G/H)^{\alpha(G/H)} \\ &= z^{'}(G)^{\alpha(G)} \end{aligned}$$

also a contradiction. Thus it must be that $\alpha(G) \leq \alpha(H)$, $\alpha(G/H)$, which means that:

$$\alpha(G) \leq \max(\alpha(H), \alpha\,(G/H)).$$

Equality above holds trivially if G is Abelian. ■

For direct product groups we have the following result.

Lemma 4.20 *$\alpha\left(G^{\times k}\right) \leq \alpha\,(G)$, where $G^{\times k}$ is the k-fold direct product of G.*

Proof. By *(4.20)* $z^{'}(G^{\times k}) \geq z^{'}(G)^{k}$. Then

$$\begin{aligned}
\alpha\left(G^{\times k}\right) &= \log_{z'(G^{\times k})^{1/3}} \left|G^{\times k}\right| \\
&\leq \log_{z'(G)^{k/3}} |G|^{k} \\
&= \frac{\not{k}}{\not{k}} \log_{z'(G)^{1/3}} |G| \\
&= \alpha\,(G)\,.
\end{aligned}$$

■

This means that for $k = 1, 2, 3, ...$ we have a descending sequence of pseudoexponent inequalities, $... \leq \alpha\left(G^{\times 3}\right) \leq \alpha\left(G^{\times 2}\right) \leq \alpha\,(G)$. We do not know of general conditions on the $G^{\times k}$ for making this sequence strict, though it would require a strict ascending sequence, $z^{'}(G) < z^{'}(G^{\times 2}) < z^{'}(G^{\times 3}) < \ldots$, for the corresponding maximal tensors $z^{'}(G^{\times k})$ of the $G^{\times k}$.

For explicit estimates of the exponents of specific types of groups we refer the reader to sections 5-7 in [CU2003], since for the derivation of estimates of the exponent ω we have found the simultaneous triple product property more useful. However, we do give some estimates for the exponents of the symmetric groups in sections *6.1.2-6.1.3* in *Chapter 6.*

4.2.2 *The Parameters* γ

Let $d^{'}(G)$ be the largest degree of an irreducible character of a group G. We define for G the number $\gamma(G)$ by:

(4.24) $\gamma(G) := \inf\left\{\gamma \in \mathbb{R}^+ \mid |G|^{\frac{1}{\gamma}} = d'(G)\right\}$.

By *Theorem 3.10* $d'(G) \leq (|G|-1)^{1/2} < |G|^{1/2}$, hence it follows from the definition *(4.24)* that $\gamma(G) > 2$. Since for a fixed group G, $\lim_{\gamma \longrightarrow \infty} |G|^{1/\gamma} = 1$, and $d'(G) = 1$ for an Abelian group G, we, therefore, define $\gamma(G) = \infty$ if G is an Abelian group. We note that $\gamma(G)$ can always be computed as:

(4.25) $\gamma(G) = \log_{d'(G)} |G|$

provided we know $d'(G)$. An example: $d'(Sym_3) = 2$, and therefore $\gamma(Sym_3) = \log_2 6 \approx 2.585$.

By *Theorem 3.10* we know that $\left(\frac{|G|}{c(G)}\right)^{1/2} < d'(G) < (|G|-1)^{1/2}$ iff G is non-Abelian, and, therefore, the bounds for the $\gamma(G)$ of non-Abelian groups G, are given by:

(4.26) $2\frac{\log|G|}{\log(|G|-1)} < \gamma(G) < 2\frac{\log|G|}{\log|G|-\log c(G)}$.

For example, $c(Sym_3) = 3$, and therefore $2\frac{\log|Sym_3|}{\log(|Sym_3|-1)} = 2\frac{\log 6}{\log 5} \approx 2.226 < \gamma(Sym_3) = \log_2 6 \approx 2.585 < 5.17 \approx 2\frac{\log 6}{\log 6-\log 3} = 2\frac{\log|Sym_3|}{\log|Sym_3|-\log c(Sym_3)}$.

This is a basic result for normal subgroups.

Lemma 4.21 *For any nontrivial normal subgroup $H \lhd G$ such that $d'(G) \geq \max\left(d'(H), d'(G/H)\right)$, $\gamma(G) \leq \gamma(H) + \gamma(G/H)$.*

Proof. For a nontrivial normal subgroup $H \lhd G$ the assumption of $d'(G) \geq \max\left(d'(H), d'(G/H)\right)$ means that

$$\begin{aligned}
\gamma(G) &= \frac{\log|G|}{\log d'(G)} \\
&= \frac{\log|H|}{\log d'(G)} + \frac{\log|G/H|}{\log d'(G)} \\
&\leq \frac{\log|H|}{\log d'(H)} + \frac{\log|G/H|}{\log d'(G/H)} \\
&= \gamma(H) + \gamma(G/H).
\end{aligned}$$

■

This is a basic result for direct product groups.

Lemma 4.22 *$\gamma(G^{\times k}) = \gamma(G)$, where $G^{\times k}$ is the k-fold direct product of G.*

Proof. We observe first that $d^{'}\left(G^{\times k}\right) = d^{'}\left(G\right)^{k}$, [SER1977]. Then

$$\begin{aligned}
\gamma(G^{\times k}) &= \log_{d^{'}(G^{\times k})}\left|G^{\times k}\right| \\
&= \log_{d^{'}(G)^{k}}|G|^{k} \\
&= \frac{\not{k}}{\not{k}}\log_{d^{'}(G)}|G| \\
&= \gamma(G).
\end{aligned}$$

■

4.3 Fundamental Relations between α, γ and the Exponent ω

Here we derive important relations between the exponent ω and the parameters α and γ.

4.3.1 *Preliminaries*

Let ω be the usual exponent of matrix multiplication over $\mathbb{C}$. The following is an important result.

Theorem 4.23 *$|G|^{\frac{\omega}{\alpha(G)}} = D_2(G)^{\frac{\omega}{\alpha(G)}} \leq D_\omega(G)$.*

Proof. Let $\left\langle n^{'}, m^{'}, p^{'}\right\rangle \epsilon\ \mathfrak{S}(G)$ be the maximal tensor realized by G of size $z^{'}(G) = n^{'}m^{'}p^{'}$ uniquely determining $\alpha(G)$, and by definition *(4.18)* $z^{'}(G) = n^{'}m^{'}p^{'} = |G|^{\frac{3}{\alpha(G)}}$. Using

Proposition 2.13 and *Corollary 4.14*:

$$\begin{aligned}\left(n^{'}m^{'}p^{'}\right)^{\frac{\omega}{3}} &= |G|^{\frac{\omega}{\alpha(G)}} = D_2(G)^{\frac{\omega}{\alpha(G)}} \qquad (*)\\ &\leq \Re\left(\left\langle n^{'}, m^{'}, p^{'}\right\rangle\right)\\ &\leq \sum_{\varrho\,\epsilon\,Irrep(G)} \Re\left(\langle d_\varrho, d_\varrho, d_\varrho\rangle\right).\end{aligned}$$

From *Theorem 4.13* $\langle n, m, p\rangle \leq_K \bigoplus_{\varrho\,\epsilon\,Irrep(G)} \langle d_\varrho, d_\varrho, d_\varrho\rangle$ and taking r^{th} tensor product powers on either side we obtain

$$\langle n^r, m^r, p^r\rangle \leq_K \bigoplus_{\varrho_{1,\ldots,}\varrho_r\,\epsilon\,Irrep(G)} \left\langle d_{\varrho_1}\cdots d_{\varrho_r}, d_{\varrho_1}\cdots d_{\varrho_r}, d_{\varrho_1}\cdots d_{\varrho_r}\right\rangle.$$

By *Proposition 2.12* for each $\varepsilon > 0$ there exists a constant $C_\varepsilon \geq 1$ such that for all k we have:

$$\Re\left(\langle k, k, k\rangle\right) \leq C_\varepsilon k^{\omega+\varepsilon}.$$

Hence, taking ranks on either side of $(*)$ we obtain that:

$$\begin{aligned}D_2\left(G\right)^{\frac{r\omega}{\alpha(G)}} &\leq C_\varepsilon\left(\sum_{\varrho\,\epsilon\,Irrep(G)} d_\varrho^{\omega+\varepsilon}\right)^r\\ &= C_\varepsilon D_{\omega+\varepsilon}\left(G\right)^r\end{aligned}$$

for some $C_\varepsilon > 0$ depending on some $\varepsilon > 0$. Taking the r^{th} root on either side we obtain

$$D_2(G)^{\frac{\omega}{\alpha(G)}} \leq \sqrt[r]{C_\varepsilon} D_{\omega+\varepsilon}\left(G\right).$$

If we take the limit as $r \longrightarrow \infty$, and then the limit as $\varepsilon \longrightarrow 0$ we obtain finally that:

$$D_2(G)^{\frac{\omega}{\alpha(G)}} \leq D_\omega(G).$$

■

By the maximality of $\left\langle n^{'}, m^{'}, p^{'}\right\rangle$ in $\mathfrak{S}(G)$ we have an elementary corollary.

Corollary 4.24 *If* $\langle n,m,p\rangle \,\epsilon\, \mathfrak{S}(G)$ *then* (1) $(nmp)^{\frac{1}{3}} \leq D_\omega(G)^{\frac{1}{\omega}}$, *and* (2) $(nmp)^{\frac{1}{3}} \leq d^{'}(G)^{1-\frac{2}{\omega}}\,|G|^{\frac{1}{\omega}}$.

Proof. For any $\langle n,m,p\rangle \,\epsilon\, \mathfrak{S}(G)$, by *(4.16)* and *Theorem 4.23*, $(nmp)^{\frac{\omega}{3}} \leq z^{'}(G)^{\frac{\omega}{3}} \leq D_2(G)^{\frac{\omega}{\alpha(G)}} \leq D_\omega(G)$, and taking ω^{th} roots, we have the result. Part (2) is a consequence of applying *(3.12)* to the right-hand side of (1). ■

Theorem 4.23 can be reexpressed as the relation.

(4.27) $|G|^{\frac{1}{\alpha(G)}} \leq D_\omega(G)^{\frac{1}{\omega}}$.

Using *(4.18)* we know:

(4.28) $|G|^{\frac{1}{\alpha(G)}} \leq D_\omega(G)^{\frac{1}{\omega}} \leq |G|^{\frac{1}{2}}$.

In the impossible case that $\alpha(G) = 2$ we would have that $|G|^{\frac{1}{2}} \leq D_\omega(G)^{\frac{1}{\omega}} \leq |G|^{\frac{1}{2}}$, which would imply that $\omega = 2$. However, since by *Lemma 4.15* $\alpha(G) > 2$ always it follows that $|G|^{\frac{1}{\alpha(G)}} < |G|^{\frac{1}{2}}$ always and, therefore, the first estimate in *(4.28)* will be strict if ω could be pushed to 2.

The following is a useful result.

Corollary 4.25 $D_r(G) \leq |G|^{\frac{r-2}{\gamma(G)}+1}$ *for* $r \geq 2$.

Proof. By *(3.12)* $D_r(G) \leq d^{'}(G)^{r-2}\,|G|$ for $r \geq 2$, and by *(4.25)* $d^{'}(G) = |G|^{\frac{1}{\gamma(G)}}$. Then

$$\begin{aligned} D_r(G) &\leq \left(|G|^{\frac{1}{\gamma(G)}}\right)^{r-2}|G| \\ &= |G|^{\frac{r-2}{\gamma(G)}+1}. \end{aligned}$$

■

Using the above, we can prove the following fundamental relation.

Corollary 4.26 *If G is a non-Abelian group such that $\alpha(G) < \gamma(G)$ then $\omega \leq \alpha(G)\left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)}\right)$.*

Proof. By *Theorem 4.23* $|G|^{\frac{\omega}{\alpha(G)}} \leq D_\omega(G)$. For $r = \omega$ in *Corollary 4.25* $D_\omega(G) \leq |G|^{\frac{\omega-2}{\gamma(G)}+1}$, from which we derive $|G|^{\frac{\omega}{\alpha(G)}} \leq |G|^{\frac{\omega-2}{\gamma(G)}+1}$. This implies that $\frac{\omega}{\alpha(G)} \leq \frac{\omega-2}{\gamma(G)}+1$, which is equivalent to $\omega\left(\frac{1}{\alpha(G)}-\frac{1}{\gamma(G)}\right) \leq 1-\frac{2}{\gamma(G)}$. Since $\gamma(G)-\alpha(G) > 0$ by assumption, it follows that $\left(\frac{1}{\alpha(G)}-\frac{1}{\gamma(G)}\right) > 0$. Dividing both sides of the previous estimate by $\left(\frac{1}{\alpha(G)}-\frac{1}{\gamma(G)}\right)$ we get $\omega \leq \left(1-\frac{2}{\gamma(G)}\right) / \left(\frac{1}{\alpha(G)}-\frac{1}{\gamma(G)}\right) = \alpha(G)\left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)}\right)$. ■

4.3.2 *Fundamental Results for the Exponent ω using Single non-Abelian Groups*

Corollary 4.27 *If G is a non-Abelian group such that $|G|^{\frac{1}{\alpha(G)}} > D_3(G)^{\frac{1}{3}}$ then $\omega < 3$. Equivalently, $\omega < 3$ if $z'(G)^{\frac{1}{3}} > D_3(G)^{\frac{1}{3}}$.*

Proof. If $|G|^{\frac{1}{\alpha(G)}} > D_3(G)^{\frac{1}{3}}$, by *(4.28)*, $D_3(G)^{\frac{1}{3}} < |G|^{\frac{1}{\alpha(G)}} \leq D_\omega(G)^{\frac{1}{\omega}}$, which implies that by the convexity property *(3.11)*, $\omega < 3$. The second part follows from the fact that $|G|^{\frac{1}{\alpha(G)}} = z'(G)^{\frac{1}{3}}$ (see *(4.18)*). ■

This is a trivial result because it has been proven that $\omega < 2.38$ [CW1990]. More useful is the following.

Corollary 4.28 (1) *$\omega \leq t < 3$ for some $t > 2$, if there is a non-Abelian group G such that $\alpha(G) < \gamma(G)$ and $\alpha(G)\left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)}\right) \leq t$.* (2) *An equivalent, but more precise statement is that $\omega \leq t < 3$, for some $t > 2$, if there is a non-Abelian group G such that $z'(G)^{\frac{1}{3}} > d'(G)$ and $\frac{z'(G)^{\frac{t}{3}}}{d'(G)^{t-2}} \geq G$.*

Proof. By *Corollary 4.26* $\omega \leq \alpha(G)\left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)}\right)$ if $\alpha(G) < \gamma(G)$. This means that if, in addition, $\alpha(G)\left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)}\right) \leq t$ for some $2 < t < 3$ then $\omega \leq t$. (2) From *(4.17)*, *(4.23)*, and *(4.25)*, we see that $\alpha(G) < \gamma(G)$ is equivalent to $z'(G)^{\frac{1}{3}} > d'(G)$. By (1) the additional condition $\alpha(G)\left(\frac{\gamma(G)-2}{\gamma(G)-\alpha(G)}\right) \leq t$ needed to prove $\omega \leq t$ is equivalent, to $\frac{\log|G|}{\log z'(G)^{1/3}}\left(\frac{\log|G|}{\log d'(G)}-2\right) \leq \left(\frac{\log|G|}{\log d'(G)}-\frac{\log|G|}{\log z'(G)^{1/3}}\right)t$. Dividing both sides of the inequality by $\log|G|$ we will still have a term on the left with numerator $\log|G|$, and making it the subject of the inequality on

the left, this becomes $\log|G| \leq t\log z^{'}(G)^{\frac{1}{3}} + (2-t)\log d^{'}(G) = \log z^{'}(G)^{\frac{t}{3}} - \log d^{'}(G)^{(t-2)} = \log \frac{z^{'}(G)^{\frac{t}{3}}}{d^{'}(G)^{(t-2)}}$. Taking antilogarithms we have the result. ■

For any given group G, from *(4.23)* we see that $|G|^{\frac{1}{3}} < z^{'}(G)^{\frac{1}{3}} < |G|^{\frac{1}{2}}$, and from part (5) of *Theorem 3.10* $c(G)^{-\frac{1}{2}}|G|^{\frac{1}{2}} < d^{'}(G) < (|G|-1)^{\frac{1}{2}}$ if G is non-Abelian. The intersection of these intervals lies in the open interval $\left(c(G)^{-\frac{1}{2}}|G|^{\frac{1}{2}}, |G|^{\frac{1}{2}}\right)$, and *Corollary 4.29* will let us prove $\omega \leq t < 3$ for some $t > 2$ if we can find a non-Abelian group G realizing matrix multiplication of largest size $z^{'}(G)$ and with an irreducible character of largest degree $d^{'}(G)$ such that $c(G)^{-\frac{1}{2}}|G|^{\frac{1}{2}} < d^{'}(G) < z^{'}(G)^{\frac{1}{3}} < |G|^{\frac{1}{2}} \leq \frac{z^{'}(G)^{\frac{t}{6}}}{d^{'}(G)^{\frac{t-2}{2}}}$.

4.3.3 *Fundamental Results for the Exponent ω using Families of non-Abelian Groups*

The following results describe ways of proving that $\omega = 2$ via families of non-Abelian groups. The first is as follows.

Corollary 4.29 *If $\{G_k\}$ is a family of non-Abelian groups such that $\alpha(G_k) \equiv \alpha_k = 2 + o(1)$, and $\gamma(G_k) \equiv \gamma_k = 2 + o(1)$, and $\alpha_k - 2 = o(\gamma_k - 2)$, as $k \longrightarrow \infty$, then $\omega = 2$.*

Proof. Assuming the conditions $\alpha_k = 2 + o(1)$, $\gamma_k = 2 + o(1)$, $\alpha_k - 2 = o(\gamma_k - 2)$, as $k \longrightarrow \infty$, for the family $\{G_k\}$, we will have

$$\begin{aligned} & (\alpha_k - \gamma_k) \\ = \; & (\alpha_k - 2) - (\gamma_k - 2) \\ = \; & o(\gamma_k - 2) - (\gamma_k - 2) \\ < \; & -\frac{1}{2}(\gamma_k - 2) < 0 \end{aligned}$$

for sufficiently large k. Then by *Corollary 4.26*, as $k \longrightarrow \infty$, we will have

$$\begin{aligned}
\omega &\leq \alpha_k \left(\frac{\gamma_k - 2}{\gamma_k - \alpha_k} \right) \\
&= \frac{\alpha_k}{\left(1 - \left(\alpha_k - 2\right) / \left(\gamma_k - 2\right)\right)} \\
&= \frac{2 + o\left(1\right)}{1 - o\left(1\right) / o\left(1\right)} \\
&= \frac{2 + o\left(1\right)}{1 - o\left(1\right)} \\
&\longrightarrow 2^{+}.
\end{aligned}$$

■

From *(4.18)*, $z^{'}(G)^{\frac{1}{3}} = |G|^{\frac{1}{\alpha(G)}}$, and from *(4.25)*, $d^{'}(G) = |G|^{\frac{1}{\gamma(G)}}$, and for a family $\{G_k\}$ of non-Abelian groups G_k realizing matrix multiplications of maximal sizes $z_k^{'} \equiv z^{'}(G_k)$ and maximal irreducible character degrees $d_k^{'} \equiv d^{'}(G_k)$, the conditions $\alpha_k = 2 + o(1)$ and $\gamma_k = 2 + o(1)$ are equivalent to the conditions $\frac{\log |G_k|^{\frac{1}{2}}}{\log z_k^{'\frac{1}{3}}} = 1 + o(1)$ and $\frac{\log (|G_k|-1)^{\frac{1}{2}}}{\log d_k^{'}} = 1 + o(1)$, respectively, which are implied by the conditions $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$ and $(|G_k| - 1)^{\frac{1}{2}} - d_k^{'} = o(1)$, respectively. Here, we describe a specific result for a family of non-Abelian groups satisfying the latter conditions.

Theorem 4.30 *Let $\{G_k\}$ be a family of non-Abelian groups G_k realizing matrix multiplications of maximal sizes $z_k^{'} \equiv z^{'}(G_k)$ and with maximal irreducible character degrees $d_k^{'} \equiv d_k^{'}(G)$. Then,* (1) *$\omega = 2$ if $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$ and $(|G_k| - 1)^{\frac{1}{2}} - d_k^{'} = o(1)$ such that $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o\left((|G_k| - 1)^{\frac{1}{2}} - d_k^{'}\right)$ as $k \longrightarrow \infty$. And more generally,* (2) *$\omega = 2$ if $|G_k| \longrightarrow \infty$ as $k \longrightarrow \infty$ and there exists a sequence $\{C_k\}$ of constants C_k for the G_k such that $2 \leq C_k \leq |G_k| - 1$, $|G_k| \geq C_k \left(1 + \frac{1}{C_k - 1}\right)$, $C_k \longrightarrow \infty$, $C_k = o(|G_k|)$, $(|G_k| - C_k)^{\frac{1}{2}} - d_k^{'} = o(1)$, $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$ and $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o\left((|G_k| - C_k)^{\frac{1}{2}} - d_k^{'}\right)$, as $k \longrightarrow \infty$.*

Proof. For an arbitrary group G, if we compare *(4.16)* and *(4.25)*, we see that $\alpha(G) < \gamma(G)$ iff $z^{'}(G)^{\frac{1}{3}} > d_k^{'}(G)$, $\alpha(G) = \gamma(G)$ iff $z^{'}(G)^{\frac{1}{3}} = d^{'}(G)$, and $\gamma(G) < \alpha(G)$ iff $z^{'}(G)^{\frac{1}{3}} < d^{'}(G)$. Moreover, $\alpha(G)$ is close to 2 iff $z^{'}(G)^{\frac{1}{3}}$ is close to $|G|^{\frac{1}{2}}$, and $\gamma(G)$ is close to 2 iff $d^{'}(G)$ is close

to $|G|^{\frac{1}{2}}$.

(1) By *Theorem 3.10*, $\left(\frac{|G|}{c(G)}\right)^{\frac{1}{2}} < d'(G) < (|G|-1)^{\frac{1}{2}} < |G|^{\frac{1}{2}}$ for a non-Abelian group G, therefore, for the non-Abelian family $\{G_k\}$ the most that we can have is $d_k^{'} \longrightarrow (|G_k|-1)^{\frac{1}{2}-}$, as $k \longrightarrow \infty$. But $d_k^{'} \longrightarrow (|G_k|-1)^{\frac{1}{2}-}$, as $k \longrightarrow \infty$ implies $\gamma_k \longrightarrow \log_{(|G_k|-1)^{1/2}} |G_k| = 2\log_{(|G_k|-1)} |G_k| \longrightarrow 2^+$, i.e. $\gamma_k = 2 + o(1)$, and if, in addition, $z_k^{'\frac{1}{3}} \longrightarrow .|G_k|^{\frac{1}{2}-}$ faster than $d_k^{'} \longrightarrow (|G_k|-1)^{\frac{1}{2}-}$ as $k \longrightarrow \infty$ then $\alpha_k = 2 + o(1)$ and $\gamma_k = 2 + o(1)$ such that $\alpha_k - 2 = o(\gamma_k - 2)$. This can also be written as $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$, $(|G_k|-1)^{\frac{1}{2}} - d_k^{'} = o(1)$ and $|G_k|^{\frac{3}{2}} - z_k^{'\frac{1}{3}} = o\left((|G_k|-1)^{\frac{1}{2}} - d_k^{'}\right)$, as $k \longrightarrow \infty$, which implies $\alpha_k = 2+o(1)$, $\gamma_k = 2+o(1)$ and $\alpha_k - 2 = o(\gamma_k - 2)$, as $k \longrightarrow \infty$, which, by *Corollary 4.29*, implies that $\omega = 2$.

(2) Assume all the conditions in (2). In particular, for the constants $2 \leq C_k \leq |G_k| - 1$, the condition $|G_k| \geq C_k\left(1 + \frac{1}{C_k - 1}\right)$ means that $\gamma_k = \log_{d_k^{'}} |G_k| \leq \log_{d_k^{'}} (|G_k| - C_k) + \log_{d_k^{'}} C_k$. Then, the condition $(|G_k| - C_k)^{\frac{1}{2}} - d_k^{'} = o(1)$, implying $d_k^{'} \longrightarrow (|G_k| - C_k)^{\frac{1}{2}-}$, as $k \longrightarrow \infty$, together with $|G_k| \longrightarrow \infty$, $C_k \longrightarrow \infty$, $C_k = o(|G_k|)$, as $k \longrightarrow \infty$, implies that $\gamma_k \longrightarrow 2\left(\log_{(|G_k|-C_k)} (|G_k| - C_k) + \log_{(|G_k|-C_k)} C_k\right) = 2 + o(1)$, as $k \longrightarrow \infty$. In addition, the conditions $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o(1)$ and $|G_k|^{\frac{1}{2}} - z_k^{'\frac{1}{3}} = o\left((|G_k| - C_k)^{\frac{1}{2}} - d_k^{'}\right)$, $k \longrightarrow \infty$, imply that $\alpha_k \longrightarrow 2^+$ faster than $\gamma_k \longrightarrow 2^+$ as $k \longrightarrow \infty$, i.e. $\alpha_k = 2 + o(1)$ and $\gamma_k = 2 + o(1)$ such that $\alpha_k - 2 = o(\gamma_k - 2)$, as $k \longrightarrow \infty$, which, by *Corollary 4.29* implies that $\omega = 2$. ■

Chapter 5

Groups and Matrix Multiplication II

Here we extend the methods introduced in *Chapter 4* to study the complexity of simultaneous independent multiplications of several pairs of matrices via a single group using the concept of simultaneous triple products. We derive some important results that bound the exponent ω in terms of the sizes of simultaneously realized tensors of single groups in relation to the sizes of the groups. In our analysis, it appears that the sharpness of estimates for ω is positively related to the *number* of simultaneous matrix multiplications supported by a group, and also that the best groups, in this regard, seem to be groups which are wreath products of Abelian groups with symmetric groups.

5.1 Realizing Simultaneous, Independent Matrix Multiplications in Groups

5.1.1 *Groups and Families of Simultaneous Index Triples and Tensors*

We define the right-quotient set $Q(X, Y)$ of any pair of subsets X, Y of a finite group G by:

(5.1) $Q(X, Y) = \left\{ xy^{-1} \mid x \in X,\ y \in Y \right\}.$

Let I be a finite index set. A collection $\{(S_i, T_i, U_i)\}_{i \,\epsilon\, I}$ of triples (S_i, T_i, U_i) of subsets $S_i, T_i, U_i \subseteq G$, of sizes $|S_i| = m_i$, $|T_i| = p_i$, $|U_i| = q_i$ respectively, is said to satisfy the *simultaneous triple product property* (STPP) iff it is the case that:

(5.2) each (S_i, T_i, U_i) satisfies the TPP and $s_i^{'} s_j^{-1} t_j^{'} t_k^{-1} u_k^{'} u_i^{-1} = 1_G \Longrightarrow i = j = k$

for all $s_i^{'} s_j^{-1} \,\epsilon\, Q(S_i, S_j)$, $t_j^{'} t_k^{-1} \,\epsilon\, Q(T_j, T_k)$, $u_k^{'} u_i^{-1} \,\epsilon\, Q(U_k, U_i)$, $i, j, k \,\epsilon\, I$. In this case, G is said to *simultaneously realize* the corresponding collection $\{\langle m_i, p_i, q_i \rangle\}_{i \,\epsilon\, I}$ of tensors through the collection $\{(S_i, T_i, U_i)\}_{i \,\epsilon\, I}$, which is called a *collection of simultaneous index triples*. For such collections, the triple product property *(4.3)* becomes a special case of the simultaneous triple product property when $|I| = 1$. Thus, every triple in a collection $\{(S_i, T_i, U_i)\}_{i \,\epsilon\, I}$ of simultaneous index triples of G is an index triple of G, though there is no converse for collections of index triples. The i^{th} tensor $\langle m_i, p_i, q_i \rangle$ in $\{\langle m_i, p_i, q_i \rangle\}_{i \,\epsilon\, I}$ is the matrix multiplication map $\mathbb{C}^{n_i \times m_i} \times \mathbb{C}^{m_i \times p_i} \longrightarrow \mathbb{C}^{n_i \times p_i}$, and the significance of the simultaneous triple product property is that it describes the property of G realizing the collection of tensors $\{\langle m_i, p_i, q_i \rangle\}_{i \,\epsilon\, I}$ via a collection $\{(S_i, T_i, U_i)\}_{i \,\epsilon\, I}$ of index triples in such a way that $|I|$ simultaneous, independent matrix multiplications can be reduced to one multiplication in its regular group algebra $\mathbb{C}G$, with a complexity not exceeding the rank of the algebra.

5.1.2 *Group-Algebra Embedding and Complexity of Simultaneous, Independent Matrix Multiplications*

Theorem 5.1 *If $\{\langle m_i, p_i, q_i \rangle\}_{i \,\epsilon\, I} \subseteq \mathfrak{S}(G)$ is a collection of tensors simultaneously realized by a group G then*

$$(1)\ \mathfrak{R}\left(\bigoplus_i \langle m_i, p_i, q_i \rangle\right) \leq \mathfrak{R}(\mathfrak{m}_{\mathbb{C}G}) \leq \sum_{\varrho \,\epsilon\, Irrep(G)} \mathfrak{R}\left(\langle d_\varrho, d_\varrho, d_\varrho \rangle\right)$$

and iff in addition G is Abelian then

$$(2)\ \mathfrak{R}\left(\bigoplus_i \langle m_i, p_i, q_i \rangle\right) \leq |G| = \mathfrak{R}(\mathfrak{m}_{\mathbb{C}G}).$$

Proof. The procedure used here is a natural generalization of *Theorem 4.13*. If $S_v, T_v, U_v \subseteq G$, $1 \leq v \leq r$, is a collection of r triples satisfying the simultaneous triple product property, and $\{(A_v, B_v)\}_{v=1}^{r}$ is a given collection of r pairs of $m_v \times p_v$ and $p_v \times q_v$ matrices $A_v = (A_{i_v j_v})$ and $B_v = \left(B_{j_v' k_v}\right)$ respectively, then we embed these pairs in $\mathbb{C}G$ as

$$\begin{aligned} \mathfrak{a}_v\left(A_v\right) &= \overline{A}_v = \sum_{s_v \,\epsilon\, S_v,\, t_v \,\epsilon\, T_v} A_{s_v,t_v} s_v^{-1} t_v \\ \mathfrak{b}_v\left(B_v\right) &= \overline{B}_v = \sum_{t_v' \,\epsilon\, T_v,\, u_v \,\epsilon\, U_v} B_{t_v',u_v} t_v'^{-1} u_v \end{aligned}$$

via pairs of injective, linear embedding maps $\mathfrak{a}_v : \mathbb{C}^{m_v \times p_v} \longrightarrow \mathbb{C}G$ and $\mathfrak{b}_v : \mathbb{C}^{p_v \times q_v} \longrightarrow \mathbb{C}G$, using the triples S_v, T_v, U_v, one triple for each pair, just as described in *Theorem 4.13*. For each v, the $(i_v, k_v)^{th}$ entry $C_{i_v k_v}$ of the product $C_v = A_v B_v$ is given by $C_{i_v j_v} = \sum\limits_{j_v = j_v'} A_{i_v j_v} B_{j_v k_v}$. The product of $\overline{A}_v$ and $\overline{B}_v$ in $\mathbb{C}G$ is given by

$$\begin{aligned} \overline{A}_v \overline{B}_v &= \sum_{s_v \,\epsilon\, S_v,\, t_v \,\epsilon\, T_v} A_{s_v,t_v} s_v^{-1} t_v \cdot \sum_{t_v' \,\epsilon\, T_v,\, u_v \,\epsilon\, U_v} B_{t_v',u_v} t_v'^{-1} u_v \\ &= \sum_{s_v \,\epsilon\, S_v,\, t_v \,\epsilon\, T_v} \; \sum_{t_v' \,\epsilon\, T_v,\, u_v \,\epsilon\, U_v} A_{s_v,t_v} B_{t_v',u_v} s_v^{-1} t_v t_v'^{-1} u_v \\ &= \sum_{s_v \,\epsilon\, S_v,\, u_v \,\epsilon\, U_v} \left(\sum_{t_v, t_v' \,\epsilon\, T_v} A_{s_v,t_v} B_{t_v',u_v} t_v t_v'^{-1} \right) s_v^{-1} u_v. \end{aligned}$$

As in the proof of *Theorem 4.13* for a given v, we can recover the matrix product $C_v = A_v B_v$ from $\overline{A}_v \overline{B}_v$ by a linear, injective extraction map $\mathfrak{x}_v : \mathbb{C}^{m_v \times q_v} \longleftarrow \mathbb{C}G$ defined on the fact that for arbitrary $s_v' \,\epsilon\, S_v$, $u_v' \,\epsilon\, U_v$, the sum of those terms of $\overline{A}_v \overline{B}_v$ for which $t_v' = t_v$ all have the group term $s_v'^{-1} u_v'$, and the sum of coefficients of these terms, $\sum\limits_{t_v = t_v' \,\epsilon\, T_v} A_{s_v',t_v} B_{t_v,u_v'}$, corresponds 1-to-1 with the $(i_v, k_v)^{th}$ entry $C_{i_v k_v}$ of $C_v = A_v B_v$. If $\mathfrak{c}_v$ denotes the embedding map $\mathbb{C}^{m_v \times q_v} \longrightarrow \mathbb{C}G$, this shows that $\mathfrak{x}_v(\overline{A}_v \overline{B}_v) = C_v = \mathfrak{c}_v^{-1}\left(\overline{C}_v\right)$. For each v, we have the composition $\mathfrak{x}_v \circ \mathfrak{m}_{\mathbb{C}G} \circ \left(\mathfrak{a}_v \times \mathfrak{b}_v\right)\left(A_v, B_v\right) = C_v \,\epsilon\, \mathbb{C}^{m_v \times q_v}$, by which we have the restrictions $\mathfrak{x}_v \circ \mathfrak{m}_{\mathbb{C}G} \circ \left(\mathfrak{a}_v \times \mathfrak{b}_v\right) = \langle m_v, p_v, q_v \rangle$ of $\mathfrak{m}_{\mathbb{C}G}$ to $\langle m_v, p_v, q_v \rangle$, i.e. $\langle m_v, p_v, q_v \rangle \leq_{\mathbb{C}} \mathfrak{m}_{\mathbb{C}G}$, by which we deduce $\mathfrak{R}\left(\langle m_v, p_v, q_v \rangle\right) \leq_{\mathbb{C}} \mathfrak{R}\left(\mathfrak{m}_{\mathbb{C}G}\right)$ (*Proposition 2.2*).

Now we prove that these restrictions are simultaneous and independent. We define the direct sum matrices $A = \overset{r}{\underset{v=1}{\oplus}} A_v \in \overset{r}{\underset{v=1}{\oplus}} \mathbb{C}^{m_v \times p_v}$, and $B = \overset{r}{\underset{v=1}{\oplus}} B_v \in \overset{r}{\underset{v=1}{\oplus}} \mathbb{C}^{p_v \times q_v}$. The product $AB \in \overset{r}{\underset{v=1}{\oplus}} \mathbb{C}^{m_v \times q_v}$ is the direct sum $\overset{r}{\underset{v=1}{\oplus}} A_v B_v$ of the r block products $A_v B_v$ of blocks A_v and B_v of dimensions $m_v \times p_v$ and $p_v \times q_v$ respectively. We embed A and B in $\mathbb{C}G$ by linear embedding maps $\mathfrak{a}$ and $\mathfrak{b}$ defined by

$$\begin{aligned} \mathfrak{a}(A) &= \overline{A} = \sum_{v=1}^{r} \sum_{s_v \in S_v,\, t_v \in T_v} A_{s_v,t_v} s_v^{-1} t_v = \sum_{v=1}^{r} \overline{A}_v \\ \mathfrak{b}(B) &= \overline{B} = \sum_{v=1}^{r} \sum_{t'_v \in T_v,\, u_v \in U_v} B_{t'_v,u_v} t_v^{'-1} u_v = \sum_{v=1}^{r} \overline{B}_v. \end{aligned}$$

Clearly, $\mathfrak{a} = \sum_{v=1}^{r} \mathfrak{a}_v$ and $\mathfrak{b} = \sum_{v=1}^{r} \mathfrak{b}_v$, and are injective by the injectivity of the $\mathfrak{a}_v$ and $\mathfrak{b}_v$. The product of $\overline{A}$ and $\overline{B}$ in $\mathbb{C}G$ is given by:

$$\begin{aligned} \overline{AB} &= \sum_{v=1}^{r} \overline{A}_v \sum_{v=1}^{r} \overline{B}_v \\ &= \sum_{v=1}^{r} \sum_{w=1}^{r} \sum_{s_v \in S_v,\, t_v \in T_v} \sum_{t'_w \in T_w,\, u_w \in U_w} A_{s_v,t_v} B_{t'_w,u_w} s_v^{-1} t_v t_w^{'-1} u_w \\ &= \sum_{v=1}^{r} \sum_{w=1}^{r} \left(\sum_{s_v \in S_v,\, t_v \in T_v} \sum_{t'_w \in T_w,\, u_w \in U_w} A_{s_v,t_v} B_{t'_w,u_w} t_v t_w^{'-1} \right) s_v^{-1} u_w. \end{aligned}$$

If we use a third index $1 \leq l \leq r$, then by the simultaneous triple product property, for arbitrary $s'_l \in S_l$, $u'_l \in U_l$, it is the case that $s_l^{'-1} u'_l = s_v^{-1} t_v t_w^{'-1} u_w \iff s'_l s_v^{-1} = t_v t_w^{'-1} = u_w u_l^{'-1} = 1 \iff l = v = w$. This means that for each v, and $s_v \in S_v$ and $u_v \in U_v$, the coefficient of the term $s_v^{-1} u_v$ in the product $\overline{AB}$ is $\sum_{t_v \in T_v} A_{s_v,t_v} B_{t_v,u_v} = (A_v B_v)_{s_v,u_v}$. In this way, we can recover the r block products $A_1 B_1, A_2 B_2, ..., A_r B_r$ *simultaneously* from $\overline{AB}$, and each block $A_v B_v$ will be the v^{th} diagonal block on the block diagonal product AB. If we define an extraction map $\mathfrak{x} : \mathbb{C}^{m \times q} \longleftarrow \mathbb{C}G$ based on this rule, then $\mathfrak{x} = \overset{r}{\underset{v=1}{\oplus}} \mathfrak{x}_v$ where $\mathbb{C}^{m \times q} = \overset{r}{\underset{v=1}{\oplus}} \mathbb{C}^{m_v \times q_v}$, and we have shown the following restriction $\mathfrak{x} \circ \mathfrak{m}_{\mathbb{C}G} \circ (\mathfrak{a} \times \mathfrak{b})(A, B) = AB \in \mathbb{C}^{m \times q}$ of $\mathfrak{m}_{\mathbb{C}G}$ to $\langle m, p, q \rangle$, i.e. $\langle m, p, q \rangle \leq_{\mathbb{C}} \mathfrak{m}_{\mathbb{C}G}$, by which we deduce $\mathfrak{R}(\langle m, p, q \rangle) \leq \mathfrak{R}(\mathfrak{m}_{\mathbb{C}G})$ (*Proposition 2.2*). By

Proposition 2.5, $\langle m,p,q\rangle = \left\langle \sum_{v=1}^{r} m_v, \sum_{v=1}^{r} p_v, \sum_{v=1}^{r} q_v \right\rangle \cong \bigoplus_{v=1}^{r} \langle m_v,p_v,q_v\rangle$, and by *Proposition 2.2*

$$\mathfrak{R}\left(\bigoplus_{v=1}^{r}\langle m_v,p_v,q_v\rangle\right) \leq \mathfrak{R}\left(\mathfrak{m}_{\mathbb{C}G}\right).$$

This takes care of (1). For (2) we note that note that $\mathfrak{R}\left(\mathfrak{m}_{\mathbb{C}G}\right) = |G|$ iff G is Abelian. ■

An immediate consequence is the following.

Corollary 5.2 *If* $\{\langle m_i,p_i,q_i\rangle\}_{i\,\epsilon\, I} \subseteq \mathfrak{S}(G)$ *is a collection of tensors simultaneously realized by a group* G *then*

$$(1)\sum_{i\,\epsilon\, I}\left(m_ip_iq_i\right)^{\frac{\omega}{3}} \leq D_\omega(G)$$

and if G *is Abelian*

$$(2)\ \sum_{i\,\epsilon\, I}\left(m_ip_iq_i\right)^{\frac{\omega}{3}} \leq |G|.$$

Proof. Assume that $\{\langle m_i,p_i,q_i\rangle\}_{i\,\epsilon\, I} \subseteq \mathfrak{S}(G)$ is a collection of tensors simultaneously realized by G. (1) By part (1) of *Theorem 5.1, (3.18)* and *Proposition 2.14*

$$\sum_{i\,\epsilon\, I}\left(m_ip_iq_i\right)^{\frac{\omega}{3}} \leq \mathfrak{R}\left(\bigoplus_{i\,\epsilon\, I}\langle m_i,p_i,q_i\rangle\right) \leq \mathfrak{R}\left(\mathfrak{m}_{\mathbb{C}G}\right) \leq \sum_{\varrho\,\epsilon\, Irrep(G)} \mathfrak{R}\left(\langle d_\varrho,d_\varrho,d_\varrho\rangle\right).$$

(1) On the right-hand side, by *Proposition 3.13* $D_\omega\left(G\right) = \sum_{\varrho\,\epsilon\, Irrep(G)} d_\varrho^\omega \leq \sum_{\varrho\,\epsilon\, Irrep(G)} \mathfrak{R}\left(\langle d_\varrho,d_\varrho,d_\varrho\rangle\right)$. Since $\langle m_i,p_i,q_i\rangle\ \epsilon\ \mathfrak{S}(G)$, by *Corollary 4.16*, it follows that $\left(m_ip_iq_i\right)^{\frac{\omega}{3}} < |G|^{\frac{\omega}{2}} = D_2\left(G\right)^{\frac{\omega}{2}} \leq D_\omega\left(G\right)^{\frac{\omega}{2}}$. Thus,

$$\begin{array}{ccc} \sum_{i\,\epsilon\, I}\left(m_ip_iq_i\right)^{\frac{\omega}{3}} & < & |I|\, D_\omega\left(G\right)^{\frac{\omega}{2}} \\ & \Longleftrightarrow & \\ \sum_{i\,\epsilon\, I}\left(m_ip_iq_i\right)^{\frac{\omega}{3}} & \leq & |I|^{-\frac{2}{\omega}}\left(\sum_{i\,\epsilon\, I}\left(m_ip_iq_i\right)^{\frac{\omega}{3}}\right)^{\frac{2}{\omega}} < D_\omega\left(G\right) \end{array}$$

(2) $D_r(G) = |G|$ for all $r \geq 1$ iff G is Abelian, and the result follows by (1). ■

Part (2) of *Corollary 5.2* points to the usefulness of Abelian groups for estimates of ω, for which we have the following useful corollary.

Corollary 5.3 *If* $\{\langle n,n,n\rangle\}_{i=1}^{r}$ *is a collection of* r *identical square tensors* $\langle n,n,n\rangle$ *simultaneously realized by an Abelian group* G *then*

$$(1)\ \omega \leq \frac{\log|G| - \log r}{\log n}$$

and

$$(2)\ \omega = 2 \text{ if } |G| = n^3 \text{ and } r = n.$$

Proof. Consequence of part (2) of *Corollary 5.2.* ■

5.1.3 *Extension Results*

The following is a basic extension of the simultaneous triple product property to direct product groups.

Lemma 5.4 *If groups* G *and* $G^{'}$ *have collections of simultaneous index triples* $\{(S_i,T_i,U_i)\}_{i\ \epsilon\ I}$, $\left\{(S^{'}_{i'},T^{'}_{i'},U^{'}_{i'})\right\}_{i'\ \epsilon\ I'}$ *of sizes* r *and* $r^{'}$ *resp., then their direct product* $G\times G^{'}$ *has the collection of* $rr^{'}$ *simultaneous index triples* $\left\{(S_i\times S^{'}_{i'},T_i\times T^{'}_{i'},U_i\times U_{i'})\right\}_{i\ \epsilon\ I,\ i'\epsilon\ I'}$.

Proof. For arbitrary indices $i,j,k\ \epsilon\ I$ and $i^{'},j^{'},k^{'}\ \epsilon\ I^{'}$, and elements $\left(s_i,s^{'}_{i'}\right)\ \epsilon\ S_i\times S^{'}_{i'}$, $\left(\overline{s}_j,\overline{s}^{'}_{j'}\right)\ \epsilon\ S_j\times S^{'}_{j'}$, $\left(t_j,t^{'}_{j'}\right)\ \epsilon\ T_j\times T^{'}_{j'}$, $\left(\overline{t}_k,\overline{t}^{'}_{k'}\right)\ \epsilon\ T_k\times T^{'}_{k'}$, $\left(u_k,u^{'}_{k'}\right)\ \epsilon\ U_k\times U^{'}_{k'}$, $\left(\overline{u}_i,\overline{u}^{'}_{i'}\right)\ \epsilon\ U_i\times U^{'}_{i'}$, and the assumption of the simultaneous triple product property for both the collections $\{(S_i,T_i,U_i)\}_{i\ \epsilon\ I}$ and $\left\{(S^{'}_{i'},T^{'}_{i'},U^{'}_{i'})\right\}_{i'\ \epsilon\ I'}$ it is the case that:

$$\begin{aligned}
& \left(s_i,s^{'}_{i'}\right)\left(\overline{s}_j,\overline{s}^{'}_{j'}\right)^{-1}\left(t_j,t^{'}_{j'}\right)\left(\overline{t}_k,\overline{t}^{'}_{k'}\right)^{-1}\left(u_k,u^{'}_{k'}\right)\left(\overline{u}_i,\overline{u}^{'}_{i'}\right)^{-1} \\
= \quad & \left(s_i\overline{s}_j^{-1},s^{'}_{i'}\overline{s}^{'-1}_{j'}\right)\left(t_j\overline{t}_k^{-1},t^{'}_{j'}\overline{t}^{'-1}_{k'}\right)\left(u_k\overline{u}_i^{-1},u^{'}_{k'}\overline{u}^{'-1}_{i'}\right) \\
= \quad & \left(s_i\overline{s}_j^{-1}t_j\overline{t}_k^{-1}u_k\overline{u}_i^{-1},s^{'}_{i'}\overline{s}^{'-1}_{j'}t^{'}_{j'}\overline{t}^{'-1}_{k'}u^{'}_{k'}\overline{u}^{'-1}_{i''}\right)=(1_G,1_{G'}) \\
\iff \quad & s_i\overline{s}_j^{-1}t_j\overline{t}_k^{-1}u_k\overline{u}_i^{-1}=1_G,\ s^{'}_{i'}\overline{s}^{'-1}_{j'}t^{'}_{j'}\overline{t}^{'-1}_{k'}u^{'}_{k'}\overline{u}^{'-1}_{i''}=1_{G'} \\
\implies \quad & s_i\overline{s}_j^{-1}t_j\overline{t}_k^{-1}u_k\overline{u}_i^{-1}=1_G,\ s^{'}_{i'}\overline{s}^{'-1}_{j'}t^{'}_{j'}\overline{t}^{'-1}_{k'}u^{'}_{k'}\overline{u}^{'-1}_{i''}=1_{G'} \text{ and} \\
i \quad = \quad & j,\ j=k,\ k=i,\ i^{'}=j^{'},\ j^{'}=k^{'},\ k^{'}=i^{'}.
\end{aligned}$$

■

This has an equivalent statement in terms of tensors.

Corollary 5.5 *If groups G and G' have collections of simultaneously realized tensors $\{\langle m_i, p_i, q_i\rangle\}_{i\,\epsilon\, I}$ and $\left\{\left\langle m'_{i'}, p_{i'}, q'_{i'}\right\rangle\right\}_{i'\,\epsilon\, I'}$ of sizes r and r' resp., then their direct product $G \times G'$ has the collection of rr' simultaneously realized pointwise product tensors $\left\{\left\langle m_i m'_{i'}, p_i p'_{i'}, q_i q'_{i'}\right\rangle\right\}_{i\,\epsilon\, I,\ i'\epsilon\, I'}$.*

Lemma 5.4 and *Corollary 5.5* are also independent consequences of *Lemma 4.8* and *Lemma 4.12* using the simultaneous triple product property *(5.2)*.

5.2 Some Useful Groups

Here we describe some special types of finite groups of particular interest to our problem.

5.2.1 *The Triangle Set Δ_n and the Symmetric Group $Sym_{n(n+1)/2}$*

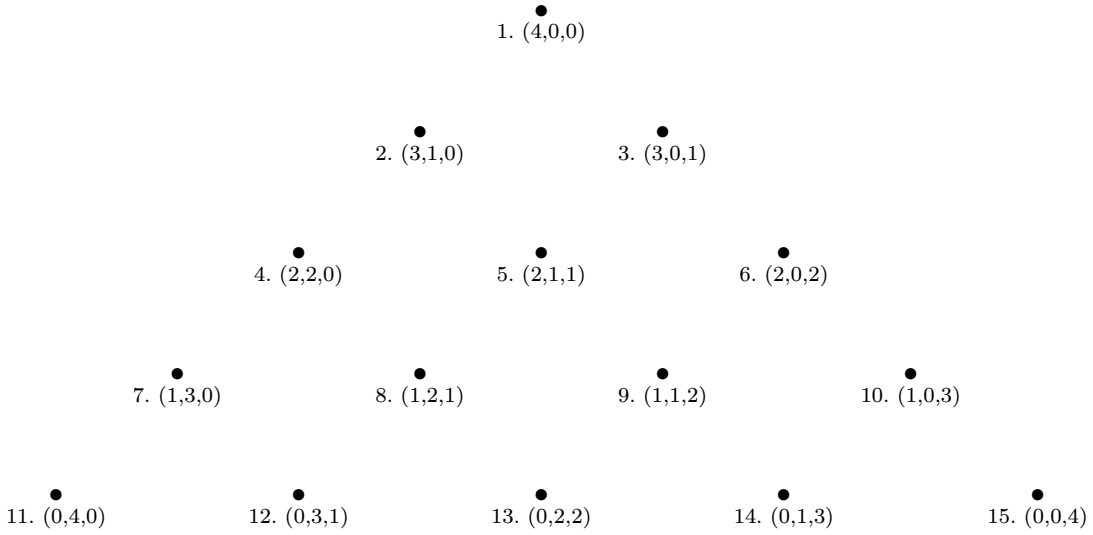
For an arbitrary fixed $n \geq 1$, we define the *triangle set* Δ_n by:

(5.3) $\Delta_n := \left\{x = (x_1, x_2, x_3)\ \epsilon\, \mathbb{N}^3 \mid x_1 + x_2 + x_3 = n - 1\right\}$.

Δ_n is of size $|\Delta_n| = \sum_{k=1}^{n} k = 1 + 2 + \cdots + n = n(n+1)/2$. The following is a table for Δ_5 ($n = 5$) written lexicographically:

	x_1	x_2	x_3	$x_1{+}x_2{+}x_3$		x_1	x_2	x_3	$x_1{+}x_2{+}x_3$		x_1	x_2	x_3	$x_1{+}x_2{+}x_3$
1.	4	0	0	4	6.	2	0	2	4	11.	0	4	0	4
2.	3	1	0	4	7.	1	3	0	4	12.	0	3	1	4
3.	3	0	1	4	8.	1	2	1	4	13.	0	2	2	4
4.	2	2	0	4	9.	1	1	2	4	14.	0	1	3	4
5.	2	1	1	4	10.	1	0	3	4	15.	0	0	4	4

The smallest triple in Δ_n is $(0, 0, n-1)$ and the largest $(n-1, 0, 0)$. The i^{th} component x_i of any triple $(x_1, x_2, x_3)\ \epsilon\ \Delta_n$ can take any one of n values $0, 1, 2, ..., .n-1$, and for any value $0 \leq k \leq n-1$ and component index $1 \leq i \leq 3$, there are exactly $n-k$ triples $(x_1, x_2, x_3)\ \epsilon\ \Delta_n$ with the i^{th} component $x_i = k$. This is a representation of Δ_5 as a triangular array or pyramid of dot elements:

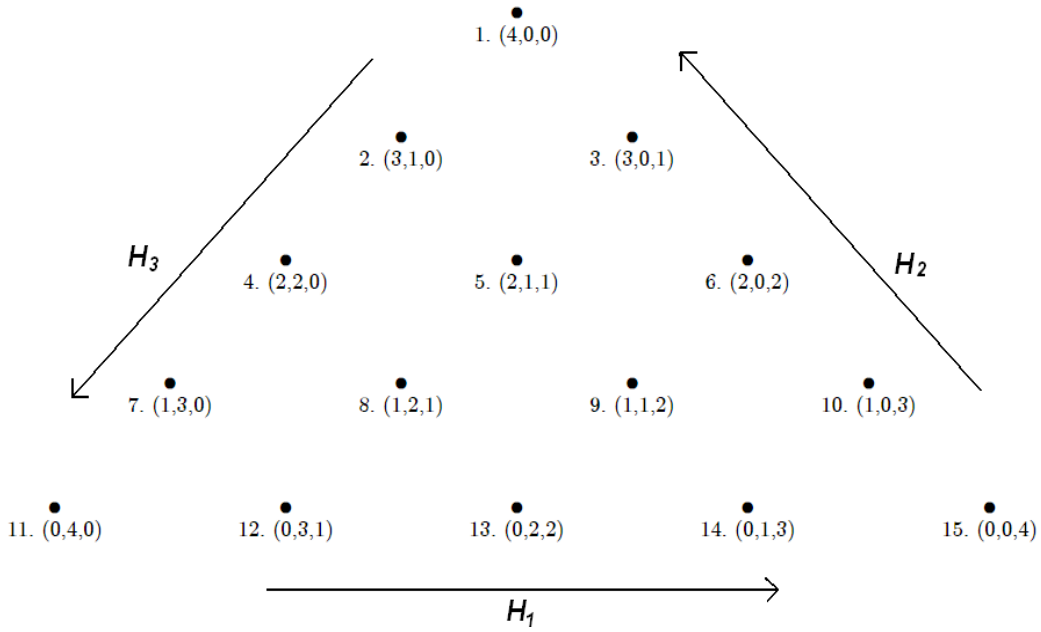


Counting the rows of this pyramid from the lowest, for $0 \leq k \leq n-1 = 4$, the k^{th} row of dots correspond to the subset of triples in Δ_5 with 1^{st} component $x_1 = k$, and in the k^{th} row each element is ordered component-wise descending order from left to right. This is precisely the lexicographic (dictionary) ordering of the elements of Δ_n. $Sym_{n(n+1)/2}$ can be understood as the permutation group of Δ_n, and we may write $Sym_{n(n+1)/2} \equiv Sym(\Delta_n)$. $Sym(\Delta_n)$ is of order $\left(\frac{1}{2}n(n+1)\right)!$. Elements $\mu\ \epsilon\ Sym(\Delta_n)$ are bijective maps $\Delta_n \cong \Delta_n$ and their actions on the components of triples $x = (x_1, x_2, x_3)\ \epsilon\ \Delta_n$ is defined by $x_i \longmapsto \mu(x)_i$, $1 \leq i \leq 3$, where $\mu(x)_i$ denotes the i^{th} component of the permuted triple $\mu(x)$. Graphically, the permutations $\mu\ \epsilon\ Sym(\Delta_n)$ are bijective transformations, such as rotations or reflections, of Δ_n or of any subset of points of Δ_n.

We define the subsets $Sym_i(\Delta_n) \subseteq Sym(\Delta_n)$ by:

(5.4) $Sym_i(\Delta_n) := \{\mu \,\epsilon\, Sym(\Delta_n) \mid \mu(x)_i = x_i,\ x \,\epsilon\, \Delta_n\}, \qquad 1 \leq i \leq 3.$

Each $Sym_i(\Delta_n)$ forms a fixed-point subgroup of $Sym(\Delta_n)$ consisting of those permutations of Δ_n leaving the i^{th} components of triples $x \,\epsilon\, \Delta_n$ fixed. For any value $0 \leq k \leq n-1$ and index $1 \leq i \leq 3$, there are exactly $n-k$ triples in Δ_n with i^{th} component $x_i = k$, there are $(n-k)!$ permutations of these triples, and for each $1 \leq i \leq 3$, there are $n!(n-1)! \cdots 2!1!$ permutations of Δ_n which fix the i^{th} components of triples $x \,\epsilon\, \Delta_n$, and $|Sym_i(\Delta_n)| = n!(n-1)! \cdots 2!1!$. Graphically, the subgroups $Sym_i(\Delta_n) \leq Sym\,(\Delta_n)$ are collections of permutations $\mu_i \,\epsilon\, Sym\,(\Delta_n)$ transforming Δ_n solely along the diagonal rows parallel to its i^{th} side, one subgroup for each side. The following is a diagram for $Sym_1(\Delta_5), Sym_2(\Delta_5), Sym_3(\Delta_5)$ on Δ_5.



The diagram above makes it clear that these fixed point subgroups have the triple product property.

Lemma 5.6 *The subgroups $Sym_1(\Delta_n)$, $Sym_2(\Delta_n)$, $Sym_3(\Delta_n) \leq Sym\,(\Delta_n)$, defined in (5.2), form an index triple of $Sym\,(\Delta_n)$.*

Proof. Since $Sym_i(\Delta_n) \leq Sym(\Delta_n)$, $1 \leq i \leq 3$, to prove the triple product property for these, it suffices to prove for arbitrary $\mu_1 \epsilon Sym_1(\Delta_n)$, $\mu_2 \epsilon Sym_2(\Delta_n)$, and $\mu_3 \epsilon Sym_3(\Delta_n)$ that $\mu_1\mu_2\mu_3 = 1$ implies that $\mu_1 = \mu_2 = \mu_3 = 1$. For a $\mu \epsilon Sym(\Delta_n)$, we define its fixed point set as $fix(\mu) = \{x \epsilon \Delta_n \mid \mu(x) = x\} \subseteq \Delta_n$, and its i^{th} component fixed point set $fix_i(\mu)$ as $fix_i(\mu) = \{x \epsilon \Delta_n \mid \mu(x)_i = x_i\} \subseteq \Delta_n$. For arbitrary $\mu \epsilon Sym(\Delta_n)$, the sets $fix(\mu)$ and $fix_i(\mu)$ are such that $\mu = 1$ iff $fix(\mu) \cap fix_i(\mu) = \Delta_n$, for all $1 \leq i \leq 3$, where 1 is the identity permutation of Δ_n. Moreover, $fix(\mu) \subseteq fix_i(\mu)$. Then, from $\mu_1\mu_2\mu_3 = 1$ it follows that $fix(\mu_1\mu_2\mu_3) \cap fix_i(\mu_1\mu_2\mu_3) = fix(\mu_1\mu_2\mu_3) = \Delta_n$, $1 \leq i \leq 3$. Since $fix_1(\mu_1) = fix_2(\mu_2) = fix_3(\mu_3) = \Delta_n$, it follows that $fix(\mu_1) = fix(\mu_2) = fix(\mu_3) = \Delta_n$. Together, $fix(\mu_1\mu_2\mu_3) = \Delta_n$ and $fix(\mu_i) = \Delta_n$, $1 \leq i \leq 3$, implies that $fix_i(\mu_1\mu_2) = fix_i(\mu_2\mu_3) = fix_i(\mu_1\mu_3) = \Delta_n$, $1 \leq i \leq 3$, which implies that $fix(\mu_1\mu_2) = fix(\mu_2\mu_3) = fix(\mu_1\mu_3) = \Delta_n$, $1 \leq i \leq 3$, which implies that $\mu_1\mu_2 = \mu_2\mu_3 = \mu_1\mu_3 = 1$, from which we deduce that $\mu_1 = \mu_2 = \mu_3 = 1$. ■

This shows that $Sym(\Delta_n)$ realizes the tensor $\left\langle \prod_{k=1}^{n} k!, \prod_{k=1}^{n} k!, \prod_{k=1}^{n} k! \right\rangle$, which means that it supports square matrix multiplication of order $\prod_{k=1}^{n} k!$, and, therefore, by *(4.21)*, we have:

(5.5) $\alpha(Sym(\Delta_n)) \leq \frac{\log\left(\frac{1}{2}n(n+1)\right)!}{\log(n!(n-1)!\cdots 2!1!)}$.

This yields concrete estimates for $\alpha(Sym_m)$, to be described in *Chapter 6*.

5.2.2 *Semidirect Product and Wreath Product Groups*

A group G is said to be the (*internal*) *semidirect product* $A \rtimes B$ of a subgroup $B \leq G$ by a normal subgroup $A \lhd G$, if $A \cap B = \{1_G\}$ and $G = AB$. Each elements $g \epsilon G = A \rtimes B$ has the form $g = ab$ for a unique element $a \epsilon A$ and a $b \epsilon B$ depending on a, and by $A \lhd G$, it is the case that $b^{-1}g = b^{-1}ab \epsilon A$. For a fixed $b \epsilon B$, the mapping $a \longmapsto bab^{-1} \equiv a^b$, $a \epsilon A$, defines an automorphism α_b of A which is conjugation of A by b, and the mapping $b \longmapsto \alpha_b$, $b \epsilon B$, is a group homomorphism $\alpha : B \longrightarrow Aut(A)$ defining the conjugation action of B on A, such that multiplication of elements $g = (ab), g' = (a'b') \epsilon G$ can be expressed as $gg' = (ab)(a'b') = (aba'b^{-1}bb') = (aa'^b)(bb') = (a\alpha_b(a'))(bb')$, and inverses of elements $g = ab$

are given by $g^{-1} = \alpha_{b^{-1}}(a^{-1})b^{-1}$. If $B \lhd G$ also then $G = A \rtimes B = A \times B$. If A and B are arbitrary groups, then for any homomorphism $\phi : B \longrightarrow Aut(A)$ there is a unique (*external*) *semidirect product* $A \rtimes B$ of B by A, with underlying set $A \times B$, for which $\alpha_b = \phi(b)$ for any $b \in B$, and $A \cong A \rtimes \{1_B\} \equiv [A] \lhd A \rtimes B$ and $B \cong \{1_A\} \rtimes B \equiv [B] \leq A \rtimes B$ such that $[A] \cap [B] = \{1_G\}$ and $G = [A][B]$. Every external semidirect product $A \rtimes B$ of groups A and B is the internal semidirect product $[A] \rtimes [B]$ of the subgroups $[A] \lhd A \rtimes B, [B] \leq A \rtimes B$. If $\pi : G \longrightarrow GL(V)$ is any nontrivial representation of G, and ι_A denotes the inclusion homomorphism $A \longrightarrow G = A \rtimes B$, then $\pi_A \equiv \pi \circ \iota_A$ is the representation $A \longrightarrow GL(V)$ of A equidimensional with π and a nontrivial subrepresentation of π. If π_A is irreducible then π must be irreducible, while any irreducible representation ϱ_B of B extends to a unique irreducible representation ϱ of G. For an Abelian subgroup $A \lhd G$ and a subgroup $B \leq G$ there is a proper subgroup $C < B$ such that an irreducible representation of $A \lhd G$.extends to an irreducible representation of $G = A \rtimes B$.

A special kind of semidirect product group $G = A \rtimes B$ exists when $A = H^n$, the n-fold direct product of H, with H being a group, and $B = Sym_n$, where multiplication in H^n is component-wise multiplication of n-tuples $h = (h_i)_{i=1}^n$ of elements of H, and multiplication in Sym_n is the composition of permutations μ of n elements. This group $G = H^n \rtimes Sym_n$ is called the *wreath product* of Sym_n by H^n, denoted by $H \wr Sym_n$, where the action of Sym_n on H_n is from the right, defined by the mapping $h \longmapsto h^\mu := (h_{\mu i})_{i=1}^n$, for n-tuples $h = (h_i)_{i=1}^n \in H^n$ and permutations $\mu \in Sym_n$, i.e. , Sym_n acts on H_n by permuting the components of its n-tuples. We sometimes write $(h)_i$ for the i^{th} coordinate h_i of an $h = (h_i)_{i=1}^n \in H^n$. H is called the base group of $H \wr Sym_n$, and if we identity H^n with the subgroup $\{h 1_{Sym_n} \mid h \in H^n\} \leq H \wr Sym_n$, then $H^n \lhd H \wr Sym_n$ and $H \wr Sym_n$ becomes an internal semidirect product. Multiplication in $H \wr Sym_n$ is given by $(h\mu)(h'\mu') = (hh'^{\mu^{-1}})(\mu\mu') = (h_i h'_{\mu^{-1}i})_{i=1}^n(\mu\mu')$, and inverses $(h\mu)^{-1}$ by $h^\mu \mu^{-1} = (h_{\mu i})_{i=1}^n \mu^{-1}$, for elements $(h\mu), (h'\mu') \in H \wr Sym_n$. The following is an elementary result about the sums of ω^{th} powers of the irreducible character degrees of $H \wr Sym_n$.

Lemma 5.7 *For an Abelian group H, $D_\omega(H \wr Sym_n) \leq (n!)^{\omega-1} |H|^n$.*

Proof. For an Abelian group H, and the wreath product group $H \wr Sym_n$, every irreducible representation $\varrho \in Irrep(H \wr Sym_n)$ is induced from an irreducible representation of the base

group $H^n \lhd H \wr Sym_n$, which has the index $[H \wr Sym_n : H^n] = |Sym_n| = n!$, [HUP1998]. Therefore, the index $[H \wr Sym_n : N]$ of any maximal Abelian normal subgroup $N \lhd H \wr Sym_n$ is at most $n!$, and by *Theorem 3.7*, $Dim\ \varrho \leq n!$ for any $\varrho \in Irrep(H \wr Sym_n)$. Then:

$$\begin{aligned}
D_\omega(H \wr Sym_n) &= \sum_{\varrho \in Irrep(H \wr Sym_n)} d_\varrho^\omega \\
&= \sum_{\varrho \in Irrep(H \wr Sym_n)} d_\varrho^{\omega-2} d_\varrho^2 \\
&\leq (n!)^{\omega-2} \sum_{\varrho \in Irrep(H \wr Sym_n)} d_\varrho^2 \\
&= (n!)^{\omega-2} |H \wr Sym_n| \\
&= (n!)^{\omega-2} (n!) |H^n| \\
&= (n!)^{\omega-1} |H|^n \\
&= (n!)^{\omega-1} D_2(H)^n \\
&\leq (n!)^{\omega-1} D_\omega(H)^n.
\end{aligned}$$

Since H is Abelian $D_\omega(H) = |H|$, and the result follows. ■

We conclude with some extension results.

Theorem 5.8 *If* $\{(S_i, T_i, U_i)\}_{i=1}^n \subset \mathfrak{J}(H)$ *is a collection of* n *simultaneous index triples of a group* H *then the triple* $\left(\prod_{i=1}^n S_i \wr Sym_n, \prod_{i=1}^n T_i \wr Sym_n, \prod_{i=1}^n U_i \wr Sym_n\right) \in \mathfrak{J}(H \wr Sym_n)$.

Proof. Assume a collection $\{(S_i, T_i, U_i)\}_{i=1}^n \subset \mathfrak{J}(H)$ of index triples of H. By *Lemma 4.8* the n-fold direct product of these triples, $\left(\prod_{i=1}^n S_i = S, \prod_{i=1}^n T_i = T, \prod_{i=1}^n U_i = U\right)$ is an index triple of H^n. Assume further that the triples (S_i, T_i, U_i) have the simultaneous triple product property (STPP). We claim that the subsets

$$\begin{aligned}
S \wr Sym_n &:= \{(s\sigma) \mid s \in S,\ \sigma \in Sym_n\}, \\
T \wr Sym_n &:= \{(t\tau) \mid t \in T,\ \tau \in Sym_n\}, \\
U \wr Sym_n &:= \{(u\upsilon) \mid u \in U,\ \upsilon \in Sym_n\},
\end{aligned}$$

satisfy the triple product property (TPP) in $H \wr Sym_n$. To see this, let $s_1\sigma_1,\ s_1^{'}\sigma_1^{'} \in S \wr Sym_n$, $t_2\tau_2,\ t_2^{'}\tau_2^{'} \in T \wr Sym_n, u_3\upsilon_3,\ u_3^{'}\upsilon_3^{'} \in U \wr Sym_n$ be arbitrary elements. Then

$$\begin{aligned}
& \left(s_1^{'}\sigma_1^{'}\right)(s_1\sigma_1)^{-1}\left(t_2^{'}\tau_2^{'}\right)(t_2\tau_2)^{-1}\left(u_3^{'}\upsilon_3^{'}\right)(u_3\upsilon_3)^{-1} \\
= \quad & s_1^{'}\sigma_1^{'}s_1^{\sigma_1}\sigma_1^{-1}t_2^{'}\tau_2^{'}\tau_2^{\tau_2}\tau_2^{-1}u_3^{'}\upsilon_3^{'}u_3^{\upsilon_3}\upsilon_3^{-1} \\
= \quad & s_1^{'}s_1^{\sigma_1^{'}\sigma_1^{-1}}\sigma_1^{'}\sigma_1^{-1}t_2^{'}t_2^{\tau_2^{'}\tau_2^{-1}}\tau_2^{'}\tau_2^{-1}u_3^{'}u_3^{\upsilon_3^{'}\upsilon_3^{-1}}\upsilon_3^{'}\upsilon_3^{-1} \\
= \quad & 1 \\
\Longrightarrow \quad & \sigma_1^{'}\sigma_1^{-1}\tau_2^{'}\tau_2^{-1}\upsilon_3^{'}\upsilon_3^{-1} = 1.
\end{aligned}$$

Putting $\mu = \sigma_1^{'}\sigma_1^{-1}$ and $\nu = \sigma_1^{'}\sigma_1^{-1}\tau_2^{'}\tau_2^{-1}$ we have that

$$\begin{aligned}
& s_1^{'}s_1^{\sigma_1^{'}\sigma_1^{-1}}\sigma_1^{'}\sigma_1^{-1}t_2^{'}t_2^{\tau_2^{'}\tau_2^{-1}}\tau_2^{'}\tau_2^{-1}u_3^{'}u_3^{\upsilon_3^{'}\upsilon_3^{-1}}\upsilon_3^{'}\upsilon_3^{-1} \\
= \quad & 1 \\
\Longrightarrow \quad & u_3^{-1}s_1^{'}\left(s_1^{-1}t_2^{'}\right)^{\mu}\left(t_2^{-1}u_3^{'}\right)^{\nu} = 1 \\
\Longleftrightarrow \quad & \left(u_3^{-1}\right)_i\left(s_1^{'}\right)_i\left(s_1^{-1}\right)_{\mu i}\left(t_2^{'}\right)_{\mu i}\left(t_2^{-1}\right)_{\nu i}\left(u_3^{'}\right)_{\nu i} = 1 \\
\Longleftrightarrow \quad & \mu i = \nu i = i, 1 \leq i \leq n \text{ (STPP for } \{(S_i, T_i, U_i)\}_{i=1}^{n}\text{)} \\
\Longleftrightarrow \quad & \mu = \nu = 1 \\
\Longleftrightarrow \quad & \sigma_1 = \sigma_1^{'}, \tau_2 = \tau_2^{'}, \upsilon_3 = \upsilon_3^{'}.
\end{aligned}$$

Thus

$$\begin{aligned}
& s_1^{'}s_1^{\sigma_1^{'}\sigma_1^{-1}}\sigma_1^{'}\sigma_1^{-1}t_1^{'}t_1^{\tau_1^{'}\tau_1^{-1}}\tau_1^{'}\tau_1^{-1}u_1^{'}u_1^{\upsilon_1^{'}\upsilon_1^{-1}}\upsilon_1^{'}\upsilon_1^{-1} \\
= \quad & 1 \\
\Longrightarrow \quad & s_1^{'}s_1^{-1}t_2^{'}t_2^{-1}u_3^{'}u_3^{-1} = 1 \\
\Longleftrightarrow \quad & s_1^{'} = s_1, t_2^{'} = t_2, u_3^{'} = u_3 \text{ (TPP for } \{(S_i, T_i, U_i)\}_{i=1}^{n}\text{)}
\end{aligned}$$

Putting these two together we deduce that for $s_1\sigma_1,\ s_1^{'}\sigma_1^{'} \in S \wr Sym_n$, $t_2\tau_2,\ t_2^{'}\tau_2^{'} \in T \wr Sym_n, u_3\upsilon_3$,

$u_3^{'}v_3^{'} \epsilon U \wr Sym_n$ it is the case that

$$\begin{aligned}
& \left(s_1^{'}\sigma_1^{'}\right)(s_1\sigma_1)^{-1}\left(t_2^{'}\tau_2^{'}\right)(t_2\tau_2)^{-1}\left(u_3^{'}v_3^{'}\right)(u_3v_3)^{-1} \\
= \quad & s_1^{'}s_1^{\sigma_1^{'}\sigma_1^{-1}}\sigma_1^{'}\sigma_1^{-1}t_1^{'}t_1^{\tau_1^{'}\tau_1^{-1}}\tau_1^{'}\tau_1^{-1}u_1^{'}u_1^{v_1^{'}v_1^{-1}}v_1^{'}v_1^{-1} \\
= \quad & 1 \\
\iff \quad & s_1^{'}\sigma_1^{'} = s_1\sigma_1, t_2^{'}\tau_2^{'} = t_2\tau_2, u_3^{'}v_3^{'} = u_3v_3.
\end{aligned}$$

This proves our claim. ■

Corollary 5.9 *If* $\{\langle m_i, p_i, q_i\rangle\}_{i=1}^n \subset \mathfrak{S}(H)$ *is a collection of* n *tensors simultaneously realized by an Abelian group* H *then*

$$(1)\ \left\langle n!\prod_{i=1}^n m_i, n!\prod_{i=1}^n p_i, n!\prod_{i=1}^n q_i \right\rangle \epsilon\ \mathfrak{S}(H \wr Sym_n)$$

and

$$(2)\ \omega \leq \frac{n\log|H| - \log n!}{\log\sqrt[3]{\prod_{i=1}^n m_i p_i q_i}}.$$

Proof. If n triples $S_i, T_i, U_i \subseteq H$, $1 \leq i \leq n$, of sizes $|S_i| = m_i$, $|T_{i,}| = p_i$, $|U_i| = q_i$, $1 \leq i \leq n$, satisfy the STPP in an Abelian group H then by *Theorem 5.8* $H \wr Sym_n$ realizes the product tensor $\left\langle n!\prod_{i=1}^n m_i, n!\prod_{i=1}^n p_i, n!\prod_{i=1}^n q_i \right\rangle$ once, and in addition, by *Corollary 5.2* and *Lemma 5.7*,

$$\begin{aligned}
& \left(n!\prod_{i=1}^n m_i \cdot n!\prod_{i=1}^n p_i \cdot n!\prod_{i=1}^n q_i\right)^{\frac{\omega}{3}} \\
= \quad & \left(n!\sqrt[3]{\prod_{i=1}^n m_i p_i q_i}\right)^{\omega} \\
\leq \quad & D_\omega(H \wr Sym_n) \\
\leq \quad & (n!)^{\omega-1}|H|^n.
\end{aligned}$$

Taking logarithms, this is equivalent to

$$\begin{aligned}
\omega \log \left(n! \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i} \right) &\leq (\omega - 1) \log n! + n \log |H| \iff \\
\omega \log n! + \omega \log \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i} &\leq \omega \log n! - \log n! + n \log |H| \iff \\
\omega &\leq \frac{n \log |H| - \log n!}{\log \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i}}.
\end{aligned}$$

■

The bound for ω in *Corollary 5.9* suggests that ω is close to 2 if we could find an Abelian group H simultaneously realizing n tensors $\langle m_i, p_i, q_i \rangle$ such that $\frac{n \log |H| - \log n!}{\log \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i}}$ is close to 2, and the following proposition is an obvious extension.

Proposition 5.10 *For any n, given n triples $S_i, T_i, U_i \subseteq H$ of sizes $|S_i| = m_i, |T_i| = p_i, |U_i| = q_i$, $1 \leq i \leq n$ satisfying the STPP in an Abelian group H, and the corresponding product triple $\prod_{i=1}^{n} S_i \wr Sym_n, \prod_{i=1}^{n} T_i \wr Sym_n, \prod_{i=1}^{n} U_i \wr Sym_n$ satisfying the TPP in the wreath product group $H \wr Sym_n$, there is a maximum number $1 \leq k_n \leq (n!)^3$ triples of permutations, $\sigma_j, \tau_j, \upsilon_j \in Sym_n$, $1 \leq j \leq k_n$, such that the k_n permuted product triples $\prod_{i=1}^{n} S_{\sigma_j(i)} \wr Sym_n, \prod_{i=1}^{n} T_{\tau_j(i)} \wr Sym_n, \prod_{i=1}^{n} U_{\upsilon_j(i)} \wr Sym_n$, $1 \leq j \leq k_n$, satisfy the STPP in $H \wr Sym_n$, and $H \wr Sym_n$ realizes the square product tensor $\left\langle n! \prod_{i=1}^{n} m_i, n! \prod_{i=1}^{n} p_i, n! \prod_{i=1}^{n} q_i \right\rangle$ k_n times simultaneously, such that*

$$\omega \leq \frac{n \log |H| - \log n! - \log k_n}{\log \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i}}.$$

The proof of this result once again uses the result $D_\omega(H \wr Sym_n) \leq (n!)^{\omega - 1} |H|^n$ for an Abelian group H (*Lemma 5.7*), in combination with *Corollary 5.2*, as described in the proof of *Corollary 5.9*. By *Theorem 5.8* we know that $k_n \geq 1$ for any given n, given n STPP triples $S_i, T_i, U_i \subseteq H$ of sizes $|S_i| = m_i, |T_i| = p_i, |U_i| = q_i$, $1 \leq i \leq n$. If the $\sigma_j, \tau_j, \upsilon_j \in Sym_n$,

$1 \leq j \leq k_n$, are taken independently of each other in Sym_n, there are a maximum number $(n!)^3$ of permuted triples $\prod_{i=1}^{n} S_{\sigma(i)} \wr Sym_n, \prod_{i=1}^{n} T_{\tau(i)} \wr Sym_n, \prod_{i=1}^{n} U_{\upsilon(i)} \wr Sym_n$, $\sigma, \tau, \upsilon \in Sym_n$, and if these satisfy the STPP in $H \wr Sym_n$, it leads to the conditional estimate $\omega < 2.012$ using the wreath product group $\left(Cyc_6^{\times 3}\right)^{\times 6} \wr Sym_{2^6}$, as described in section *6.2.3*. For a given n, there is no known general method of determining k_n for the group $H \wr Sym_n$, with H being Abelian and having a family of n STPP triples $S_i, T_i, U_i \subseteq H$ of sizes $|S_i| = m_i, |T_i| = p_i, |U_i| = q_i$, $1 \leq i \leq n$. The objective is to find the number $1 \leq k_n \leq (n!)^3$ of these triples of permutations in Sym_n such that the bound $\omega \leq \frac{n \log|H| - \log n! - \log k_n}{\log \sqrt[3]{\prod_{i=1}^{n} m_i p_i q_i}}$ is as tight as possible. It so happens that *Theorem 7.1*, [CUKS2005], is a special case of *Proposition 5.10* for $k_n = 1$, except there the group is not required to be Abelian.

Chapter 6

Applications

In this chapter, we apply the methods and general results in *Chapters 4-5* to describe the general conditions needed to prove results for ω using the parameters α and γ of concrete families of non-Abelian groups or of single non-Abelian groups. We conclude with a number of concrete upper estimates of ω in the region $2.82-2.93$. However, our most important result is a general estimate that $\omega \leq \frac{2^n \log n^{3n} - \log 2^n! - \log k_{2^n}}{2^n n \log(n-1)}$, for some undetermined $1 \leq k_{2^n} \leq (2^n!)^3$, where this k_{2^n} is the number of times the wreath product group $\left(Cyc_n^{\times 3}\right)^{\times n} \wr Sym_{2^n}$ (i.e. $\left(\left(Cyc_n^{\times 3}\right)^{\times n}\right)^{\times 2^n} \rtimes Sym_{2^n}$) realizes the product tensor $\left\langle 2^n! \left(n-1\right)^{n2^n}, 2^n! \left(n-1\right)^{n2^n}, 2^n! \left(n-1\right)^{n2^n} \right\rangle$ simultaneously, and the closer k_{2^n} is to $(2^n!)^3$ the closer ω is to 2.02 (from the upper side).

6.1 Analysis of α and γ for the Symmetric Groups

Here we derive upper estimates of α and γ for the symmetric groups $Sym\left(\Delta_n\right) \equiv Sym_{n(n+1)/2}$, and generally for Sym_m. We start with $\gamma\left(Sym\left(\Delta_n\right)\right)$.

6.1.1 *Estimates for* $\gamma\left(Sym\left(\Delta_n\right)\right)$

Our first estimate for $\left(Sym\left(\Delta_n\right)\right)$ follows from McKay's estimate of $d'\left(Sym_n\right)$ [MCK1976, p. 631].

(6.1) $2\sqrt{6}\left(\frac{n(n+1)}{2}\right)^{\frac{n(n+1)}{4}+1} e^{\sqrt{\frac{n(n+1)}{4}}\left(1-\frac{\pi}{3}\sqrt{12}\right)-\frac{n(n+1)+1}{4}} \leq d^{'}\left(Sym\left(\Delta_n\right)\right) \leq \left(\sqrt{2\pi}e^{-\frac{n(n+1)}{2}}\right)^{\frac{1}{2}}\left(\frac{n(n+1)}{2}\right)^{\frac{n(n+1)+1}{4}}$.

This yields the following result for $\gamma(Sym\left(\Delta_n\right))$.

Corollary 6.1 $\gamma(Sym\left(\Delta_n\right)) = 2 + O(\frac{1}{n})$.

Proof. Applying *(4.26)* and *(5.6)* to *(6.1)*, and using Stirling's formula, we have the initial estimate

$$\begin{aligned}
\gamma(Sym\left(\Delta_n\right)) &\geq \frac{n^2\log n - \frac{1}{2}n^2\left(1+\log 2\right) + O\left(n\log n\right)}{\log\left[\left(\sqrt{2\pi}e^{-\frac{n(n+1)}{2}}\right)^{\frac{1}{2}}\left(\frac{n(n+1)}{2}\right)^{\frac{n(n+1)+1}{4}}\right]} \\
\gamma(Sym\left(\Delta_n\right) &\leq \frac{n^2\log n - \frac{1}{2}n^2\left(1+\log 2\right) + O\left(n\log n\right)}{\log\left[2\sqrt{6}\left(\frac{n(n+1)}{2}\right)^{\frac{n(n+1)}{4}+1} e^{\sqrt{\frac{n(n+1)}{4}}\left(1-\frac{\pi}{3}\sqrt{6}\right)-\frac{n(n+1)+1}{4}}\right]}
\end{aligned}$$

Dividing numerator and denominator on both sides above by $n^2\log n - \frac{1}{2}n^2\left(1+\log 2\right)$, and then dividing $O(n\log n)$ by $n^2\log n$, we arrive at the result. ■

A second estimate of $\gamma\left(Sym\left(\Delta_n\right)\right)$ follows from Vershik and Kirov's estimate of $d^{'}\left(Sym\left(\Delta_n\right)\right)$ [VK1985, p. 21].

(6.2) $e^{-\frac{C_1}{2}\sqrt{\frac{n(n+1)}{2}}}\sqrt{\left(\frac{n(n+1)}{2}\right)!} \leq d^{'}\left(Sym\left(\Delta_n\right)\right) \leq e^{-\frac{C_2}{2}\sqrt{\frac{n(n+1)}{2}}}\sqrt{\left(\frac{n(n+1)}{2}\right)!}$,

where C_1, $C_2 > 0$ constants independent of n.

Corollary 6.2 $\gamma(Sym\left(\Delta_n\right)) = 2 + \Theta\left(\frac{1}{n\log n}\right)$.

Proof. Consequence of *(6.2)*.

$$\begin{aligned}
\gamma(Sym\left(\Delta_n\right)) &\geq \frac{n^2\log n - \frac{1}{2}n^2\left(1+\log 2\right) + O\left(n\log n\right)}{-\frac{C_2}{2}\sqrt{\frac{n(n+1)}{2}} + \frac{1}{2}n^2\log n - \frac{1}{4}n^2\left(1+\log 2\right) + \frac{1}{2}O\left(n\log n\right)} \\
\gamma(Sym\left(\Delta_n\right)) &\leq \frac{n^2\log n - \frac{1}{2}n^2\left(1+\log 2\right) + O\left(n\log n\right)}{-\frac{C_1}{2}\sqrt{\frac{n(n+1)}{2}} + \frac{1}{2}n^2\log n - \frac{1}{4}n^2\left(1+\log 2\right) + \frac{1}{2}O\left(n\log n\right)}
\end{aligned}$$

for positive constants C_1 and C_2. Dividing numerator and denominator on both sides by $n^2 \log n$, we obtain the result. ■

6.1.2 *An Upper Estimate for* $\alpha(Sym\,(\Delta_n)$

The main result here is that $\alpha(Sym\,(\Delta_n)) \leq 2 + O(\frac{1}{\log n})$.

Lemma 6.3 $\alpha(Sym\,(\Delta_n)) \leq 2 + O(\frac{1}{\log n})$.

Proof. $|Sym(\Delta_n)| = \left(\frac{1}{2}n(n+1)\right)!$, and $\left\langle \prod_{k=1}^{n} k!, \prod_{k=1}^{n} k!, \prod_{k=1}^{n} k! \right\rangle \epsilon\, \mathfrak{S}\,(Sym(\Delta_n))$ *(Lemma 5.6),* and implies that $\alpha(Sym\,(\Delta_n)) \leq \frac{\log\left(\frac{1}{2}n(n+1)\right)!}{\log(n!(n-1)!\cdots 2!1!)}$ by *(4.22).* By Stirling's asymptotic formula $\log n! \sim n\log n - n + O\,(\log n)$, as $n \longrightarrow \infty$, we have

$$\begin{aligned}
\log\left(\frac{1}{2}n(n+1)\right)! &= \frac{1}{2}n(n+1)\log\left(\frac{1}{2}n(n+1)\right) - \frac{1}{2}n(n+1) + O\left(\log\left(\frac{1}{2}n(n+1)\right)\right) \\
&= n^2\log n - \frac{1}{2}n^2\,(1+\log 2) + O\,(n\log n)\,.
\end{aligned}$$

For $\log\,(n!(n-1)!\cdots 2!1!)$ we have the estimate:

$$\begin{aligned}
&\log\,(n!(n-1)!\cdots 2!1!) = \log\left(2^{n-1}3^{n-2}....n\right) \\
= \;& (n-1)\log 2 + (n-2)\log 3 + ... + 2\log\,(n-1) + \log n \\
= \;& n\,(\log 2 + ... + \log n) - (\log 2 + 2\log 3 + ... + (n-1)\log n) \\
= \;& n\log\,(n!) - (\log 2 + 2\log 3 + ... + (n-1)\log n)\,.
\end{aligned}$$

Now, $n\log n! = n^2\log n - n^2 + O\,(n\log n)$, and $(\log 2 + 2\log 3 + ... + (n-1)\log n)$ is the result of the evaluation of the definite integral $\int_1^n (x-1)\log x\ dx + O\,(n\log n)$, which becomes $\frac{1}{2}\left[(x-1)^2\log x\right]_1^n - \frac{1}{2}\int_1^n \frac{(x-1)^2}{x}\ dx + O\,(n\log n)$ when we integrate by parts. We find that $\frac{1}{2}\left[(x-1)^2\log x\right]_1^n - \frac{1}{2}\int_1^n \frac{(x-1)^2}{x}\ dx + O\,(n\log n) = \frac{1}{2}n^2\log n - \frac{1}{4}n^2 + O\,(n\log n)$. Thus, $(\log 2 + 2\log 3 + ... + (n-1)\log n) = \frac{1}{2}n^2\log n - \frac{1}{4}n^2 + O\,(n\log n)$ which implies the estimate

for $\log(n!(n-1)!\cdots 2!1!)$ of

$$\begin{aligned}
& \log(n!(n-1)!\cdots 2!1!) \\
= \;& n\log(n!) - (\log 2 + 2\log 3 + ... + (n-1)\log n) \\
= \;& n^2\log n - n^2 + O(n\log n) - \frac{1}{2}n^2\log n + \frac{1}{4}n^2 - O(n\log n) \\
= \;& \frac{1}{2}n^2\log n - \frac{3}{4}n^2 + O(n\log n).
\end{aligned}$$

Then for $\frac{\log\left(\frac{1}{2}n(n+1)\right)!}{\log(n!(n-1)!\cdots 2!1!)}$ we have the estimate:

$$\begin{aligned}
& \frac{\log\left(\frac{1}{2}n(n+1)\right)!}{\log(n!(n-1)!\cdots 2!1!)} \\
= \;& \frac{n^2\log n - \frac{1}{2}n^2(1+\log 2) + O(n\log n)}{\frac{1}{2}n^2\log n - \frac{3}{4}n^2 + O(n\log n)} \\
= \;& \frac{2 - \frac{1+\log 2}{\log n} + O\left(\frac{1}{n}\right)}{1 - \frac{3}{2}\frac{1}{\log n} + O\left(\frac{1}{n}\right)} \\
= \;& \left(2 - (1+\log 2)\frac{1}{\log n}\right)\left(1 + \frac{3}{2}\frac{1}{\log n}\right) + O\left(\frac{1}{(\log n)^2}\right) \\
= \;& 2 + \frac{2-\log 2}{\log n} + O\left(\frac{1}{(\log n)^2}\right) \\
= \;& 2 + O\left(\frac{1}{\log n}\right).
\end{aligned}$$

■

If we denote by $z'(Sym(\Delta_n))$ the size of the maximal tensor realized by $Sym(\Delta_n)$, then we have following corollary.

Corollary 6.4 $n^{\frac{1}{3}n^2+O(n)}(2e)^{-\frac{1}{6}n^2} \leq z'(Sym(\Delta_n))^{\frac{1}{3}} < n^{\frac{1}{2}n^2+O(n)}(2e)^{-\frac{1}{4}n^2}$.

Proof. $|Sym(\Delta_n)| = \left(\frac{1}{2}n(n+1)\right)!$, and by *(4.23)* $\left(\frac{1}{2}n(n+1)\right)! \leq z'(Sym(\Delta_n)) < \left(\left(\frac{1}{2}n(n+1)\right)!\right)^{\frac{3}{2}}$. Taking logarithms on all sides, and substituting the estimate $\log\left(\frac{1}{2}n(n+1)\right)! = n^2\log n - \frac{1}{2}n^2(1+\log 2) + O(n\log n)$ from *Lemma 6.3*, and taking antilogarithms, we obtain the result. $z'(Sym(\Delta_n))^{\frac{1}{3}}$ is the maximal mean size of matrix multiplication supported by $Sym(\Delta_n)$, and the result describes bounds for these in terms of the order of $Sym(\Delta_n)$, which grows exponentially with n. ■

Lemma 6.3 shows that it suffices to work with the symmetric groups $Sym(\Delta_n)$ since for every integer $m \geq 2$, there exists an integer $n \geq 1$ such that $\left(\frac{1}{2}n(n+1)\right)! \mid m!$.

6.1.3 *An Upper Estimate for* $\alpha(Sym_n)$

Following *Lemma 6.3* we show that a similar estimate applies to the $\alpha(Sym_n)$ of arbitrary symmetric groups Sym_n.

Corollary 6.5 $\alpha(Sym_n) \leq 2 + O\left(\frac{1}{\log m}\right) + O\left(\frac{1}{(\log m)^2}\right) + O\left(\frac{1}{m(m+1)}\right)$, *for some* $m < n$.

Proof. It suffices to prove that $\alpha(Sym_n) \leq \alpha\left(Sym\left(\Delta_m\right)\right) + O\left(\frac{1}{m(m+1)}\right)$, for some integer $m < n$. By Lagrange's theorem the order $|H|$ of a proper subgroup $H < G$ is a proper divisor of the order $|G|$ of G. For every integer $n \geq 2$, there exists an integer $m \geq 1$ such that $\left(\frac{1}{2}m(m+1)\right)! \mid n!$. This is most obviously the case when $n = \sum_{i=1}^{m} k = Z_m = \left(\frac{1}{2}m(m+1)\right)$, i.e. when n is the sum of the first m positive integers for some m, in which case $Sym_n = Sym\left(\Delta_m\right)$, and $\alpha(Sym_n) = \alpha\left(Sym\left(\Delta_m\right)\right)$. If $Z_m < n < Z_{m+1}$ for some m, then $\frac{1}{2}m(m+1) \leq n-1 \leq \frac{1}{2}\left(m+1\right)\left(m+2\right)$, and this m is the least integer such that $\left(\frac{1}{2}m(m+1)\right)!$ is the largest proper divisor of $n!$. Consequently, for this m, $Sym\left(\Delta_m\right)$ occurs as the maximal subgroup of Sym_n of order $\left|Sym\left(\Delta_m\right)\right| = \left(\frac{1}{2}m(m+1)\right)! \leq (n-1)!$. We can deduce from these facts, by using *Lemma 4.19* that:

$$\begin{aligned}
\alpha(Sym_n) &\leq \alpha(Sym\left(\Delta_m\right)) + \log_{z'(Sym(\Delta_m))^{1/3}}\left[Sym_n : Sym\left(\Delta_m\right)\right] \\
&\leq \alpha(Sym\left(\Delta_m\right)) + \frac{\log \frac{1}{2}m(m+1)+1}{\log\left(z'(Sym\left(\Delta_m\right))\right)^{\frac{1}{3}}} \\
&\leq \alpha(Sym\left(\Delta_m\right)) + \frac{\log \frac{1}{2}m(m+1)+1}{3^{-1}\log\left(\frac{1}{2}m(m+1)\right)!} \qquad \text{(using } \textit{(4.23)}\text{)} \\
&\sim \alpha(Sym\left(\Delta_m\right)) + \frac{3}{2^{-1}m(m+1)}\frac{\log \frac{1}{2}m(m+1)+1}{\log \frac{1}{2}m(m+1)-1} \\
&\sim \alpha(Sym\left(\Delta_m\right)) + \frac{3}{2^{-1}m(m+1)} \\
&= \alpha(Sym\left(\Delta_m\right)) + O\left(\frac{1}{m\left(m+1\right)}\right) \\
&\leq 2 + \frac{2-\log 2}{\log m} + O\left(\frac{1}{(\log m)^2}\right) + O\left(\frac{1}{m\left(m+1\right)}\right).
\end{aligned}$$

■

Lemma 6.5 shows that it suffices to work with the symmetric groups $Sym(\Delta_n)$.

6.1.4 *Applications to* ω

Here we examine the implications of the above analysis for ω using the groups $Sym(\Delta_n)$.

By *Lemma 6.3* $\alpha(Sym(\Delta_n)) = 2 + \frac{2-\log 2}{\log n} + O\left(\frac{1}{(\log n)^2}\right) = 2 + O(\frac{1}{\log n})$. For as small as $n \geq 4$, the leading term $2 + \frac{2-\log 2}{\log n} < 3$. The following is a table of values of $2 + \frac{2-\log 2}{\log n}$ for $2 \leq n \leq 10$.

n	$\lvert Sym(\Delta_n)\rvert$	$\frac{\log\left(\frac{1}{2}n(n+1)\right)!}{\log(n!(n-1)!\cdots 2!1!)}$
2	6	3.88539
3	720	3.18955
4	3,628,800	2.94270
5	1.30767×10^{12}	2.81199
6	5.10909×10^{19}	2.72937
7	3.04888×10^{29}	2.67159
8	3.71993×10^{41}	2.62846
9	1.19622×10^{56}	2.59477
10	1.26964×10^{73}	2.56756

$\lvert Sym(\Delta_n)\rvert \longrightarrow \infty$ of the order of n^{n^2}, much faster than $2 + \frac{2-\log 2}{\log n} \longrightarrow 2$. *Lemma 6.3* (or *Lemma 6.5*) shows that $\alpha(Sym(\Delta_n)) - 2 = O(\gamma(Sym(\Delta_n)))$, which is contrary to the limit condition of *Corollary 4.28* needed to prove $\omega = 2$, i.e. we cannot prove $\omega = 2$ using the limit results *Corollary 4.30* or *Theorem 4.31* for the family of groups $Sym(\Delta_n)$.

However, the application of *Corollary 4.29*, and the estimate $\lvert Sym(\Delta_n)\rvert = \left(\frac{n(n+1)}{2}\right)! = n^{\frac{3}{2}n^2+Kn}(2e)^{-\frac{1}{2}n^2}$, where K is some constant independent of n, this yields the following open question.

Problem 6.6 *Is there a symmetric group $Sym(\Delta_n)$, for some $n > 1$, such that $z^{'}(Sym(\Delta_n))^{\frac{1}{3}} > d^{'}(Sym(\Delta_n))$ and $\frac{z^{'}(Sym(\Delta_n))^{\frac{t}{3}}}{d^{'}(Sym(\Delta_n))^{t-2}} \geq n^{\frac{3}{2}n^2+Kn}(2e)^{-\frac{1}{2}n^2}$, for some $2 < t < 3$, where K is a constant independent of n?*

6.2 Some Estimates for the Exponent ω

Here we derive a number of estimates for ω, using wreath products of Abelian groups with symmetric groups. We start with the Abelian group $Cyc_n^{\times 3} \equiv Cyc_n \times Cyc_n \times Cyc_n$, for which we start with a basic lemma.

Lemma 6.7 *For the Abelian group $Cyc_n^{\times 3}$ the subset triples (S_1, T_1, U_1) and (S_2, T_2, U_2) defined by*

$$S_1 \ : \ = Cyc_n \backslash \{1\} \times \{1\} \times \{1\}, \ T_1 := \{1\} \times Cyc_n \backslash \{1\} \times \{1\}, \ U_1 := \{1\} \times \{1\} \times Cyc_n \backslash \{1\},$$
$$S_2 \ : \ = \{1\} \times Cyc_n \backslash \{1\} \times \{1\}, \ T_2 := \{1\} \times \{1\} \times Cyc_n \backslash \{1\}, \ U_2 := Cyc_n \backslash \{1\} \times \{1\} \times \{1\},$$

(1) *have the triple product property, and* (2) *have the simultaneous triple product property.*

Proof. (1) For arbitrary elements $\left(s^{'}, 1, 1\right), (s, 1, 1) \, \epsilon \, S_1 = Cyc_n \backslash \{1\} \times \{1\} \times \{1\}$, $\left(1, t^{'}, 1\right), (1, t, 1) \, \epsilon \, T_1 = \{1\} \times Cyc_n \backslash \{1\} \times \{1\}$, $\left(1, 1, u^{'}\right), (1, 1, u) \, \epsilon \, U = \{1\} \times \{1\} \times Cyc_n \backslash \{1\}$, the condition $\left(s^{'}, 1, 1\right)(s, 1, 1)^{-1}\left(1, t^{'}, 1\right)(1, t, 1)^{-1}\left(1, 1, u^{'}\right)(1, 1, u)^{-1} = \left(s^{'}s^{-1}, t^{'}t^{-1}, u^{'}u^{-1}\right) = (1, 1, 1)$ can only occur if $s^{'} = s$, $t^{'} = t$, $u^{'} = u$, which implies that $\left(s^{'}, 1, 1\right) = (s, 1, 1)$, $\left(1, t^{'}, 1\right) = (1, t, 1)$, $\left(1, 1, u^{'}\right) = (1, 1, u)$. Thus, (S_1, T_1, U_1) has the triple product property, and we can prove the same for (S_2, T_2, U_2).
(2) Refer to *Proposition 5.2*, [CUKS2005]. ■

The following is an elementary corollary.

Corollary 6.8 *The Abelian group $Cyc_n^{\times 3}$ realizes the tensor $\langle n-1, n-1, n-1\rangle$ 2 times simultaneously.*

Proof. Consequence of definition *(5.2)* with respect to the triples in *Lemma 6.11.* ■

6.2.1 $\omega < 2.82$ *via* $Cyc_{16}^{\times 3}$

By *Corollary 6.12* $Cyc_n^{\times 3}$ realizes the identical tensors $\langle n-1, n-1, n-1\rangle$ and $\langle n-1, n-1, n-1\rangle$ simultaneously, and, thereby, supports two independent, simultaneous multiplications of square matrices of order $n-1$, and by *Corollary 5.3*, we have the inequality

$$\omega \leq \frac{\log n^3 - \log 2}{\log (n-1)}.$$

The expression $\frac{\log n^3 - \log 2}{\log(n-1)}$ achieves a minimum 2.81553... for $n = 16$, i.e. $\omega < 2.81554$.

6.2.2 $\omega < 2.93$ *via* $Cyc_{41}^{\times 3} \wr Sym_2$

From above, $Cyc_n^{\times 3}$ realizes the tensor $\langle n-1, n-1, n-1\rangle$ 2 times simultaneously. By part (1) of *Corollary 5.9* $Cyc_n^{\times 3} \wr Sym_2$ realizes the tensor $\left\langle 2(n-1)^2, 2(n-1)^2, 2(n-1)^2 \right\rangle$ once, and by part (2)

$$\omega \leq \frac{6\log n - \log 2}{2\log (n-1)}.$$

The minimum value $\omega \leq 2.92613048...$ is attained for $n = 41$.

More generally, by *Proposition 5.10* $Cyc_n^{\times 3} \wr Sym_2$ realizes the product tensor $\left\langle 2(n-1)^2, 2(n-1)^2, 2(n-1$ some $1 \leq k_2 < (2!)^3$ times simultaneously such that

$$\begin{aligned} \omega &\leq \frac{6\log n - \log 2 - \log k_2}{2\log (n-1)} \\ &\leq \frac{6\log n - \log 2}{2\log (n-1)} \\ &< 2.93. \end{aligned}$$

If, for example, $k_2 = (2!)^3$ we would have $\frac{6\log n - \log 2 - \log k_2}{2\log(n-1)} = \frac{6\log n - \log 16}{2\log(n-1)}$, which achieves a minimum of 2.478495... at $n = 6$. The following table gives minima for the expression $\frac{6\log n - \log 2 - \log k_2}{2\log(n-1)}$ for the values of $1 \leq k_2 \leq (2!)^3$:

k_2	$\omega \leq \min\left(\frac{6\log n - \log 2 - \log k_2}{2\log(n-1)}\right)$
1	2.9261
2	2.8163
3	2.7351
4	2.6700
5	2.6142
6	2.5647
7	2.5200
8	2.4785

Here we know only the case $k_2 = 1$ based ultimately on *Theorem 5.8*, and we conclude that $\omega \leq 2.9261$, and for the values $2 \leq k_2 \leq 8$ the table's bounds for ω are *conditional* on those values of k_2.

6.2.3 $\omega < 2.82$ *via* $\left(Cyc_{25}^{\times 3}\right)^{\times 25} \wr Sym_{2^{25}}$

As before, we start we start with $Cyc_n^{\times 3}$, which realizes the tensor $\langle n-1, n-1, n-1\rangle$ 2 times simultaneously. By *Corollary 5.5* the m-fold direct product $\left(Cyc_n^{\times 3}\right)^{\times m}$ realizes the pointwise product tensor $\langle (n-1)^m, (n-1)^m, (n-1)^m\rangle$ 2^m times simultaneously. By part (1) of *Corollary 5.9* the group $\left(Cyc_n^{\times 3}\right)^{\times m} \wr Sym_{2^m}$ (i.e. $\left(\left(Cyc_n^{\times 3}\right)^{\times m}\right)^{\times 2^m} \rtimes Sym_{2^m}$) realizes the product tensor $\left\langle 2^m!\,(n-1)^{2^m m}, 2^m!\,(n-1)^{2^m m}, 2^m!\,(n-1)^{2^m m}\right\rangle$ once, and by part (2)

$$\begin{aligned}\omega &\leq \frac{2^m \log n^{3m} - \log 2^m!}{2^m m \log(n-1)} \\ &\sim \frac{3m\log n - m\log 2 + 1}{m\log(n-1)}.\end{aligned}$$

If we let $m \longrightarrow \infty$ the right hand side tends to 2.815... we derive that $\omega < 2.82$, as good a result as in section *6.2.1*.

If we consider the n-fold direct product $\left(Cyc_n^{\times 3}\right)^{\times n}$, then more generally, by *Proposition 5.10* $\left(Cyc_n^{\times 3}\right)^{\times n} \wr Sym_{2^n}$ (i.e. $\left(\left(Cyc_n^{\times 3}\right)^{\times n}\right)^{\times 2^n} \rtimes Sym_{2^n}$) realizes the product tensor

$\left\langle 2^n!\,(n-1)^{n2^n}, 2^n!\,(n-1)^{n2^n}, 2^n!\,(n-1)^{n2^n} \right\rangle$ some $1 \leq k_{2^n} \leq (2^n!)^3$ times simultaneously such that

$$\omega \leq \frac{2^n \log n^{3n} - \log 2^n! - \log k_{2^n}}{2^n n \log (n-1)}.$$

If here $k_{2^n} = (2^n!)^3$ then $\omega \leq \frac{2^n \log n^{3n} - 4 \log 2^n!}{2^n n \log (n-1)}$, the latter achieving a minimum of 2.012 for $n = 6$. In general, for the groups $\left(Cyc_n^{\times 3}\right)^{\times n} \wr Sym_{2^n}$ the closer k_{2^n} is to $(2^n!)^3$, the closer we could push ω down towards 2.012 (from the upper side).

These results point to the utility of finding triples of permutations $\sigma_j, \tau_j, \upsilon_j \in Sym_n$ in order that a maximum number $1 \leq k_n \leq (n!)^3$ of permuted product triples $\prod_{i=1}^{n} S_{\sigma_j(i)} \wr Sym_n$, $\prod_{i=1}^{n} T_{\tau_j(i)} \wr Sym_n$, $\prod_{i=1}^{n} U_{\upsilon_j(i)} \wr Sym_n$, $1 \leq j \leq k_n$, satisfy the STPP in $H \wr Sym_n$, where H is Abelian with a given STPP family $\{(S_i, T_i, U_i)\}_{i=1}^{n}$. Using such groups and their triples in this way, the sharpest upper bounds for ω will occur where the ratio $k_n / (n!)^3$ is highest. Therefore, we pose the following problem.

Problem 6.9 *For any given n, and group $H \wr Sym_n$, with H being Abelian, and a given family $\{(S_i, T_i, U_i)\}_{i=1}^{n}$ of n STPP triples of H, what is the largest number $1 \leq k_n \leq (n!)^3$ such that there are k_n triples of permutations $\sigma_j, \tau_j, \upsilon_j \in Sym_n$ such that the k_n triples $\prod_{i=1}^{n} S_{\sigma_j(i)} \wr Sym_n$, $\prod_{i=1}^{n} T_{\tau_j(i)} \wr Sym_n$, $\prod_{i=1}^{n} U_{\upsilon_j(i)} \wr Sym_n$, $1 \leq j \leq k_n$, satisfy the STPP in $H \wr Sym_n$?*

Bibliography

1. [BOA1982], Boas, P. van Emde, *Berekeningscomplexiteit van Bilineaire en Kwadratische Vormen (Computational Complexity of Bilinear and Quadratic Forms)*, in Vitanyi, P. M. V., van Leeuwen, J., & van Emde Boas, P. (eds.), Colloquium Complexiteit en Algorithmen MC Syllabi 48.2, Amsterdam, 1982, pp.3–68.

2. [BCS1997], Bürgisser, P., Clausen, M., & Shokrollahi, A., *Algebraic Complexity Theory*, Springer, Berlin, 1997.

3. [COH2007], Cohn, H., 'Group-theoretic Algorithms for Matrix Multiplication', (private email, 30/03/2007).

4. [CUKS2005], Cohn, H., Umans, C., Kleinberg, R., Szegedy, B., 'Group-theoretic Algorithms for Matrix Multiplication', *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science 2005*, IEEE Computer Society, 2005, pp. 438–449, arXiv:math.GR/0511460.

5. [CU2003], Cohn, H. & Umans, C., 'A Group-theoretic Approach to Fast Matrix Multiplication', *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science 2003*, IEEE Computer Society, 2003, pp. 379–388, arXiv:math.GR/0307321.

6. [CW1990], Coppersmith, D., & Winograd, S., 'Matrix Multiplication via Arithmetic Progressions', *Journal of Symbolic Computation*, 9, 1990, pp. 251-280.

7. [DDHK2006], Demmel, J., Dumitriu, I., Holtz, O., & Kleinberg, R., 'Fast Matrix Multiplication is Stable', 2006, arXiv:math.NA/0603207.

8. [HUP1998], Huppert, B., *Character Theory of Finite Groups*, Walter de Gruyter, Berlin, 1998.

9. [LAN2006], Landsberg, J. M., 'Geometry and Complexity of Matrix Multiplication', 2006.

10. [MIL2003], Milne, J. S., 'Group Theory', 2003, http://www.jmilne.org/math/.

11. [MR2003], Maslen, D. K., & Rockmore, D. N., 'The Cooley-Tukey FFT and Group Theory', *Modern Signal Processing*, 46:2003, pp. 281-301.

12. [MCK1976], McKay, J., 'The Largest Degrees of Irreducible Characters of the Symmetric Group', *Mathematics of Computation*, 223:6, 1976, pp. 624-631.

13. [PAN1984], Pan, V, 'How can we Speed up Matrix Multiplication', *SIAM Review*, 26:3, 1984, pp. 393-415.

14. [SER1977], Serre, J. P., *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

15. [STR1969], Strassen, V., 'Gaussian Elimination is not Optimal', *Numerische Mathematik*, 13, 1969, pp. 354–356.

16. [UMA2007], Umans, C., 'Group-theoretic Algorithms for Matrix Multiplication', (private email, 22/03/2007).

17. [VK1985], Vershik, A. M., Kerov, S. V., 'Asymptotics of the Largest and the Typical Dimensions of Irreducible Representations of a Symmetric Group', *Funktsional'nyi Analiz i Ego Prilozheniya* (trans. *Functional Analysis and Applications*), 19:1, 1985, pp. 25-36.

18. [WIN1971], Winograd, S., 'On Multiplication of 2×2 Matrices, *Linear Algebra and Applications*, 4:?, 1971, pp. 381-388.