<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Counting commutativities in finite algebraic systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Dolan, Brian; MacHale, Desmond; MacHale, Peter</td>
</tr>
<tr>
<td><strong>Publication date</strong></td>
<td>2016</td>
</tr>
<tr>
<td><strong>Type of publication</strong></td>
<td>Article (peer-reviewed)</td>
</tr>
<tr>
<td></td>
<td>Access to the full text of the published version may require a subscription.</td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 2016 Irish Mathematical Society</td>
</tr>
<tr>
<td><strong>Item downloaded from</strong></td>
<td><a href="http://hdl.handle.net/10468/9600">http://hdl.handle.net/10468/9600</a></td>
</tr>
</tbody>
</table>

Downloaded on 2020-02-28T05:05:06Z
Counting Commutativities in Finite Algebraic Systems

BRIAN DOLAN, DES MACHALE AND PETER MACHALE

Abstract. We examine the total possible number of commutativi- ties in a finite algebraic system, concentrating on groups, but also examining rings and semigroups. Numerical restrictions are found and bounds for the total number of commutativities in subgroups and factor groups are derived. Finally, a curious connection with group representations is explored.

1. Introduction

Consider the Cayley table of a finite group $G$. For $a, b, \in G$, if $ab = ba$, we place a 1 in each of the boxes corresponding to $ab$ and $ba$. This is called a commutativity in $G$. Otherwise we put a 0 in each of these boxes, indicating a non-commutativity in $G$. If $G$ is an abelian group, there will be a 1 in each box, so we disregard this uninteresting case.

We call this matrix of 1's and 0's the commutativity chart for $G$. Here for example is the commutativity chart for $S_3$, the group of all permutations on the set \{1, 2, 3\} under composition. $S_3$ is in fact the smallest non-abelian group.

\[
\begin{array}{|c|c|c|c|c|c|}
\hline
  & e & (123) & (132) & (12) & (13) & (23) \\
\hline
 e & 1 & 1 & 1 & 1 & 1 & 1 \\
(123) & 1 & 1 & 1 & 0 & 0 & 0 \\
(132) & 1 & 1 & 1 & 0 & 0 & 0 \\
(12) & 1 & 0 & 0 & 1 & 0 & 0 \\
(13) & 1 & 0 & 0 & 0 & 1 & 0 \\
(23) & 1 & 0 & 0 & 0 & 0 & 1 \\
\hline
\end{array}
\]

We denote by $I(G)$ the number of times that 1 appears in the commutativity chart and by $O(G)$ the number of times that 0 appears. Thus $I(S_3) = 18$ and $O(S_3) = 18$ also.

In general we see that $I(G) + O(G) = |G|^2$ and $O(G) > 0$ since we are assuming $G$ is non-abelian. Also we have $I(G) > 0$ since for
example \(xx = xx\) for all \(x \in G\). One of our objectives of this note will be to discuss the possible values of \(I(G)\) and \(O(G)\), where \(G\) is a finite non-abelian group and to investigate the values of \(I(S)\) and \(O(S)\) for other non-commutative algebraic systems \(S\).

Since if \(ab \neq ba\) then \(ba \neq ab\) and \(xx = xx\) for all \(x\), we see that \(O(G)\) is always an even number, but there are examples to show that \(I(G)\) can be either even or odd. For example, \(I(A_4) = 48\), where \(A_4\) is the alternating group of order 12, while \(I(G(21)) = 105\), where \(G(21)\) is the non-abelian group of order 21. We emphasise that throughout, \(G\) denotes a finite non-abelian group.

2. Some Elementary Results

Let us recall some facts from elementary group theory. Two elements \(x\) and \(y\) in \(G\) are said to be conjugate if there exists \(w \in G\) with \(y = w^{-1}xw\). The relation of conjugacy is easily seen to be an equivalence relation on \(G\), under which \(G\) is partitioned into disjoint conjugacy classes. For example, in the group \(S_3\), the conjugacy classes are \(\{e\}, \{(123), (132)\}\) and \(\{(12), (13), (23)\}\).

In general, let \(G\) have exactly \(k(G)\) conjugacy classes and let \(C_{G}(x)\), the centralizer of \(x\) in \(G\), be the subgroup of \(G\) given by \(C_{G}(x) = \{a \in G \mid ax = xa\}\). There is a nice connection between conjugacy classes and centralizers viz. \(|C_{G}(x)| = (G : C_{G}(x))\), i.e. the number of cosets of \(C_{G}(x)\) in \(G\), and both these numbers are divisors of \(|G|\).

From the definition, we have that

\[
I(G) = \sum_{x \in G} |C_{G}(x)| = \sum_{x \in G} \frac{|G|}{|C_{G}(x)|} = |G| \sum_{x \in G} \frac{1}{|C_{G}(x)|} = |G|k(G). \text{ See [5].}
\]

It follows that \(O(G) = |G|^2 - I(G) = |G|(|G| - k(G))\). Thus in the case of \(S_3\), since \(k(S_3) = 3\), we have \(I(G) = 6 \cdot 3 = 18\) and \(O(G) = 6 \cdot (6 - 3) = 18\), in agreement with our previous calculations.

**Theorem 2.1.** If \(|G|\) is odd, then \(k(G)\) is odd.

**Proof.** If \(|G|\) is odd, since \(O(G)\) is even and \(O(G) = |G|(|G| - k(G))\), we see that \(|G| - k(G)\) must be even, so \(k(G)\) is odd. \(\square\)

We note that the converse of this result is not true; \(k(S_3) = 3\), but \(|S_3| = 6\).
**Theorem 2.2.** \( I(G) \) is odd if and only if \(|G|\) is odd.

**Proof.** If \(|G|\) is odd then by Theorem 2.1 \( k(G) \) is odd, so \( I(G) = |G|k(G) \) is odd. Conversely, if \( I(G) \) is odd then \(|G|\) clearly must be odd. \( \square \)

In fact the smallest possible odd value of \( I(G) = 105 = 21 \cdot 5 \), arising from \( G(21) \), which is the smallest odd-order non-abelian group. We remark that Theorem 2.1, which says that if \(|G|\) is odd, then \(|G| - k(G) \equiv 0 \pmod{2} \), can be improved upon considerably using the theory of matrix group representations. A lovely theorem of Burnside \([3]\) states that if \(|G|\) is odd, then \(|G| - k(G) \equiv 0 \pmod{16} \).

Again, \( G(21) \) shows that this result is the best possible. Since \( O(G) = |G|(|G| - k(G)) \) we have

**Theorem 2.3.** If \(|G|\) is odd, then \( O(G) \) is a multiple of \( 16|G| \).

Again, \( O(G(21)) = 336 = 16 \cdot 21 \), shows that this result is the best possible.

We now investigate the possible values of \( I(G) \) and \( O(G) \) as \( G \) ranges over all finite non-abelian groups. For a given group \( G \) it is easy, if tedious, to calculate the value of \( k(G) \), and for certain classes of groups, and for groups of small order, this information is readily available from a variety of sources.

In particular let \( D_n \) be the dihedral group of order \( 2n \) \((n > 2)\) given by

\[
< a, b \mid a^n = 1 = b^2; b^{-1}ab = a^{-1} >
\]

Then if \( n = 2m \) is even, we have \( k(D_{2m}) = m + 3 \), making \( I(D_{2m}) = 4m(m + 3) = 4m^2 + 12m \).

If \( n = 2m + 1 \) is odd, then \( k(D_{2m+1}) = m + 2 \), so \( I(D_{2m+1}) = (4m + 2)(m + 2) = 4m^2 + 10m + 4 \).

The values of \( O(D_n) \) can be found from \( O(G) = |G|^2 - I(G) \).

The symmetric group \( S_n \) of order \( n! \) has exactly \( p(n) \) conjugacy classes, where \( p(n) \) is the (integer) partition function, so \( I(S_n) = n!p(n) \) and \( O(S_n) = n!(n! - p(n)) \).

For distinct odd primes \( p \) and \( q \), with \( p < q \) where \( p|(q - 1) \), there is a unique non-abelian group \( G(pq) \) of order \( pq \). Easy calculations show that \( G(pq) \) has exactly \( p + \frac{q-1}{p} \) conjugacy classes, so that \( I(G(pq)) = q(p^2 + q - 1) \) and \( O(G(pq)) = p^2q^2 - I(G) = q(q-1)(p^2 - 1) \).

We now present a chart with three columns. In the first column are the possible orders of a finite non-abelian group \( G \). In the second
and third columns we give the values of $I(G)$ and $O(G)$ for each non-abelian group of order $|G|$. Since it is known that there are only finitely many groups with a given order and also only finitely many groups with a given number of conjugacy classes ([6], [9]), we see that there are just finitely many (maybe zero) groups with a given $I(G)$ or a given $O(G)$. Note that there may be several different groups of order $|G|$ with the same $k(G)$ and hence the same $I(G)$ and $O(G)$.

| $|G|$ | $I(G)$ | $O(G)$ | $|G|$ | $I(G)$ | $O(G)$ | $|G|$ | $I(G)$ | $O(G)$ |
|-----|-------|-------|-----|-------|-------|-----|-------|-------|
| 6   | 18    | 18    | 32  | 544   | 480   | 48  | 1152  | 1152  |
| 8   | 40    | 24    | 34  | 340   | 816   | 48  | 1440  | 864   |
| 10  | 40    | 60    | 36  | 216   | 1080  | 50  | 700   | 1800  |
| 12  | 48    | 96    | 36  | 324   | 972   | 50  | 1000  | 1500  |
| 12  | 72    | 72    | 36  | 360   | 936   | 52  | 364   | 2340  |
| 14  | 70    | 126   | 36  | 432   | 864   | 52  | 832   | 1872  |
| 16  | 112   | 144   | 38  | 418   | 1026  | 54  | 540   | 2376  |
| 16  | 160   | 96    | 39  | 273   | 1248  | 54  | 972   | 1944  |
| 18  | 108   | 216   | 40  | 400   | 1200  | 54  | 1188  | 1728  |
| 18  | 162   | 162   | 40  | 520   | 1080  | 54  | 1458  | 1458  |
| 20  | 100   | 300   | 40  | 640   | 960   | 55  | 385   | 2640  |
| 20  | 160   | 240   | 40  | 1000  | 600   | 56  | 448   | 2688  |
| 21  | 105   | 336   | 42  | 294   | 1470  | 56  | 952   | 2184  |
| 22  | 154   | 330   | 42  | 420   | 1344  | 56  | 1120  | 2016  |
| 24  | 120   | 456   | 42  | 504   | 1260  | 56  | 1960  | 1176  |
| 24  | 168   | 408   | 42  | 630   | 1134  | 57  | 513   | 2736  |
| 24  | 192   | 384   | 42  | 882   | 882   | 58  | 928   | 2436  |
| 24  | 216   | 360   | 44  | 616   | 1320  | 60  | 300   | 3300  |
| 24  | 288   | 288   | 46  | 598   | 1518  | 60  | 540   | 3060  |
| 24  | 360   | 216   | 48  | 384   | 1920  | 60  | 720   | 2800  |
| 26  | 208   | 468   | 48  | 480   | 1824  | 60  | 900   | 2700  |
| 27  | 297   | 432   | 48  | 576   | 1728  | 60  | 1080  | 2520  |
| 28  | 280   | 504   | 48  | 672   | 1632  | 60  | 1200  | 2400  |
| 30  | 270   | 630   | 48  | 720   | 1584  | 60  | 1440  | 2160  |
| 30  | 360   | 540   | 48  | 768   | 1536  | 60  | 1800  | 1800  |
| 32  | 352   | 672   | 48  | 864   | 1440  | 60  | 1008  | 1296  |
| 32  | 448   | 576   | 48  | 1008  | 1296  | 60  | 1008  | 1296  |

We note that for direct products of groups $G_1$ and $G_2$, $I(G_1 \times G_2) = I(G_1)I(G_2)$ and $k(G_1 \times G_2) = k(G_1)k(G_2)$. However, $O(S_3)O(S_3) = 18 \cdot 18 = 324 \neq 972 = O(S_3 \times S_3)$.

By [7] we have $\frac{k(G)}{|G|} \leq \frac{5}{8}$ so $I(G) \leq \frac{5}{8}|G|^2$, and $O(G) \geq \frac{3}{8}|G|^2$.

Also, by examining Cayley tables, it is clear that $I(G) \geq 3|G| - 2$, so that $O(G) \leq |G|^2 - 3|G| + 2$. 
Thus, consulting the above charts, we see that the allowable values for $I(G)$ are: 18, 40, 48, 70, 72, 100, 105, 108, 112, 120, 154, 160, 162, 168, 192, 208, 216, 270, 273, 280, 288, 294, 297, 300, 324, 340, 352, 360, 364, 384, 385, 400, 418, 432, ... 

Similarly the allowable values for $O(G)$ are: 18, 24, 60, 72, 96, 126, 144, 162, 216, 240, 288, 300, 330, 336, 360, 384, 408, 432, 450, 456, 468, 480, 504, 540, 576, 600, 630, 648, 672, ... 

We mention that the function $|G| - k(G)$ is examined in considerable detail in [1]. Also, one can show that $I(G) = O(G)$ if and only if $G/Z(G) = S_3$, where $Z(G)$ is the centre of $G$.

3. Subgroups and Factor Groups

Gallagher [4] gives elementary proofs of the following results for all finite groups $G$, where $H$ is a subgroup of $G$ and $N$ is a normal subgroup of $G$.

(i) $k(H) < (G : H)k(G)$, for $H \neq G$;  
(ii) $k(G) \leq (G : H)k(H)$;  
(iii) $k(G) \leq k(G/N)k(N)$.

In our notation, these results immediately become

Theorem 3.1.  
(i) $I(H) < I(G)$ if $H \neq G$;  
(ii) $I(G) \leq (G : H)^2I(H)$;  
(iii) $I(G/N) \geq I(G)/I(N)$.

4. Other Algebraic Systems

Let $S = \{a, b\}$ be a set of cardinality 2. Define a binary operation $*$ on $S$ as follows

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

Easy calculations show that $S$ is a non-commutative semigroup with $I(S) = 2 = O(S)$, so the sequences of allowable value of $I(S)$ and $O(S)$ for semigroups are different from those of $I(G)$ and $O(G)$ for groups.

The reader is invited to determine the sequences of allowable values of $I(S)$ and $O(S)$ for non-commutative semigroups.

Moving on to rings, consider the following set of $2 \times 2$ matrices over $\mathbb{Z}_2$ under matrix addition and multiplication mod 2:  

$R = \{ (0 \ 0, \ (0 \ 1), \ (1 \ 0), \ (1 \ 1) \}$
It is easy to see that \( \{ R, +, \cdot \} \) is a non-commutative ring of order 4. The commutativity chart for \( \{ R, \cdot \} \) looks as follows:

\[
\begin{array}{c|cccc}
     & (0,0) & (0,1) & (1,0) & (1,1) \\
\hline
(0,0) & 1 & 1 & 1 & 1 \\
(0,1) & 1 & 1 & 0 & 0 \\
(1,0) & 1 & 0 & 1 & 0 \\
(1,1) & 1 & 0 & 0 & 1 \\
\end{array}
\]

Thus \( I(R) = 10 \) and \( O(R) = 6 \). This single example shows that the sequences of allowable values of \( I(R) \) and \( O(R) \) for finite rings are different from those for finite groups.

Again the reader is invited to investigate this problem for other algebraic systems such as near–rings, loops, quasigroups etc.

We remark that if \( S \) is a set with \(|S| = n\) we can always choose closed binary operations \( \ast \) and \( \circ \) on \( S \) such that \( I(S, \ast) = n \) \((n > 1)\), and \( O(S, \circ) = 2n \) \((n \text{ arbitrary})\).

For example, if \( S = \{a, b, c\} \) define \( \ast \) by

\[
\begin{array}{c|ccc}
     * & a & b & c \\
\hline
     a & a & a & c \\
     b & b & b & b \\
     c & a & c & c \\
\end{array}
\]

to achieve \( I(S, \ast) = 3 \) and similarly for the general case.

\[
\begin{array}{c|ccc}
     \circ & a & b & c \\
\hline
     a & a & a & a \\
     b & b & a & a \\
     c & b & b & c \\
\end{array}
\]

Also in the second example \( O(S, \circ) = 6 \) and similarly for the general case.

5. A Connection with Matrix Representations of Groups

There is a surprising connection between \( I(G) \) and matrix representations of \( G \). For definitions we refer the interested reader to [5].

Let \( d_i, 1 \leq i \leq k \), be the degrees of the irreducible complex matrix representations of a finite group \( G \) i.e. the sizes of the square matrices involved. There are \( k(G) \) of these where \( G \) has \( k(G) \) conjugacy classes.
Let \( T(G) = \sum_{i=1}^{k(G)} d_i \).

[For example, for \( S_3 \), \((d_1, d_2, d_3) = (1, 1, 2) \) so \( T(S_3) = 4 \).]

Using the Cauchy-Schwarz inequality on \((1, 1, 1, \ldots, 1)\) and \((d_1, d_2, d_3, \ldots, d_k)\) as in [8], and remembering that \( \sum_{i=1}^{k} d_i^2 = |G|\), we find that

\[(T(G))^2 < k(G)|G| = I(G). \quad \text{(G non–abelian)}\]

Let us see how this inequality looks for some specific groups of small order.

[We use the notation \( Q_n \) for the dicyclic group of order \( 4n \) for \( n > 1 \) where \( Q_n = \langle a, b|a^{2n} = 1; b^2 = a^n, b^{-1}ab = a^{-1} \rangle \).]

### Group \((T(G))^2\) \( I(G)\)

<table>
<thead>
<tr>
<th>Group</th>
<th>(T(G))^2)</th>
<th>(I(G))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S_3)</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>(D_4)</td>
<td>36</td>
<td>40</td>
</tr>
<tr>
<td>(Q_2)</td>
<td>36</td>
<td>40 (quaternion group)</td>
</tr>
<tr>
<td>(D_5)</td>
<td>36</td>
<td>40</td>
</tr>
<tr>
<td>(D_6)</td>
<td>64</td>
<td>72</td>
</tr>
<tr>
<td>(Q_3)</td>
<td>64</td>
<td>72</td>
</tr>
<tr>
<td>(A_4)</td>
<td>36</td>
<td>48</td>
</tr>
<tr>
<td>(D_7)</td>
<td>64</td>
<td>70</td>
</tr>
<tr>
<td>(S_4)</td>
<td>100</td>
<td>120</td>
</tr>
</tbody>
</table>

When we write \( T(G) < \sqrt{I(G)} \) in a particular case such as \( D_4 \), we get \( T_4 < \sqrt{I(D_4)} = \sqrt{40} = 6.3245 \). Now \( T(D_4) \) is an integer so \( T(D_4) \leq 6 \) and 6 is actually the correct answer!

Similarly in the case of \( S_4 \), we get \( T(S_4) < \sqrt{120} = 10.95445 \). Again \( T(S_4) \) is an integer, so \( T(S_4) \leq 10 \) which gives the correct value of \( T(S_4) = 10 \).

It is remarkable that such a basic function as \( I(G) \), whose values can be read from the Cayley table, can be used to find information about \( T(G) \), which would appear to be a much more advanced group theoretic concept.

### 6. Analogues of \( I(G) \) and \( O(G) \)

There are so many analogies between \( k(G) \) and \( T(G) \) (as defined in section 5) that we make the following definitions:
For a finite non-abelian group $G$, let $N(G) = |G|T(G)$ and $M(G) = |G|(|G| - T(G))$.

It is not immediately clear what the interpretations of $N(G)$ and $M(G)$ are, but these functions have many properties analogous to $I(G)$ and $O(G)$. To save space we state results only, but methods of proof are very similar to those for results concerning $I(G)$ and $O(G)$. We remark that the properties of $|G| - T(G)$ are examined in some detail in [2].

**Theorem 6.1.** $I(G) < N(G)$ and $O(G) > M(G)$.

**Theorem 6.2.** There are only finitely many groups $G$ (maybe zero) with a given $N(G)$ or a given $M(G)$.

**Theorem 6.3.** $N(G)$ is odd if and only if $|G|$ is odd.

**Theorem 6.4.** If $|G|$ is odd, $M(G)$ is a multiple of $4|G|$.

**Theorem 6.5.** If $H$ is a proper subgroup of $G$, then $N(H) < N(G)$.

**Theorem 6.6.** $M(G)$ is always even.

**Theorem 6.7.** $N(G) < |G|^\frac{3}{2}(k(G))^{\frac{1}{2}}$.

**Theorem 6.8.** $N(G_1 \times G_2) = N(G_1) \cdot N(G_2)$.

**Theorem 6.9.** For the non-abelian group $G(pq)$, we have $N(G) = pq(p + q - 1)$ and $M(G) = pq(p - 1)(q - 1)$, where $p$ and $q$ are distinct odd primes.

**Theorem 6.10.** $N(G) \leq \frac{3}{4}|G|^2$ and $M(G) \geq \frac{1}{4}|G|^2$.

Finally, we give a chart of values of $N(G)$ and $M(G)$ for non-abelian groups $G$ of small order which leads to information about the sequences of allowable values of $N(G)$ and $M(G)$.
The sequence of allowable values of $N(G)$ thus begins 24, 48, 60, 72, 96, 112, 120, 160, 189, 192, 240, 264, 288, . . .

The sequence of allowable values of $M(G)$ thus begins 12, 16, 40, 48, 64, 72, 84, 136, 144, . . .

References


Brian Dolan is a mathematical graduate of University College Cork. He works currently in Computer Science in the UK.

Des MacHale is Emeritus Professor of Mathematics at University College Cork where he taught for nearly forty years. His mathematical interests are in abstract algebra but he also works in number theory, geometry, combinatorics and the
history of mathematics. His other interests include humour, geology and words. **Peter MacHale** is the Systems Manager in the Insight Centre for Data Analytics, Computer Science Department in University College Cork. His interests are constraint programming and graph theory. His other interests include music, science fiction and gaming.

(Brian Dolan and Des MacHale) **SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY COLLEGE CORK**

(Peter MacHale) **INSIGHT CENTRE FOR DATA ANALYTICS, UNIVERSITY COLLEGE CORK**

_E-mail address:_ curlyjim@gmail.com, d.machale@ucc.ie, p.machale@ucc.ie