Groups with every minimal generating set of fixed size

Jonathan McDougall-Bagnall

University of St Andrews

7th August, 2009

Groups St Andrews: Bath
Supported by the EPSRC doctoral training grant.
Outline Of Talk

1 Introduction
   • Motivation
   • History
   • A Few Examples

2 Theoretical Results

3 A Constructed Example
   • Results From the Construction

4 Future Work
Motivation

Definition

A generating set $A$ of a group $G$ is said to be minimal if no proper subset of $A$ generates $G$. 

Burnside Basis Theorem:

For a $p$-group $G$:

- Min gen sets for $G$ ↔ bases for the vector space $G/\Phi(G)$.

Every min gen set for $G$ has fixed size. (B) 

This is the property we will investigate.
A generating set $A$ of a group $G$ is said to be minimal if no proper subset of $A$ generates $G$.

Burnside Basis Theorem: $G$ a $p$-group:

- Min gen sets for $G \longleftrightarrow$ bases for the v. space $G/\Phi(G)$.
- Every min gen set for $G$ has fixed size. ($B$)
A generating set $A$ of a group $G$ is said to be minimal if no proper subset of $A$ generates $G$.

**Burnside Basis Theorem:** $G$ a $p$-group:

- Min gen sets for $G \leftrightarrow$ bases for the v. space $G/\Phi(G)$.
- Every min gen set for $G$ has fixed size. ($B$)

This is the property we will investigate.
Scapellato, Verardi (1991)

- Investigated a more restricted class of groups, called matroidal groups.
- These groups satisfy property $B$ and two other conditions satisfied by $v$ spaces.
Scapellato, Verardi (1991)

- Investigated a more restricted class of groups, called matroidal groups.
- These groups satisfy property $B$ and two other conditions satisfied by $v$ spaces.
- Matroidal group $G$ with trivial Frattini subgroup is
  - An elementary abelian $p$-group
  - $|G| = p^nq$ and $\text{Fit } G$ is elementary abel, $|\text{Fit } G| = p^n$, $p, q$ prime $p \equiv 1 \pmod{q}$, and an element of order $q$ induces a power automorphism on $\text{Fit } G$. 
Scapellato, Verardi (1991)

- Investigated a more restricted class of groups, called matroidal groups.
- These groups satisfy property $\mathcal{B}$ and two other conditions satisfied by $\nu$ spaces.
- Matroidal group $G$ with trivial Frattini subgroup is
  - An elementary abelian $p$-group
  - $|G| = p^n q$ and $\text{Fit} G$ is elementary abel, $|\text{Fit} G| = p^n$, $p, q$ prime $p \equiv 1 \pmod{q}$, and an element of order $q$ induces a power automorphism on $\text{Fit} G$.

A power automorphism preserves subgroups and so greatly restricts the structure of a group and so we see that property $\mathcal{B}$ is a more natural property to investigate.
Groups with property $\mathcal{B}$

The following groups have property $\mathcal{B}$:

- $p$-groups, from Burnside's Basis Theorem.
- Dihedral groups of order $2p^n$ where $p$ is prime (matroidal).
- $A_4$ (not matroidal) and $S_3$.

We will also provide a construction of a class of groups with property $\mathcal{B}$ later on.
The following groups have property $B$:

- $p$-groups, from Burnside’s Basis Theorem.
The following groups have property $B$:

- $p$-groups, from Burnside’s Basis Theorem.
- Dihedral groups of order $2p^n$ where $p$ is prime (matroidal).
Groups with property $\mathcal{B}$

The following groups have property $\mathcal{B}$:

- $p$-groups, from Burnside’s Basis Theorem.
- Dihedral groups of order $2p^n$ where $p$ is prime (matroidal).
- $A_4$ (not matroidal) and $S_3$
Groups with property $B$

The following groups have property $B$:

- $p$-groups, from Burnside’s Basis Theorem.
- Dihedral groups of order $2p^n$ where $p$ is prime (matroidal).
- $A_4$ (not matroidal) and $S_3$

We will also provide a construction of a class of groups with property $B$ later on.
Groups without property $B$

We also have several examples of groups without property $B$:

- Cyclic groups of non-prime power order e.g. $C_6$.
- $S_n$ where $n > 3$.
  - $S_n$ is minimally generated by the set of transpositions $\{(12), (23), (34), \ldots, ((n-1)n)\}$ and the set $\{(12 \ldots n), (12)\}$.

Non-abelian simple groups.

The proof of this relies on the CFSG and is sketched as follows:

- All non-abelian simple groups are minimally generated by 2 elements, CFSG (Guralnick, Kantor, 2000).
- Let $T$ be the set of all elements of $G$ of order 2 and since $\langle T \rangle$ is normal in $G$ it is in fact $G$.
- Let $T_0$ be a subset of $T$ that minimally generates $G$.
  - $T_0$ must have more than 2 elements otherwise $\langle T_0 \rangle = G$ would be isomorphic to a dihedral group.
Groups without property $\mathcal{B}$

We also have several examples of groups without property $\mathcal{B}$:

- Cyclic groups of non-prime power order e.g. $C_6$. 

Non-abelian simple groups.
The proof of this relies on the CFSG and is sketched as follows:

Let $T$ be the set of all elements of $G$ of order 2 and since $\langle T \rangle$ is normal in $G$ it is in fact $G$.

Let $T_0$ be a subset of $T$ that minimally generates $G$.

$T_0$ must have more than 2 elements otherwise $\langle T_0 \rangle = G$ would be isomorphic to a dihedral group.
We also have several examples of groups without property $B$:

- Cyclic groups of non-prime power order e.g. $C_6$.
- $S_n$ where $n > 3$. 

Non-abelian simple groups.

The proof of this relies on the CFSG and is sketched as follows:

Let $T$ be the set of all elements of $G$ of order 2 and since $\langle T \rangle$ is normal in $G$, it is in fact $G$.

Let $T_0$ be a subset of $T$ that minimally generates $G$.

$T_0$ must have more than 2 elements otherwise $\langle T_0 \rangle = G$ would be isomorphic to a dihedral group.
We also have several examples of groups without property \( \mathcal{B} \):

- Cyclic groups of non-prime power order e.g. \( C_6 \).
- \( S_n \) where \( n > 3 \).
  \( S_n \) is minimally generated by the set of transpositions \( \{(12), (23), (34), \ldots, ((n-1)n)\} \) and the set \( \{(12 \ldots n), (12)\} \).

Non-abelian simple groups. The proof of this relies on the CFSG and is sketched as follows:

All non-abelian simple groups are minimally generated by 2 elements, CFSG (Guralnick, Kantor, 2000).

Let \( T \) be the set of all elements of \( G \) of order 2 and since \( \langle T \rangle \) is normal in \( G \) it is in fact \( G \).

Let \( T_0 \) be a subset of \( T \) that minimally generates \( G \).

\( T_0 \) must have more than 2 elements otherwise \( \langle T_0 \rangle = G \) would be isomorphic to a dihedral group.
We also have several examples of groups without property $B$:

- Cyclic groups of non-prime power order e.g. $C_6$.
- $S_n$ where $n > 3$.
  $S_n$ is minimally generated by the set of transpositions $\{(12), (23), (34), \ldots, ((n - 1)n)\}$ and the set $\{(12 \ldots n), (12)\}$.
- Non-abelian simple groups.
Groups without property $\mathcal{B}$

We also have several examples of groups without property $\mathcal{B}$:

- Cyclic groups of non-prime power order e.g. $C_6$.
- $S_n$ where $n > 3$.
  $S_n$ is minimally generated by the set of transpositions
  $\{(12), (23), (34), \ldots, ((n-1)n)\}$ and the set $\{(12\ldots n), (12)\}$.
- Non-abelian simple groups.
  The proof of this relies on the CFSG and is sketched as follows:
  - All non-abelian simple groups are minimally generated by 2 elements, CFSG (Guralnick, Kantor, 2000).
  - Let $T$ be the set of all elements of $G$ of order 2 and since $\langle T \rangle$ is normal in $G$ it is in fact $G$.
  - Let $T_0$ be a subset of $T$ that minimally generates $G$.
  - $T_0$ must have more than 2 elements otherwise $\langle T_0 \rangle = G$ would be isomorphic to a dihedral group.
We have the following results about how property $B$ behaves under extensions.
We have the following results about how property $\mathcal{B}$ behaves under extensions.

**Theorem**

The group $G \times H$ has property $\mathcal{B}$ if and only if $G \times H$ is a $p$-group.
Extensions of Groups with Property $\mathcal{B}$

We have the following results about how property $\mathcal{B}$ behaves under extensions

**Theorem**

The group $G \times H$ has property $\mathcal{B}$ if and only if $G \times H$ is a $p$-group.

**Lemma**

The wreath product of $G$ and $H$ has property $\mathcal{B}$ if both $G$ and $H$ have property $\mathcal{B}$.
Lemma

\( G \) has \( \mathcal{B} \) \( \iff \) \( G/\Phi(G) \) has property \( \mathcal{B} \).

This holds by simply exploiting the Frattini subgroup to be the set of non-generators of \( G \). But what about quotients in general.
How Property $\mathcal{B}$ Transfers to a Quotient

**Lemma**

$G$ has $\mathcal{B} \iff G/\Phi(G)$ has property $\mathcal{B}$.

This holds by simply exploiting the Frattini subgroup to be the set of non-generators of $G$. But what about quotients in general.

**Theorem**

*If $G$ has $\mathcal{B}$ and $M$ is a minimal normal subgroup of $G$ then $G/M$ has $\mathcal{B}$.***

There are 2 cases to the proof of this theorem, either $G$ splits over $M$ or it doesn’t.
Sketch of Proof:  $G$ Splits Over $M$

$G = MQ$ where $Q \cong G/M$ and is the complement of $M$. 

Jonathan McDougall-Bagnall (St. And) 7th August, 2009
Sketch of Proof: $G$ Splits Over $M$

$G = MQ$ where $Q \cong G/M$ and is the complement of $M$.

- Let $x_1, \ldots, x_d$ be minimal s.t. $\langle x_1, \ldots, x_d \rangle^Q = M$. 
Sketch of Proof: \( G \) Splits Over \( M \)

\[
G = MQ \quad \text{where} \quad Q \cong G/M \quad \text{and is the complement of} \quad M.
\]

- Let \( x_1, \ldots, x_d \) be minimal s.t. \( \langle x_1, \ldots, x_d \rangle^Q = M \).
- \( A = \{ x_1, \ldots x_d, y_1, \ldots y_k \} \) where \( \{ y_1, \ldots, y_k \} \) is a min gen set for \( Q \implies A \) min gen set for \( G \).
Sketch of Proof: $G$ Splits Over $M$

$G = MQ$ where $Q \cong G/M$ and is the complement of $M$.

- Let $x_1, \ldots, x_d$ be minimal s.t. $\langle x_1, \ldots, x_d \rangle^Q = M$.
- $A = \{x_1, \ldots, x_d, y_1, \ldots, y_k\}$ where $\{y_1, \ldots, y_k\}$ is a min gen set for $Q \Rightarrow A$ min gen set for $G$.
- Exploit the fact that $G$ has $B$ which forces $k$ to be of fixed size $\Rightarrow Q \cong G/M$ has $B$. 
Assume \( M \) is elementary abelian.
Assume $M$ is elementary abelian.

- View $M$ as an $\mathbb{F}_p Q$-module.
- Let $x_1, x_2, \ldots, x_d$ be elements of $G$ s.t. $A = \{Mx_1, Mx_2, \ldots, Mx_d\}$ a min gen set for $Q$.
- $X = \langle x_1, x_2, \ldots, x_d \rangle \implies G = MX$ and $M \cap X \neq 1$.
- Take $y \in M \cap X$. $M$ is abelian so $\langle y^X \rangle = \langle y^{MX} \rangle = \langle y^G \rangle = M$.
- So $M < X \implies X = G$. Thus $x_1, x_2, \ldots, x_d$ is a min gen set for $G$.
- $G$ has $B$ so $d$ of fixed size $\implies Q \cong G/M$ has $B$. 

If we assume that $M$ is non-abelian we have a similar set up. In the elementary abelian case we showed that $M \cap X = M$ and the result followed. When $M$ is non-abelian we have 2 cases.
If we assume that $M$ is non-abelian we have a similar set up. In the elementary abelian case we showed that $M \cap X = M$ and the result followed. When $M$ is non-abelian we have 2 cases.

- $M \cap X = M$: Here we exploit a result by Gaschütz (1955) which shows that if this happens for one choice of $X$ it happens for all choices of $X$. This allows us to lift a generating set for the quotient to $G$ as in the elementary abelian case.
If we assume that $M$ is non-abelian we have a similar set up. In the elementary abelian case we showed that $M \cap X = M$ and the result followed. When $M$ is non-abelian we have 2 cases.

- $M \cap X = M$: Here we exploit a result by Gaschütz (1955) which shows that if this happens for one choice of $X$ it happens for all choices of $X$. This allows us to lift a generating set for the quotient to $G$ as in the elementary abelian case.

- $M \cap X < M$: Here we must use a paper by Stein (1998) which shows we need one more generator for $M$. 
All this gives us the following corollary
All this gives us the following corollary

**Corollary**

*If $G$ has property $B$ then any quotient $G/N$ also has property $B$.***
All this gives us the following corollary

**Corollary**

*If $G$ has property $\mathcal{B}$ then any quotient $G/N$ also has property $\mathcal{B}$.***

The proof proceeds by induction on the order of $N$.

- Let $M$ be a min norm subgroup of $G$ s.t. $M$ is contained in $N$.
- By the third isomorphism theorem we have that, $G/N \cong \frac{G/M}{N/M}$.
- By induction this quotient has property $\mathcal{B}$ if $G/M$ has property $\mathcal{B}$.
Initially the only non $p$-groups we found that had $\mathcal{B}$ were the Dihedral groups mentioned earlier. After some computational work we found other examples existed. We noticed that these groups all had similar structure.
Initially the only non $p$-groups we found that had $\mathcal{B}$ were the Dihedral groups mentioned earlier. After some computational work we found other examples existed. We noticed that these groups all had similar structure. A dihedral group with $\mathcal{B}$ can be viewed as the semidirect product

$$\underbrace{(C_p \times \cdots \times C_p) \rtimes C_2}_{n \text{ times}}$$

where the cyclic group of order two acts by inversion. Our construction turns out to be similar.
Take $V$ to be the additive group of $\mathbb{F}_{p^n}$ isomorphic to $n$ direct products of $C_p$. 
1. Take $V$ to be the additive group of $\mathbb{F}_{p^n}$ isomorphic to $n$ direct products of $C_p$.

2. Let $H$ be $C_{q^m}$ embedded as the unique subgroup of the multiplicative group of the field $\mathbb{F}_{p^n}$ ($q^m | p^n - 1$ where $p$ and $q$ are primes).
The Construction

1. Take $V$ to be the additive group of $\mathbb{F}_{p^n}$ isomorphic to $n$ direct products of $C_p$.

2. Let $H$ be $C_{q^m}$ embedded as the unique subgroup of the multiplicative group of the field $\mathbb{F}_{p^n}$ ($q^m \mid p^n - 1$ where $p$ and $q$ are primes).

3. Now we define a mapping $\phi : H \rightarrow \text{Aut}(V)$ such that $h\phi$ is the automorphism of $V$, $v \mapsto vh$. 

4. Create the semidirect product $V \rtimes \phi H$ which is isomorphic to $(C_p \times \cdots \times C_p) \rtimes \phi C_{q^m}$. The cyclic group of order $q^m$ acts on the left hand side by multiplication in the field $\mathbb{F}_{p^n}$ and we can see that $\phi$ induces upon $V$ the structure of an $\mathbb{F}_p H$-module.
The Construction

1. Take $V$ to be the additive group of $\mathbb{F}_{p^n}$ isomorphic to $n$ direct products of $C_p$.

2. Let $H$ be $C_{q^m}$ embedded as the unique subgroup of the multiplicative group of the field $\mathbb{F}_{p^n}$ ($q^m | p^n - 1$ where $p$ and $q$ are primes).

3. Now we define a mapping $\phi : H \to \text{Aut}(V)$ such that $h\phi$ is the automorphism of $V$, $v \mapsto vh$.

4. Create the semidirect product $V \rtimes_{\phi} H$ which is isomorphic to

\[
(C_p \times \cdots \times C_p) \rtimes_{\phi} C_{q^m}
\]

$n$ times
1. Take \( V \) to be the additive group of \( \mathbb{F}_{p^n} \) isomorphic to \( n \) direct products of \( C_p \).

2. Let \( H \) be \( C_{q^m} \) embedded as the unique subgroup of the multiplicative group of the field \( \mathbb{F}_{p^n} \) \((q^m|p^n - 1 \text{ where } p \text{ and } q \text{ are primes})\).

3. Now we define a mapping \( \phi : H \rightarrow \text{Aut}(V) \) such that \( h\phi \) is the automorphism of \( V \), \( v \mapsto vh \).

4. Create the semidirect product \( V \rtimes \phi H \) which is isomorphic to

\[
(C_p \times \cdots \times C_p) \rtimes \phi C_{q^m}
\]

\( n \) times

The cyclic group of order \( q^m \) acts on the left hand side by multiplication in the field \( \mathbb{F}_{p^n} \) and we can see that \( \phi \) induces upon \( V \) the structure of an \( \mathbb{F}_pH \)-module.
Some Results

**Theorem**

If $G$ is isomorphic to $V \rtimes \phi H$ then $G$ has property $\mathcal{B}$ with $d(G)$ being $k + 1$ where $V$ is the sum of $k$ of irreducible $\mathbb{F}_pH$-modules and $\Phi(G)$ is trivial.
Some Results

Theorem

If $G$ is isomorphic to $V \rtimes \phi H$ then $G$ has property $B$ with $d(G)$ being $k+1$ where $V$ is the sum of $k$ of irreducible $\mathbb{F}_pH$-modules and $\Phi(G)$ is trivial.

Generalizing ideas from Scapellato and Verardi (1991) we were able to obtain the following
Some Results

Theorem

If $G$ is isomorphic to $V \rtimes_\phi H$ then $G$ has property $B$ with $d(G)$ being $k + 1$ where $V$ is the sum of $k$ of irreducible $\mathbb{F}_pH$-modules and $\Phi(G)$ is trivial.

Generalizing ideas from Scapellato and Verardi (1991) we were able to obtain the following

Theorem

If $G$ is a group such that the quotient group $G/\Phi(G)$ is isomorphic to $V \rtimes_\phi H$ then

1. $G$ has a unique Sylow $p$-subgroup $P$,
2. $G$ is isomorphic to $P \rtimes Q$ for any Sylow $q$-subgroup $Q$ and all Sylow $q$-subgroups of $G$ are cyclic,
3. $\Phi(G) = \Phi(P) \times \langle x^q \rangle$ where $\langle x^q \rangle$ is the subgroup of index $q^m$ in $Q = \langle x \rangle$. 

Jonathan McDougall-Bagnall (St. And) 7th August, 2009 15 / 16
Some Results

Theorem

If $G$ is isomorphic to $V \rtimes_{\phi} H$ then $G$ has property $\mathcal{B}$ with $d(G)$ being $k + 1$ where $V$ is the sum of $k$ of irreducible $\mathbb{F}_p H$-modules and $\Phi(G)$ is trivial.

Generalizing ideas from Scapellato and Verardi (1991) we were able to obtain the following

Theorem

If $G$ is a group such that the quotient group $G/\Phi(G)$ is isomorphic to $V \rtimes_{\phi} H$ then

1. $G$ has a unique Sylow $p$-subgroup $P$,
Some Results

Theorem

If $G$ is isomorphic to $V \rtimes_{\phi} H$ then $G$ has property $\mathcal{B}$ with $d(G)$ being $k + 1$ where $V$ is the sum of $k$ of irreducible $\mathbb{F}_p H$-modules and $\Phi(G)$ is trivial.

Generalizing ideas from Scapellato and Verardi (1991) we were able to obtain the following

Theorem

If $G$ is a group such that the quotient group $G/\Phi(G)$ is isomorphic to $V \rtimes_{\phi} H$ then

1. $G$ has a unique Sylow $p$-subgroup $P$, 
2. $G$ is isomorphic to $P \rtimes Q$ for any Sylow $q$-subgroup $Q$ and all Sylow $q$-subgroups of $G$ are cyclic,
Some Results

Theorem

If $G$ is isomorphic to $V \rtimes_{\phi} H$ then $G$ has property $B$ with $d(G)$ being $k + 1$ where $V$ is the sum of $k$ of irreducible $\mathbb{F}_p H$-modules and $\Phi(G)$ is trivial.

Generalizing ideas from Scapellato and Verardi (1991) we were able to obtain the following

Theorem

If $G$ is a group such that the quotient group $G/\Phi(G)$ is isomorphic to $V \rtimes_{\phi} H$ then

1. $G$ has a unique Sylow $p$-subgroup $P$,
2. $G$ is isomorphic to $P \rtimes Q$ for any Sylow $q$-subgroup $Q$ and all Sylow $q$-subgroups of $G$ are cyclic,
3. $\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$ where $\langle x^{q^m} \rangle$ is the subgroup of index $q^m$ in $Q = \langle x \rangle$. 
Future Work

We are currently working towards proving the following

Conjecture
If $G$ is a group with trivial Frattini subgroup and has property $B$
then
either,
$G$ is a $p$-group or,
$G$ is a group of the form $V \rtimes \phi H$.
Computational results lead us to believe this to be true. In fact using GAP for groups of order up to 500 we have found this conjecture to hold. We have made some progress on the proof but as of yet it is not complete.
We are currently working towards proving the following

**Conjecture**

If $G$ is a group with trivial Frattini subgroup and has property $\mathcal{B}$ then either,
- $G$ is a $p$-group or,
- $G$ is a group of the form $V \rtimes \phi H$. 
We are currently working towards proving the following

Conjecture

If $G$ is a group with trivial Frattini subgroup and has property $B$ then either,

- $G$ is a $p$-group or,
- $G$ is a group of the form $V times \phi H$.

Computational results lead us to believe this to be true. In fact using GAP for groups of order up to 500 we have found this conjecture to hold. We have made some progress on the proof but as of yet it is not complete.