Improving Cayley's Theorem for Groups of Order p^4

Sean McAfee

University of Illinois at Chicago

Undergraduate Mathematics Symposium – October 1, 2011

Statement of the Theorem

Cayley's Theorem: Let G be a group of order n. Then G is isomorphic to a subgroup of S_n.

Statement of the Theorem

Cayley's Theorem: Let G be a group of order n. Then G is isomorphic to a subgroup of S_n.

This theorem tells us that every group can be understood as a permutation group. However, it does little to tell us about the structure of G.

Statement of the Theorem

Cayley's Theorem: Let G be a group of order n. Then G is isomorphic to a subgroup of S_n.

This theorem tells us that every group can be understood as a permutation group. However, it does little to tell us about the structure of G.

Based on this information alone, all we can say is that G is contained in a group of size n!.

Can we do better?

A natural question to ask is, can this bound be improved?

Can we do better?

A natural question to ask is, can this bound be improved?

Can we find integers $m < n$ such that G is contained in S_m?

Can we do better?

A natural question to ask is, can this bound be improved?

Can we find integers $m < n$ such that G is contained in S_m?

Can we find the *least* integer ℓ such that G is contained in S_ℓ?

Can we do better?

A natural question to ask is, can this bound be improved?

Can we find integers $m < n$ such that G is contained in S_m?

Can we find the *least* integer ℓ such that G is contained in S_ℓ?

In many cases we can, and we will see that this number is closely tied to the minimal normal subgroups of G.

Restating the Question

It will be helpful to frame this problem in terms of group actions.

Restating the Question

It will be helpful to frame this problem in terms of group actions.

Suppose G is isomorphic to a subgroup of S_ℓ. This is the same as saying that G acts *faithfully* on some set A of size ℓ:

$$G \curvearrowright A.$$

Restating the Question

It will be helpful to frame this problem in terms of group actions.

Suppose G is isomorphic to a subgroup of S_ℓ. This is the same as saying that G acts *faithfully* on some set A of size ℓ:

$$G \curvearrowright A.$$

This is equivalent to G acting on the disjoint union of orbits of A:

$$G \curvearrowright \mathcal{O}_{x_1} \sqcup \ldots \sqcup \mathcal{O}_{x_k}.$$

Restating the Question

For a given orbit $\mathcal{O}_{x_i}$, we have a bijection between $\mathcal{O}_{x_i}$ and the collection of cosets $\frac{G}{Stab_{x_i}}$, where $Stab_{x_i} = \{g \in G | gx_i = x_i\}$. Thus our group action is equivalent to

Restating the Question

For a given orbit $\mathcal{O}_{x_i}$, we have a bijection between $\mathcal{O}_{x_i}$ and the collection of cosets $\frac{G}{Stab_{x_i}}$, where $Stab_{x_i} = \{g \in G | gx_i = x_i\}$.
Thus our group action is equivalent to

$$G \curvearrowright \frac{G}{Stab_{x_1}} \sqcup \ldots \sqcup \frac{G}{Stab_{x_k}}.$$

Restating the Question

Now, since the stabilizer of an element of A is a subgroup of G, we have that any group action can be represented by

Restating the Question

Now, since the stabilizer of an element of A is a subgroup of G, we have that any group action can be represented by

$$G \curvearrowright \frac{G}{H_1} \sqcup \ldots \sqcup \frac{G}{H_k},$$

for some subgroups $H_1,\ldots,H_k$ in G.

Restating the Question

Now, since the stabilizer of an element of A is a subgroup of G, we have that any group action can be represented by

$$G \curvearrowright \frac{G}{H_1} \sqcup \ldots \sqcup \frac{G}{H_k},$$

for some subgroups $H_1,\ldots,H_k$ in G.

It can be shown that this action is faithful if and only if the intersection of the H_i's contains no nontrivial minimal normal subgroups of G.

Restating the Question

This means that in order to find a smallest ℓ with G isomorphic to a subgroup of S_ℓ, we need a collection of subgroups $\{H_i\}$ of G such that:

Restating the Question

This means that in order to find a smallest ℓ with G isomorphic to a subgroup of S_ℓ, we need a collection of subgroups $\{H_i\}$ of G such that:

1. The intersection of the H_i's does not contain a minimal normal subgroup of G.

Restating the Question

This means that in order to find a smallest ℓ with G isomorphic to a subgroup of S_ℓ, we need a collection of subgroups $\{H_i\}$ of G such that:

1. The intersection of the H_i's does not contain a minimal normal subgroup of G.
2. $\left|\frac{G}{H_1}\right| + \ldots + \left|\frac{G}{H_k}\right|$ is as small as possible.

What Next?

How do we find such a collection of subgroups of G?

What Next?

How do we find such a collection of subgroups of G?

This can be difficult in general. For an arbitrary group G, we can't say much about what the minimal normal subgroups look like or where they might be found inside of G.

What Next?

How do we find such a collection of subgroups of G?

This can be difficult in general. For an arbitrary group G, we can't say much about what the minimal normal subgroups look like or where they might be found inside of G.

With groups of prime power order, however, our search is much easier..

Working with p-groups

A group G of order p^k has three properties which will be useful to us:

Working with p-groups

A group G of order p^k has three properties which will be useful to us:

1. The minimal normal subgroups of G are all of order p.

Working with p-groups

A group G of order p^k has three properties which will be useful to us:

1. The minimal normal subgroups of G are all of order p.
2. The minimal normal subgroups of G all lie in the center of G, denoted Z(G).

Working with p-groups

A group G of order p^k has three properties which will be useful to us:

1. The minimal normal subgroups of G are all of order p.
2. The minimal normal subgroups of G all lie in the center of G, denoted Z(G).
3. Every subgroup of Z(G) with order p is a minimal normal subgroup.

Working with p-groups

A group G of order p^k has three properties which will be useful to us:

1. The minimal normal subgroups of G are all of order p.
2. The minimal normal subgroups of G all lie in the center of G, denoted Z(G).
3. Every subgroup of Z(G) with order p is a minimal normal subgroup.

In other words, the minimal normal subgroups of G are *precisely* the subgroups of Z(G) of order p.

Working with p-groups

Therefore, if we know what Z(G) looks like, we can use this information to assemble a collection of subgroups of G which will allow us to calculate ℓ.

Working with p-groups

Therefore, if we know what Z(G) looks like, we can use this information to assemble a collection of subgroups of G which will allow us to calculate ℓ.

How do we do this? Let's work through a basic example.

An Example

Consider G$=\mathbb{Z}_p \times \mathbb{Z}_p$.

An Example

Consider $G = \mathbb{Z}_p \times \mathbb{Z}_p$.

This is an abelian group, so Z(G) is G itself.

An Example

Consider G=$\mathbb{Z}_p \times \mathbb{Z}_p$.

This is an abelian group, so Z(G) is G itself.

Thus we have that $N_1 = \{\mathbf{e}\} \times \mathbb{Z}_p$, $N_2 = \mathbb{Z}_p \times \{\mathbf{e}\}$, and $N_3 = \{(x, x) | x \in \mathbb{Z}_p\}$ are the minimal normal subgroups of G.

An Example

Recall that, in order to find our ℓ, we need a collection of subgroups $\{H_i\}$ in G whose intersection does not contain a minimal normal subgroup of G and such that $\left|\frac{G}{H_1}\right| + \ldots + \left|\frac{G}{H_k}\right|$ is as small as possible.

An Example

Recall that, in order to find our ℓ, we need a collection of subgroups $\{H_i\}$ in G whose intersection does not contain a minimal normal subgroup of G and such that $\left|\frac{G}{H_1}\right| + ... + \left|\frac{G}{H_k}\right|$ is as small as possible.

Let's try $H_1 = \{\mathbf{e}\} \times \mathbb{Z}_p$ and $H_2 = \mathbb{Z}_p \times \{\mathbf{e}\}$.

An Example

Recall that, in order to find our ℓ, we need a collection of subgroups $\{H_i\}$ in G whose intersection does not contain a minimal normal subgroup of G and such that $\left|\frac{G}{H_1}\right| + \ldots + \left|\frac{G}{H_k}\right|$ is as small as possible.

Let's try $H_1 = \{\mathbf{e}\} \times \mathbb{Z}_p$ and $H_2 = \mathbb{Z}_p \times \{\mathbf{e}\}$.

We have $H_1 \cap H_2 = \{\mathbf{e}\}$, thus the intersection doesn't contain a minimal normal subgroup of G.

An Example

Recall that, in order to find our ℓ, we need a collection of subgroups $\{H_i\}$ in G whose intersection does not contain a minimal normal subgroup of G and such that $\left|\frac{G}{H_1}\right| + \ldots + \left|\frac{G}{H_k}\right|$ is as small as possible.

Let's try $H_1 = \{\mathbf{e}\} \times \mathbb{Z}_p$ and $H_2 = \mathbb{Z}_p \times \{\mathbf{e}\}$.

We have $H_1 \cap H_2 = \{\mathbf{e}\}$, thus the intersection doesn't contain a minimal normal subgroup of G.

Also, note that if H_1 or H_2 were any larger, their intersection would have to contain N_1, N_2, or N_3.

An Example

This means we have $\left|\frac{G}{H_1}\right| + \left|\frac{G}{H_2}\right|$ as small as possible.

An Example

This means we have $\left|\frac{G}{H_1}\right| + \left|\frac{G}{H_2}\right|$ as small as possible.

This gives us $\ell = \left|\frac{G}{H_1}\right| + \left|\frac{G}{H_2}\right| = \frac{p^2}{p} + \frac{p^2}{p} = 2p$.

An Example

This means we have $\left|\frac{G}{H_1}\right| + \left|\frac{G}{H_2}\right|$ as small as possible.

This gives us $\ell = \left|\frac{G}{H_1}\right| + \left|\frac{G}{H_2}\right| = \frac{p^2}{p} + \frac{p^2}{p} = 2p$.

Thus we have $\mathbb{Z}_p \times \mathbb{Z}_p$ isomorphic to a subgroup of S_{2p}, with 2p being the smallest integer with this property.

A Simple Algorithm

We were able to solve this example by inspection; as p-groups become larger and more complicated, it may not be as clear what our choice of subgroups should be.

A Simple Algorithm

We were able to solve this example by inspection; as p-groups become larger and more complicated, it may not be as clear what our choice of subgroups should be.

In their paper *Finding minimal permutation representations of finite groups*, Ben Elias, Lior Silberman, and Ramin Takloo-Bighash offer an algorithm to determine ℓ for a given p-group, provided we know something about its subgroup structure.

A Simple Algorithm

We were able to solve this example by inspection; as p-groups become larger and more complicated, it may not be as clear what our choice of subgroups should be.

In their paper *Finding minimal permutation representations of finite groups*, Ben Elias, Lior Silberman, and Ramin Takloo-Bighash offer an algorithm to determine ℓ for a given p-group, provided we know something about its subgroup structure.

To understand how this algorithm works, we need to make a quick definition.

A Simple Algorithm

We define the **socle** of a group G to be the smallest subgroup in G containing all of its minimal normal subgroups. We denote the socle by M.

A Simple Algorithm

We define the **socle** of a group G to be the smallest subgroup in G containing all of its minimal normal subgroups. We denote the socle by M.

In our previous example, then, we have that the socle of the group is the group itself (this will not be the case in general):

$$G = \mathbb{Z}_p \times \mathbb{Z}_p = M.$$

A Simple Algorithm

We define the **socle** of a group G to be the smallest subgroup in G containing all of its minimal normal subgroups. We denote the socle by M.

In our previous example, then, we have that the socle of the group is the group itself (this will not be the case in general):

$$G = \mathbb{Z}_p \times \mathbb{Z}_p = M.$$

With this definition in mind, we can describe an algorithm for finding ℓ in any p-group.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

Step 1: Find a subgroup K_1 in G of maximal size such that $M \not\subseteq K_1$.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

Step 1: Find a subgroup K_1 in G of maximal size such that $M \not\subseteq K_1$. If $M \cap K_1 = \{\mathbf{e}\}$, we are done. If not, proceed to step 2.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

Step 1: Find a subgroup K_1 in G of maximal size such that $M \not\subseteq K_1$. If $M \cap K_1 = \{\mathbf{e}\}$, we are done. If not, proceed to step 2.

Step 2: Find a subgroup K_2 in G of maximal size such that $(M \cap K_1) \not\subseteq K_2$.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

Step 1: Find a subgroup K_1 in G of maximal size such that $M \not\subseteq K_1$. If $M \cap K_1 = \{\mathbf{e}\}$, we are done. If not, proceed to step 2.

Step 2: Find a subgroup K_2 in G of maximal size such that $(M \cap K_1) \not\subseteq K_2$. If $M \cap K_1 \cap K_2 = \{\mathbf{e}\}$, we are done. If not, proceed to step 3.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

Step 1: Find a subgroup K_1 in G of maximal size such that $M \not\subseteq K_1$. If $M \cap K_1 = \{\mathbf{e}\}$, we are done. If not, proceed to step 2.

Step 2: Find a subgroup K_2 in G of maximal size such that $(M \cap K_1) \not\subseteq K_2$. If $M \cap K_1 \cap K_2 = \{\mathbf{e}\}$, we are done. If not, proceed to step 3.

Step n: Find a subgroup K_n in G of maximal size such that $(M \cap K_1 \cap \ldots \cap K_{n-1}) \not\subseteq K_n$.

A Simple Algorithm

Let G be a group of prime power order, and let M be the socle of G.

Step 1: Find a subgroup K_1 in G of maximal size such that $M \not\subseteq K_1$. If $M \cap K_1 = \{\mathbf{e}\}$, we are done. If not, proceed to step 2.

Step 2: Find a subgroup K_2 in G of maximal size such that $(M \cap K_1) \not\subseteq K_2$. If $M \cap K_1 \cap K_2 = \{\mathbf{e}\}$, we are done. If not, proceed to step 3.

Step n: Find a subgroup K_n in G of maximal size such that $(M \cap K_1 \cap \ldots \cap K_{n-1}) \not\subseteq K_n$. If $M \cap K_1 \cap \ldots \cap K_n = \{\mathbf{e}\}$, we are done. If not, proceed to step n+1.

A Simple Algorithm

This process will terminate after a finite number of steps, and the result will be a collection $\{K_1, K_2, \ldots, K_n\}$ of subgroups of G such that:

A Simple Algorithm

This process will terminate after a finite number of steps, and the result will be a collection $\{K_1, K_2, \ldots, K_n\}$ of subgroups of G such that:

1. The intersection of the K_i's does not contain a minimal normal subgroup of G.

A Simple Algorithm

This process will terminate after a finite number of steps, and the result will be a collection $\{K_1, K_2, \ldots, K_n\}$ of subgroups of G such that:

1. The intersection of the K_i's does not contain a minimal normal subgroup of G.
2. $\left|\frac{G}{K_1}\right| + \ldots + \left|\frac{G}{K_n}\right|$ is as small as possible.

Working with $|G| = p^4$

By applying this algorithm to a database of groups of order p^4, the authors of the paper were able to make the following conjecture:

Working with $|G| = p^4$

By applying this algorithm to a database of groups of order p^4, the authors of the paper were able to make the following conjecture:
For $p > 3$,

$$\sum_{|G|=p^4} \ell = 9p + 11p^2 + 5p^3 + p^4.$$

Working with $|G| = p^4$

By applying this algorithm to a database of groups of order p^4, the authors of the paper were able to make the following conjecture:
For $p > 3$,

$$\sum_{|G|=p^4} \ell = 9p + 11p^2 + 5p^3 + p^4.$$

Verifying this conjecture was a matter of researching presentations of groups of order p^4, determining their subgroup structure, and applying the algorithm.

Abelian groups of order p^4

There are 15 groups of order p^4 up to isomorphism, 5 of which are abelian:

Abelian groups of order p^4

There are 15 groups of order p^4 up to isomorphism, 5 of which are abelian:

	p-group	ℓ
(i)	$\mathbb{Z}_{p^4}$	p^4
(ii)	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p$	$p + p^3$
(iii)	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$	$2p^2$
(iv)	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$	$2p + p^2$
(v)	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$	$4p$

Non-Abelian Groups of Order p^4

In their paper *On p-groups of low power order*, Gustav Stahl and Johan Laine provide presentations of groups of order p^4 as semi-direct products. This form of presentation allows us to easily calculate the center and socle of a given p-group. It is then a process of trial and error to find ℓ for each group.

Non-Abelian Groups of Order p^4

	p-group	ℓ
(vi)	$\mathbb{Z}_{p^3} \rtimes_\varphi \mathbb{Z}_p$	p^3
(vii)	$(\mathbb{Z}_{p^2} \times \mathbb{Z}_p) \rtimes_\varphi \mathbb{Z}_p$	p^3
(viii)	$\mathbb{Z}_{p^2} \rtimes_\varphi \mathbb{Z}_{p^2}$	$2p^2$
(ix)	$(\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p) \times \mathbb{Z}_p$	$p + p^2$
(x)	$(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes_\varphi \mathbb{Z}_{p^2}$	$2p^2$
(xi)	$(\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p) \rtimes_{\varphi_1} \mathbb{Z}_p$	p^2
(xii)	$(\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p) \rtimes_{\varphi_2} \mathbb{Z}_p$	p^3
(xiii)	$(\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p) \rtimes_{\varphi_3} \mathbb{Z}_p$	p^3
(xiv)	$((\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p) \times \mathbb{Z}_p$	$p + p^2$
(xv)	$(\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p) \rtimes_\varphi \mathbb{Z}_p$	p^2

Verifying the Conjecture

Taking the sum of the ℓ's from these results gives us:

Verifying the Conjecture

Taking the sum of the ℓ's from these results gives us:

$$\sum_{\ell} = 9p + 11p^2 + 5p^3 + p^4,$$

which verifies the conjecture.

Thank You