# How many elements does it take to generate a finite permutation group?

Gareth Tracey

June 11, 2014

# Generating finite groups

For a group $G$, let $d(G)$ denote the minimal number of elements required to generate $G$.

# Generating finite groups

For a group $G$, let $d(G)$ denote the minimal number of elements required to generate $G$.

**Task:** Find an upper bound for $d(G)$ of the form

$$d(G) \leq f(\text{something to do with } G)$$

# Generating finite groups

For a group $G$, let $d(G)$ denote the minimal number of elements required to generate $G$.

**Task:** Find an upper bound for $d(G)$ of the form

$$d(G) \leq f(\text{something to do with } G)$$

What could the "something to do with $G$" be?

# Order?

# Order?

Fix a finite field $K$ of order $q$. Then the dimension of a (finite) vector space $V$ over $K$ is completely determined by its order, since $\dim V = \log_q(|V|)$.

# Order?

Fix a finite field $K$ of order $q$. Then the dimension of a (finite) vector space $V$ over $K$ is completely determined by its order, since $\dim V = \log_q(|V|)$.

Could we use the same principle with finite groups? That is, could we find a bound of the form

$$d(G) \leq f(|G|)$$

for some function $f$ of $|G|$?

# Order?

No!! Order has no effect (in general) on minimal generator numbers in finite groups.

# Order?

No!! Order has no effect (in general) on minimal generator numbers in finite groups.

<u>**Example:**</u> Let $p$ be prime, $n \geq 1$, and let $E_{p^n} = \mathbb{Z}_p^n$, which is a group under addition, the *elementary abelian* group of order $p^n$. Now, viewing $E_{p^n}$ as a group is completely equivalent to viewing $E_{p^n}$ as a vector space over $\mathbb{Z}_p$, and hence $d(E_{p^n}) = \dim_{\mathbb{Z}_p} E_{p^n} = n$. However, if $C_m$ denotes the cyclic group of order $m$, then $d(C_{p^n}) = 1$. Thus, we have two groups of the same order; one needing $n$ generators ($n$ can be arbitrarily large) and the other needing 1 generator.

# Order?

So cyclic groups give problems.. But what if we refine our search, and just look at the set of non-cyclic finite groups? Can we then find a correlation between order and the function $d$?

# Order?

So cyclic groups give problems.. But what if we refine our search, and just look at the set of non-cyclic finite groups? Can we then find a correlation between order and the function $d$?

No! There are many examples where we can see that there is no relationship between the functions $|.|$ and $d$ on the set of finite groups.

# Order?

So cyclic groups give problems.. But what if we refine our search, and just look at the set of non-cyclic finite groups? Can we then find a correlation between order and the function $d$?

No! There are many examples where we can see that there is no relationship between the functions $|.|$ and $d$ on the set of finite groups.

**Example:** As we've seen already, the elementary abelian group of order $8 = 2^3$ needs three generators, i.e. $d(E_8) = 3$.

# Order?

So cyclic groups give problems.. But what if we refine our search, and just look at the set of non-cyclic finite groups? Can we then find a correlation between order and the function $d$?

No! There are many examples where we can see that there is no relationship between the functions $|.|$ and $d$ on the set of finite groups.

**Example:** As we've seen already, the elementary abelian group of order $8 = 2^3$ needs three generators, i.e. $d(E_8) = 3$.

Now consider the largest of the finite simple groups, the Fischer-Griess Monster group, $M$. We have

$$|M| = 808017424794512875886459904961710757005754368000000000$$

# Order?

So cyclic groups give problems.. But what if we refine our search, and just look at the set of non-cyclic finite groups? Can we then find a correlation between order and the function $d$?

No! There are many examples where we can see that there is no relationship between the functions $|.|$ and $d$ on the set of finite groups.

**Example:** As we've seen already, the elementary abelian group of order $8 = 2^3$ needs three generators, i.e. $d(E_8) = 3$.

Now consider the largest of the finite simple groups, the Fischer-Griess Monster group, $M$. We have

$$|M| = 808017424794512875886459904961710757005754368000000000$$

But $d(M) = 2$.

# The behaviour of $d$ on the set of subgroups of $G$?

# The behaviour of $d$ on the set of subgroups of $G$?

In particular, the last example shows that, for finite groups $H$ and $G$, $|H| \leq |G| \not\Rightarrow d(H) \leq d(G)$. But is it true that $H \leq G$ (subgroup) $\Rightarrow d(H) \leq d(G)$?

# The behaviour of $d$ on the set of subgroups of $G$?

In particular, the last example shows that, for finite groups $H$ and $G$, $|H| \leq |G| \not\Rightarrow d(H) \leq d(G)$. But is it true that $H \leq G$ (subgroup) $\Rightarrow d(H) \leq d(G)$?

No..

# The behaviour of $d$ on the set of subgroups of $G$?

In particular, the last example shows that, for finite groups $H$ and $G$, $|H| \leq |G| \not\Rightarrow d(H) \leq d(G)$. But is it true that $H \leq G$ (subgroup) $\Rightarrow d(H) \leq d(G)$?

No..

**Example:** Let $n > 5$ be even, and consider the symmetric group $S_n$ of degree $n$. The permutations $(1, 2)$ and $(1, 2, \ldots, n)$ generate $S_n$ (and $S_n$ is noncyclic), so $d(S_n) = 2$.

# The behaviour of $d$ on the set of subgroups of $G$?

In particular, the last example shows that, for finite groups $H$ and $G$, $|H| \leq |G| \not\Rightarrow d(H) \leq d(G)$. But is it true that $H \leq G$ (subgroup) $\Rightarrow d(H) \leq d(G)$?

No..

**Example:** Let $n > 5$ be even, and consider the symmetric group $S_n$ of degree $n$. The permutations $(1,2)$ and $(1,2,\ldots,n)$ generate $S_n$ (and $S_n$ is noncyclic), so $d(S_n) = 2$.

Now consider $H = \langle (1,2),(3,4),\ldots,(n-1,n) \rangle \leq S_n$. Since all generators commute, and have order 2, we have $H \cong E_{2^{n/2}}$. Hence $d(H) = n/2$, so we have $H \leq S_n$, but $d(H) = n/2 > 2 = d(S_n)$.

# Some invariants of $G$ that have worked

(a) Minimal normal subgroups

# Some invariants of $G$ that have worked

(a) Minimal normal subgroups

**Theorem (Lucchini, 1995 (CFSG))**

*Let $N$ be a proper, minimal normal subgroup of the finite group $G$. Then $d(G) \leq d(G/N) + 1$.*

# Some invariants of $G$ that have worked

(a) Minimal normal subgroups

**Theorem (Lucchini, 1995 (CFSG))**

*Let $N$ be a proper, minimal normal subgroup of the finite group $G$. Then $d(G) \leq d(G/N) + 1$.*

**Theorem (Lucchini; Menegazzo, 1997 (CFSG))**

*Let the finite non-cyclic group $G$ have a unique minimal normal subgroup $M$. Then $d(G) = \max(2, d(G/M))$.*

# Some invariants of $G$ that have worked

(b) Sylow $p$-subgroups: Let

$$r(G) = \max\{d(P) : P \text{ a Sylow subgroup of} G\}$$

# Some invariants of $G$ that have worked

(b) Sylow $p$-subgroups: Let

$$r(G) = \max\{d(P) : P \text{ a Sylow subgroup of} G\}$$

**Theorem (Kovács, 1968)**

*Let $G$ be a finite soluble group. Then $d(G) \leq r(G) + 1$.*

# Some invariants of $G$ that have worked

(b) Sylow $p$-subgroups: Let

$$r(G) = \max\{d(P) : P \text{ a Sylow subgroup of} G\}$$

**Theorem (Kovács, 1968)**

*Let $G$ be a finite soluble group. Then $d(G) \leq r(G) + 1$.*

**Theorem (Longobardi; Maj, 1988 (CFSG))**

*Let $G$ be a finite group. Then $d(G) \leq 2r(G)$.*

# Some invariants of $G$ that have worked

(b) Sylow $p$-subgroups: Let

$$r(G) = \max\{d(P) : P \text{ a Sylow subgroup of} G\}$$

**Theorem (Kovács, 1968)**

*Let $G$ be a finite soluble group. Then $d(G) \leq r(G) + 1$.*

**Theorem (Longobardi; Maj, 1988 (CFSG))**

*Let $G$ be a finite group. Then $d(G) \leq 2r(G)$.*

**Theorem (Guralnick, 1989 (CFSG))**

*Let $G$ be a finite group. Then $d(G) \leq r(G) + 1$.*

# Some invariants of $G$ that have worked

(b) Sylow $p$-subgroups: Let

$$r(G) = \max\{d(P) : P \text{ a Sylow subgroup of} G\}$$

**Theorem (Kovács, 1968)**

*Let $G$ be a finite soluble group. Then $d(G) \leq r(G) + 1$.*

**Theorem (Longobardi; Maj, 1988 (CFSG))**

*Let $G$ be a finite group. Then $d(G) \leq 2r(G)$.*

**Theorem (Guralnick, 1989 (CFSG))**

*Let $G$ be a finite group. Then $d(G) \leq r(G) + 1$.*

All of these (apart from Kovács' 1968 result) rely heavily on the following idea:

# “Factorising” $G$

# "Factorising" $G$

Let $G$ be a finite group. Then $G$ has a composition series

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$

where each $G_i/G_{i-1}$ is simple.

## “Factorising” $G$

Let $G$ be a finite group. Then $G$ has a composition series

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$

where each $G_i/G_{i-1}$ is simple.

By the Jordan-Hölder Theorem, any two composition series for $G$ have the same length (called the *composition length* of $G$). Moreover, the set of composition factors $\{G_i/G_{i-1} : 1 \leq i \leq r\}$ is uniquely determined by $G$.

# "Factorising" $G$

Let $G$ be a finite group. Then $G$ has a composition series

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$

where each $G_i/G_{i-1}$ is simple.

By the Jordan-Hölder Theorem, any two composition series for $G$ have the same length (called the *composition length* of $G$). Moreover, the set of composition factors $\{G_i/G_{i-1} : 1 \leq i \leq r\}$ is uniquely determined by $G$.

Thus, the finite groups are, in some sense, built from the finite simple groups. This led to the following question, which dominated group theory in the twentieth century:

# “Factorising” $G$

Let $G$ be a finite group. Then $G$ has a composition series

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$

where each $G_i/G_{i-1}$ is simple.

By the Jordan-Hölder Theorem, any two composition series for $G$ have the same length (called the *composition length* of $G$). Moreover, the set of composition factors $\{G_i/G_{i-1} : 1 \leq i \leq r\}$ is uniquely determined by $G$.

Thus, the finite groups are, in some sense, built from the finite simple groups. This led to the following question, which dominated group theory in the twentieth century:

What are the finite simple groups?

# The classification of finite simple groups (CFSG): Timeline

# The classification of finite simple groups (CFSG): Timeline

Late 1800s: E. Mathieu and C. Jordan were first to realise the importance of simple groups in finite group theory; both discovered a number of finite simple groups; Mathieu discovered, in particular, five curious ones which would later form part of the list of the 26 sporadic simple groups.

# The classification of finite simple groups (CFSG): Timeline

Late 1800s: E. Mathieu and C. Jordan were first to realise the importance of simple groups in finite group theory; both discovered a number of finite simple groups; Mathieu discovered, in particular, five curious ones which would later form part of the list of the 26 sporadic simple groups.

Early 1900s: L. Dickson discovered finite analogues to the infinite groups (*Lie groups*) which were being constructed by S. Lie and E. Cartan. These turned out to be simple, and became known as *groups of Lie type*.

# The CFSG: Timeline

1905: List of known finite simple groups ran as follows:

- Groups of prime order;
- Groups of Lie type;
- Alternating groups;
- Mathieu's curious five.

# The CFSG: Timeline

1905: List of known finite simple groups ran as follows:

- Groups of prime order;
- Groups of Lie type;
- Alternating groups;
- Mathieu's curious five.

1955: Chevalley, Suzuki and Ree completed the construction of groups of Lie type.

# The CFSG: Timeline

1905: List of known finite simple groups ran as follows:

- Groups of prime order;
- Groups of Lie type;
- Alternating groups;
- Mathieu's curious five.

1955: Chevalley, Suzuki and Ree completed the construction of groups of Lie type.

1962: Feit-Thompson Theorem: Every finite group of odd order is solvable.

# The CFSG: Timeline

1905: List of known finite simple groups ran as follows:

- Groups of prime order;
- Groups of Lie type;
- Alternating groups;
- Mathieu's curious five.

1955: Chevalley, Suzuki and Ree completed the construction of groups of Lie type.

1962: Feit-Thompson Theorem: Every finite group of odd order is solvable.

1965: Z. Janko discovered the first new sporadic finite simple group since Mathieu's five.

# The CFSG: Timeline

Next dozen years: One or two new finite simple groups found per year, using ideas of the odd order theorem. Meanwhile, the classification gathered pace, led by Daniel Gorenstein, but with contribution from a number of authors (Thompson, Fischer, Glauberman, Alperin, . . .).

# The CFSG: Timeline

Next dozen years: One or two new finite simple groups found per year, using ideas of the odd order theorem. Meanwhile, the classification gathered pace, led by Daniel Gorenstein, but with contribution from a number of authors (Thompson, Fischer, Glauberman, Alperin, ...).

February 1981: Classification is completed, when Simon Norton proved the uniqueness of the Monster group, $M$.

# The CFSG

The proof of CFSG spans around 10,000 pages, 500 different journal articles, and was contributed to by around 100 different authors.

# The CFSG

The proof of CFSG spans around 10,000 pages, 500 different journal articles, and was contributed to by around 100 different authors.

Inevitably, mistakes were found! Most were rectified fairly easily, apart from the last one found, which took two books and seven years to fix; it was finally settled in 2004 by M. Aschbacher and S.Smith. According to Aschbacher, the proof has no further holes, and so the CFSG can now be regarded as a theorem.

# The CFSG

**Theorem (Classification of finite simple groups)**

*Every finite simple group is isomorphic to one of the following:*

- *Cyclic groups of prime order;*
- *Alternating groups;*
- *Groups of Lie type;*
- *26 sporadic simple groups.*

# Back to our original question

**Question:** How many elements does it take to generate a permutation group $G$ of degree $d$?

# Back to our original question

**Question:** How many elements does it take to generate a permutation group $G$ of degree $d$?

Recall that we want to find an upper bound on $d(G)$ of the form

$$d(G) \leq f(\text{something to do with } G)$$

# Back to our original question

**Question:** How many elements does it take to generate a permutation group $G$ of degree $d$?

Recall that we want to find an upper bound on $d(G)$ of the form

$$d(G) \leq f(\text{something to do with } G)$$

Here, the "something to do with $G$" will be the degree, $d$, of $G$ as a permutation group. That is, we want to bound $d(G)$ in terms of $d$.

# Theorems

The first main result in this direction came before CFSG:

# Theorems

The first main result in this direction came before CFSG:

**Theorem (Jerrum, 1976)**

*Let $G$ be a permutation group of degree $d$. Then $d(G) \leq d$.*

# Theorems

The first main result in this direction came before CFSG:

**Theorem (Jerrum, 1976)**

*Let $G$ be a permutation group of degree $d$. Then $d(G) \leq d$.*

After CFSG, Neumann made a significant improvement..

# Theorems

The first main result in this direction came before CFSG:

**Theorem (Jerrum, 1976)**

*Let $G$ be a permutation group of degree $d$. Then $d(G) \leq d$.*

After CFSG, Neumann made a significant improvement..

**Theorem (Neumann, 1989 (CFSG))**

*Let $G$ be a permutation group of degree $d$. Then $d(G) \leq d/2$, except that $d(G) = 2$ when $d = 3$ and $G \cong S_3$. Furthermore, if $G$ is transitive and $d \geq 5$, then $d(G) < d/2$, unless $d = 8$ and $G \cong D_8 \circ D_8$.*

# Theorems

The first main result in this direction came before CFSG:

**Theorem (Jerrum, 1976)**

*Let $G$ be a permutation group of degree $d$. Then $d(G) \leq d$.*

After CFSG, Neumann made a significant improvement..

**Theorem (Neumann, 1989 (CFSG))**

*Let $G$ be a permutation group of degree $d$. Then $d(G) \leq d/2$, except that $d(G) = 2$ when $d = 3$ and $G \cong S_3$. Furthermore, if $G$ is transitive and $d \geq 5$, then $d(G) < d/2$, unless $d = 8$ and $G \cong D_8 \circ D_8$.*

.. however, it was long suspected that substantially lower bounds would hold for special classes of permutation groups. For example, one of the more recent results is as follows:

# Theorems

**Theorem (Holt; Roney-Dougal, 2013 (CFSG))**

*Let $G$ be a primitive permutation group of degree $d$. Then $d(G) \leq \log_2(d)$.*

# Theorems

**Theorem (Holt; Roney-Dougal, 2013 (CFSG))**

*Let $G$ be a primitive permutation group of degree $d$. Then $d(G) \leq \log_2(d)$.*

After Neumann's 1989 result, the main focus turned to the asymptotic behaviour of $d(G)$, in terms of $d$.

# Asymptotic results

**Theorem (Kovács; Newman, 1988)**

*There exists a constant $c_1$ such that whenever $G$ is a nilpotent transitive permutation group of degree $d \geq 2$, then*

$$d(G) \leq c_1 d / \sqrt{\log_2 d}$$

# Asymptotic results

**Theorem (Kovács; Newman, 1988)**

*There exists a constant $c_1$ such that whenever $G$ is a nilpotent transitive permutation group of degree $d \geq 2$, then*

$$d(G) \leq c_1 d / \sqrt{\log_2 d}$$

**Theorem (Bryant; Kovács; Robinson, 1995 (CFSG))**

*There exists a constant $c_2$ such that whenever $G$ is a soluble transitive permutation group of degree $d \geq 2$, then*

$$d(G) \leq c_2 d / \sqrt{\log_2 d}$$

# Asymptotic results

**Theorem (Lucchini, 1998 (CFSG))**

*There exists a constant $c_3$ such that whenever $G$ is a permutation group of degree $d \geq 2$, containing a soluble transitive subgroup, then*

$$d(G) \leq c_3 d / \sqrt{\log_2 d}$$

# Asymptotic results

**Theorem (Lucchini, 1998 (CFSG))**

*There exists a constant $c_3$ such that whenever $G$ is a permutation group of degree $d \geq 2$, containing a soluble transitive subgroup, then*

$$d(G) \leq c_3 d / \sqrt{\log_2 d}$$

**Theorem (Lucchini; Menegazzo; Morigi, 2000 (CFSG))**

*There exists a constant $c_4$ such that whenever $G$ is a transitive permutation group of degree $d \geq 2$, then*

$$d(G) \leq c_4 d / \sqrt{\log_2 d}$$

# Constants

In fact, Kovács and Newman proved (in the nilpotent transitive case) that

$$d(G) \leq 4d/\sqrt{\log_2 d}$$

for all $d \geq 2$.

# Constants

In fact, Kovács and Newman proved (in the nilpotent transitive case) that

$$d(G) \leq 4d/\sqrt{\log_2 d}$$

for all $d \geq 2$.

However, the methods used in the proofs of the later results failed to yield estimates for the constants involved (although, Bryant et. al showed in their 1995 paper that the constant $c_1$ in the nilpotent case must satisfy $C \geq 1/\sqrt{2}$)..

# Estimating the constants

# Estimating the constants

**Theorem A**

*Let $G$ be a soluble transitive permutation group of degree $d \geq 2$. Then*

$$d(G) \leq c_2 d / \sqrt{\log_2 d}$$

*where* $c_2 = \sqrt{3}/2 = 0.8660254\ldots$.

# Estimating the constants

**Theorem A**

*Let $G$ be a soluble transitive permutation group of degree $d \geq 2$. Then*

$$d(G) \leq c_2 d / \sqrt{\log_2 d}$$

*where $c_2 = \sqrt{3}/2 = 0.8660254\ldots$.*

**Theorem B**

*Let $G$ be a transitive permutation group of degree $d \geq 2$. Then*

$$d(G) \leq c_4 d / \sqrt{\log_2 d}$$

*where $c_4 = 0.978113$.*

# Key idea of proofs: Wreath products

**Definition**

Let $R$ be a permutation group of degree $m$ (acting on $\{1, 2, \ldots, m\}$), and let $n \geq 1$. Then the *(permutational) wreath product* of $R$ with $S_n$, denoted $R \wr S_n$, is defined to be the semi-direct product $(R_1 \times R_2 \times \ldots \times R_n) \rtimes S_n$, where each $R_i \cong R$, and $G$ acts on $(R_1 \times R_2 \times \ldots \times R_n)$ by permutation of coordinates (e.g. $n = 3$, $r_i \in R_i \Rightarrow (r_1, r_2, r_3)^{(1,2,3)} = (r_3, r_1, r_2)$).

# Key idea of proofs: Wreath products

**Definition**

Let $R$ be a permutation group of degree $m$ (acting on $\{1, 2, \ldots, m\}$), and let $n \geq 1$. Then the *(permutational) wreath product* of $R$ with $S_n$, denoted $R \wr S_n$, is defined to be the semi-direct product $(R_1 \times R_2 \times \ldots \times R_n) \rtimes S_n$, where each $R_i \cong R$, and $G$ acts on $(R_1 \times R_2 \times \ldots \times R_n)$ by permutation of coordinates (e.g. $n = 3$, $r_i \in R_i \Rightarrow (r_1, r_2, r_3)^{(1,2,3)} = (r_3, r_1, r_2)$).

Let $\Omega_t = \{1, 2, \ldots, t\}$, for $t \geq 1$. $R \wr S_n$ acts on the cartesian product $\Omega := \Omega_m \times \Omega_n$ via

$$((r_1, r_2, \ldots, r_n), \sigma).(i, j) = (r_{\sigma(j)}.i, \sigma(j))$$

(e.g. $m = 4$, $n = 3$: $(((1,4),(1,3),(1,2)),(1,3,2)).(4,2) = (1,1)$)

# Key idea of proofs: Wreath products

Clearly this is an imprimitive action, with blocks $\Delta_j := \Omega_m \times \{j\}$, $1 \leq j \leq n$. So we have constructed examples of imprimitive permutation groups of degree $d = mn$. In fact, it turns out that all imprimitive permutation groups can be realised as a subgroup of one of the groups constructed above..

# Key idea of proofs: Wreath products

Clearly this is an imprimitive action, with blocks $\Delta_j := \Omega_m \times \{j\}$, $1 \leq j \leq n$. So we have constructed examples of imprimitive permutation groups of degree $d = mn$. In fact, it turns out that <u>all</u> imprimitive permutation groups can be realised as a subgroup of one of the groups constructed above..

**Theorem (Suprunenko, 1976)**

*Let $G$ be an imprimitive permutation group of degree $d$, and minimal block size $m$ (so $1 < m < d$). Then $G$ is (isomorphic to) a subgroup in a wreath product $R \wr S_n$, where $R$ is primitive of degree $m$, and $n = d/m$.*

# Idea of proofs

The proof proceeds by induction on $|G|$:

Initial step: Prove the theorem for primitive $G$. This follows immediately from

# Idea of proofs

The proof proceeds by induction on $|G|$:

Initial step: Prove the theorem for primitive $G$. This follows immediately from

**Theorem (Holt; Roney-Dougal, 2013)**

*Let $G$ be a primitive permutation group of degree $d$. Then $d(G) \leq \log_2(d)$.*

Inductive step: This concerns imprimitive $G$. By Suprunenko's Theorem, we have

$$G \leq R \wr S_n$$

for some primitive group $R$ of degree $m$, where $1 < m, n < d$, and $mn = d$.

# Examples

| $d$ | Neumann's Theorem gives $d(G) \leq$ | Theorem B gives $d(G) \leq$ | Max. value of $d(G)$ among the transitive groups of degree $d$ |
|---|---|---|---|
| 5 | 2 | 2 | 2 |
| 6 | 2 | 3 | 2 |
| 7 | 3 | 3 | 2 |
| 8 | 4 | 4 | 4 |
| 9 | 4 | 4 | 3 |
| 10 | 4 | 4 | 3 |

# Examples

## $G$ transitive of degree $d = 16$

Neumann's Theorem $\Rightarrow d(G) \leq 7$

# Examples

## $G$ transitive of degree $d = 16$

Neumann's Theorem $\Rightarrow d(G) \leq 7$

Theorem B $\Rightarrow d(G) \leq 6$

# Examples

**$G$ transitive of degree $d = 16$**

Neumann's Theorem $\Rightarrow d(G) \leq 7$

Theorem B $\Rightarrow d(G) \leq 6$

Maximum value of $d(G)$ among the transitive groups of degree 16 $= 6$

# Examples

## $G$ transitive of degree $d = 16$

Neumann's Theorem $\Rightarrow d(G) \leq 7$

Theorem B $\Rightarrow d(G) \leq 6$

Maximum value of $d(G)$ among the transitive groups of degree 16 $= 6$

## $G$ transitive of degree $d = 24$

Neumann's Theorem $\Rightarrow d(G) \leq 11$

# Examples

## $G$ transitive of degree $d = 16$

Neumann's Theorem $\Rightarrow d(G) \leq 7$

Theorem B $\Rightarrow d(G) \leq 6$

Maximum value of $d(G)$ among the transitive groups of degree 16 $= 6$

## $G$ transitive of degree $d = 24$

Neumann's Theorem $\Rightarrow d(G) \leq 11$

Theorem B $\Rightarrow d(G) \leq 9$

# Examples

**$G$ transitive of degree $d = 16$**

Neumann's Theorem $\Rightarrow d(G) \leq 7$

Theorem B $\Rightarrow d(G) \leq 6$

Maximum value of $d(G)$ among the transitive groups of degree 16 $= 6$

**$G$ transitive of degree $d = 24$**

Neumann's Theorem $\Rightarrow d(G) \leq 11$

Theorem B $\Rightarrow d(G) \leq 9$

Maximum value of $d(G)$ among the transitive groups of degree 24 $= 6$

# Examples

## $G$ transitive of degree $d = 32$

Neumann's Theorem $\Rightarrow d(G) \leq 15$

# Examples

**$G$ transitive of degree $d = 32$**

Neumann's Theorem $\Rightarrow d(G) \leq 15$

Theorem B $\Rightarrow d(G) \leq 12$

# Examples

**$G$ transitive of degree $d = 32$**

Neumann's Theorem $\Rightarrow d(G) \leq 15$

Theorem B $\Rightarrow d(G) \leq 12$

Maximum value of $d(G)$ among the transitive groups of degree 32 $= 10$

# Examples

### $G$ transitive of degree $d = 32$

Neumann's Theorem $\Rightarrow d(G) \leq 15$

Theorem B $\Rightarrow d(G) \leq 12$

Maximum value of $d(G)$ among the transitive groups of degree 32 $= 10$

### $G$ transitive of degree $d = 1000$

Neumann's Theorem $\Rightarrow d(G) \leq 499$

# Examples

## $G$ transitive of degree $d = 32$

Neumann's Theorem $\Rightarrow d(G) \leq 15$

Theorem B $\Rightarrow d(G) \leq 12$

Maximum value of $d(G)$ among the transitive groups of degree 32 $= 10$

## $G$ transitive of degree $d = 1000$

Neumann's Theorem $\Rightarrow d(G) \leq 499$

Theorem B $\Rightarrow d(G) \leq 274$

# Examples

**$G$ transitive of degree $d = 32$**

Neumann's Theorem $\Rightarrow d(G) \leq 15$

Theorem B $\Rightarrow d(G) \leq 12$

Maximum value of $d(G)$ among the transitive groups of degree 32 $= 10$

**$G$ transitive of degree $d = 1000$**

Neumann's Theorem $\Rightarrow d(G) \leq 499$

Theorem B $\Rightarrow d(G) \leq 274$

Maximum value of $d(G)$ among the transitive groups of degree 1000 $=$ unknown