

# Separation defects, bases and the “single-orbit” conjecture

Robert Bailey  
*Carleton University*

Groups, Combinatorics and Computation 2009

Do I really need to say this?

Do I really need to say this?

Throughout this talk,  $G$  is a group acting on a set,  $\Omega$ .

# Separating subsets

- ▶ **Definition (Praeger):** Let  $\Gamma$  and  $\Delta$  be subsets of  $\Omega$ , such that  $|\Gamma^g \cap \Delta|$  is finite for some  $g \in G$ .  
The **separation defect** of  $\Gamma$  and  $\Delta$  (w.r.t.  $G$ ) is

$$\text{sepdef}(\Gamma, \Delta) := \min_{g \in G} |\Gamma^g \cap \Delta|.$$

# Separating subsets

- ▶ **Definition (Praeger):** Let  $\Gamma$  and  $\Delta$  be subsets of  $\Omega$ , such that  $|\Gamma^g \cap \Delta|$  is finite for some  $g \in G$ .  
The **separation defect** of  $\Gamma$  and  $\Delta$  (w.r.t.  $G$ ) is

$$\text{sepdef}(\Gamma, \Delta) := \min_{g \in G} |\Gamma^g \cap \Delta|.$$

- ▶ If  $\text{sepdef}(\Gamma, \Delta) = 0$ , then we call the pair  $(\Gamma, \Delta)$  **separable**.

## Two theorems

- ▶ **Theorem (Birch, Burns, Macdonald, Neumann, 1976):**  
Let  $\Gamma, \Delta \subseteq \Omega$ , and suppose that every orbit of  $G$  has size strictly larger than  $|\Gamma| \cdot |\Delta|$ . Then  $(\Gamma, \Delta)$  is separable.

## Two theorems

- ▶ **Theorem (Birch, Burns, Macdonald, Neumann, 1976):**  
Let  $\Gamma, \Delta \subseteq \Omega$ , and suppose that every orbit of  $G$  has size strictly larger than  $|\Gamma| \cdot |\Delta|$ . Then  $(\Gamma, \Delta)$  is separable.
- ▶ **Theorem (Praeger, c. 1996):**  
Suppose  $\text{sepdef}(\Gamma, \Delta) = m > 0$ . Then  $G$  has an orbit of size at most  $\frac{|\Gamma| \cdot |\Delta|}{m}$ .

## A new definition

- ▶ What I'm interested in is keeping a given subset fixed, and “separating” it from *all* subsets of a given size.

## A new definition

- ▶ What I'm interested in is keeping a given subset fixed, and “separating” it from *all* subsets of a given size.
- ▶ **Definition:** Suppose  $\Gamma \subseteq \Omega$ . Then the  $k$ -**separation defect** is

$$k\text{-sepdef}(\Gamma) := \max_{K \in \binom{\Omega}{k}} \text{sepdef}(\Gamma, K).$$

## A new definition

- ▶ What I'm interested in is keeping a given subset fixed, and “separating” it from *all* subsets of a given size.
- ▶ **Definition:** Suppose  $\Gamma \subseteq \Omega$ . Then the  $k$ -**separation defect** is

$$k\text{-sepdef}(\Gamma) := \max_{K \in \binom{\Omega}{k}} \text{sepdef}(\Gamma, K).$$

- ▶  $\Gamma$  is  $k$ -**separable** if  $k\text{-sepdef}(\Gamma) = 0$ .

## A new definition

- ▶ What I'm interested in is keeping a given subset fixed, and “separating” it from *all* subsets of a given size.
- ▶ **Definition:** Suppose  $\Gamma \subseteq \Omega$ . Then the  $k$ -**separation defect** is

$$k\text{-sepdef}(\Gamma) := \max_{K \in \binom{\Omega}{k}} \text{sepdef}(\Gamma, K).$$

- ▶  $\Gamma$  is  $k$ -**separable** if  $k\text{-sepdef}(\Gamma) = 0$ .
- ▶ If  $\Gamma$  is  $k$ -separable for all  $k \in \mathbb{N}$ , then it is **highly separable**.

# Bases

- ▶ Suppose  $G$  is now finite.

# Bases

- ▶ Suppose  $G$  is now finite.
- ▶ A **base** for  $G$  is a sequence of points  $B = (x_1, \dots, x_b)$  from  $\Omega$  whose pointwise stabiliser in  $G$  is trivial.

# Bases

- ▶ Suppose  $G$  is now finite.
- ▶ A **base** for  $G$  is a sequence of points  $B = (x_1, \dots, x_b)$  from  $\Omega$  whose pointwise stabiliser in  $G$  is trivial.
- ▶  $B$  is **irredundant** if  $x_i$  is not fixed by the stabiliser of  $(x_1, \dots, x_{i-1})$ .

# Bases

- ▶ Suppose  $G$  is now finite.
- ▶ A **base** for  $G$  is a sequence of points  $B = (x_1, \dots, x_b)$  from  $\Omega$  whose pointwise stabiliser in  $G$  is trivial.
- ▶  $B$  is **irredundant** if  $x_i$  is not fixed by the stabiliser of  $(x_1, \dots, x_{i-1})$ .
- ▶ Example: a basis for  $\mathbb{F}_q^n$  is an irredundant base for  $GL(n, q)$  acting on the non-zero vectors.

# Uncoverings-by-bases (UBBs)

- ▶ Let  $r$  be a suitably-chosen integer.

# Uncoverings-by-bases (UBBs)

- ▶ Let  $r$  be a suitably-chosen integer.
- ▶ **Definition:** An **uncovering-by-bases** for  $G$  is a collection  $\mathcal{U}$  of bases for  $G$  such that any  $r$ -subset of  $\Omega$  is disjoint from at least one member of  $\mathcal{U}$ .

# Uncoverings-by-bases (UBBs)

- ▶ Let  $r$  be a suitably-chosen integer.
- ▶ **Definition:** An **uncovering-by-bases** for  $G$  is a collection  $\mathcal{U}$  of bases for  $G$  such that any  $r$ -subset of  $\Omega$  is disjoint from at least one member of  $\mathcal{U}$ .
- ▶ These were introduced in the context of decoding permutation codes, when we take  $r = \left\lfloor \frac{d-1}{2} \right\rfloor$  (where  $d$  is the *minimum degree* of  $G$ .)

## Example

- ▶ Consider the Mathieu group  $M_{12}$  acting on  $\{1, \dots, 12\}$ .

## Example

- ▶ Consider the Mathieu group  $M_{12}$  acting on  $\{1, \dots, 12\}$ .
- ▶ This is *sharply 5-transitive*, so any 5-tuple is an irredundant base.

## Example

- ▶ Consider the Mathieu group  $M_{12}$  acting on  $\{1, \dots, 12\}$ .
- ▶ This is *sharply 5-transitive*, so any 5-tuple is an irredundant base.
- ▶ The following is a UBB for  $M_{12}$ , for  $r = 3, \dots$

## Example, continued

1	2	3	4	5
1	2	6	11	12
1	3	7	8	9
1	4	6	7	10
1	5	8	9	11
2	4	8	9	12
2	5	7	10	11
3	4	7	11	12
3	5	6	10	12
3	6	8	9	11
6	7	8	9	10

# The “single-orbit” conjecture

- ▶ **Conjecture (B, c. 2010):** For any finite permutation group  $G$ , there exists a UBB for  $G$  which is contained in a single orbit on irredundant bases, for  $r$  as given above.

# The “single-orbit” conjecture

- ▶ **Conjecture (B, c. 2010):** For any finite permutation group  $G$ , there exists a UBB for  $G$  which is contained in a single orbit on irredundant bases, for  $r$  as given above.
- ▶ We say  $G$  has the *single-orbit property* if it satisfies the conjecture.

# The “single-orbit” conjecture

- ▶ **Conjecture (B, c. 2010):** For any finite permutation group  $G$ , there exists a UBB for  $G$  which is contained in a single orbit on irredundant bases, for  $r$  as given above.
- ▶ We say  $G$  has the *single-orbit property* if it satisfies the conjecture.
- ▶ This is known to be true for various interesting cases, such as  $S_m$  acting on 2-subsets, and there is assorted other evidence.

## Another theorem

- ▶ **Theorem (B/Cameron, 2008):** The single-orbit conjecture is true for  $k$ -transitive groups with a base of size  $k + 1$ .

## Another theorem

- ▶ **Theorem (B/Cameron, 2008):** The single-orbit conjecture is true for  $k$ -transitive groups with a base of size  $k + 1$ .
- ▶ **Proof:** For  $k = 1$ , we use the Birch *et al* “separation” theorem directly.

## Another theorem

- ▶ **Theorem (B/Cameron, 2008):** The single-orbit conjecture is true for  $k$ -transitive groups with a base of size  $k + 1$ .
- ▶ **Proof:** For  $k = 1$ , we use the Birch *et al* “separation” theorem directly.  
For  $k \geq 2$ , we use induction on  $k$ .

## Restating the conjecture

- ▶ The following allows us to restate the conjecture:

## Restating the conjecture

- ▶ The following allows us to restate the conjecture:
- ▶ **Proposition** TFAE:

# Restating the conjecture

- ▶ The following allows us to restate the conjecture:
- ▶ **Proposition** TFAE:
  - (i)  $G$  has the single-orbit property;

# Restating the conjecture

- ▶ The following allows us to restate the conjecture:
- ▶ **Proposition** TFAE:
  - (i)  $G$  has the single-orbit property;
  - (ii)  $G$  has an irredundant base  $B$  which is  $r$ -separable.

## Restating the conjecture

- ▶ The following allows us to restate the conjecture:
- ▶ **Proposition** TFAE:
  - (i)  $G$  has the single-orbit property;
  - (ii)  $G$  has an irredundant base  $B$  which is  $r$ -separable.
- ▶ **Proof:** [(i) $\Rightarrow$ (ii)] Pick a base  $B \in \mathcal{U}$ .  
Since  $\mathcal{U}$  is a UBB, there is a base  $B' \in \mathcal{U}$  disjoint from any  $r$ -subset  $R$ .

## Restating the conjecture

▶ The following allows us to restate the conjecture:

▶ **Proposition** TFAE:

- (i)  $G$  has the single-orbit property;
- (ii)  $G$  has an irredundant base  $B$  which is  $r$ -separable.

▶ **Proof:** [(i) $\Rightarrow$ (ii)] Pick a base  $B \in \mathcal{U}$ .

Since  $\mathcal{U}$  is a UBB, there is a base  $B' \in \mathcal{U}$  disjoint from any  $r$ -subset  $R$ .

By the single-orbit property,  $B' = B^g$  for some  $g \in G$ .

Hence  $B$  is  $r$ -separable.

## Restating the conjecture

▶ The following allows us to restate the conjecture:

▶ **Proposition** TFAE:

- (i)  $G$  has the single-orbit property;
- (ii)  $G$  has an irredundant base  $B$  which is  $r$ -separable.

▶ **Proof:** [(i) $\Rightarrow$ (ii)] Pick a base  $B \in \mathcal{U}$ .

Since  $\mathcal{U}$  is a UBB, there is a base  $B' \in \mathcal{U}$  disjoint from any  $r$ -subset  $R$ .

By the single-orbit property,  $B' = B^g$  for some  $g \in G$ .

Hence  $B$  is  $r$ -separable.

[(ii) $\Rightarrow$ (i)] The orbit  $B^G$  is a UBB.

## Pros and cons

- ▶ The good: version (ii) is easier to sell to group theorists.  
(Maybe.)

## Pros and cons

- ▶ The good: version (ii) is easier to sell to group theorists.  
(Maybe.)
- ▶ The bad: so far I haven't been able to do anything with this  
(for finite groups at least).

# Infinite groups

- ▶ For infinite permutation groups, one has to be careful how one defines “base”. It may be finite or infinite.

# Infinite groups

- ▶ For infinite permutation groups, one has to be careful how one defines “base”. It may be finite or infinite.
- ▶ Example:  $G = GL(n, \mathbb{K})$ , for an infinite field  $\mathbb{K}$ , has a finite base.

# Infinite groups

- ▶ For infinite permutation groups, one has to be careful how one defines “base”. It may be finite or infinite.
- ▶ Example:  $G = GL(n, \mathbb{K})$ , for an infinite field  $\mathbb{K}$ , has a finite base.
- ▶ **Proposition:** If  $G$  is infinite, all its orbits are infinite, but has a finite base  $B$ , then  $B$  is highly separable.

# Infinite groups

- ▶ For infinite permutation groups, one has to be careful how one defines “base”. It may be finite or infinite.
- ▶ Example:  $G = GL(n, \mathbb{K})$ , for an infinite field  $\mathbb{K}$ , has a finite base.
- ▶ **Proposition:** If  $G$  is infinite, all its orbits are infinite, but has a finite base  $B$ , then  $B$  is highly separable.
- ▶ **Proof:** Use Birch *et al* again.

## Infinite groups, II

- ▶ An example of an infinite group with a countable base is  $GL(V)$ , where  $V = \mathbb{K}[x]$ .

## Infinite groups, II

- ▶ An example of an infinite group with a countable base is  $GL(V)$ , where  $V = \mathbb{K}[x]$ .
- ▶ Such a base is  $B = \{1, x, x^2, \dots, x^i, \dots\}$ .

## Infinite groups, II

- ▶ An example of an infinite group with a countable base is  $GL(V)$ , where  $V = \mathbb{K}[x]$ .
- ▶ Such a base is  $B = \{1, x, x^2, \dots, x^i, \dots\}$ .
- ▶ **Proposition:** Suppose  $\mathbb{K}$  is infinite. Then the base  $B$  for  $GL(V)$  is highly separable.

## Infinite groups, II

- ▶ An example of an infinite group with a countable base is  $GL(V)$ , where  $V = \mathbb{K}[x]$ .
- ▶ Such a base is  $B = \{1, x, x^2, \dots, x^i, \dots\}$ .
- ▶ **Proposition:** Suppose  $\mathbb{K}$  is infinite. Then the base  $B$  for  $GL(V)$  is highly separable.
- ▶ **Proof:** Elementary linear algebra, and the pigeonhole principle.

## Some questions

- ▶ Given a finite group  $G$  (or infinite family of such), for which  $k$  is a base  $k$ -separable?

## Some questions

- ▶ Given a finite group  $G$  (or infinite family of such), for which  $k$  is a base  $k$ -separable?
- ▶ What can we say about a group with a given  $k$ -separation defect?

## Some questions

- ▶ Given a finite group  $G$  (or infinite family of such), for which  $k$  is a base  $k$ -separable?
- ▶ What can we say about a group with a given  $k$ -separation defect?
- ▶ Separating infinite subsets: for a given infinite permutation group  $G$ , when is a subset  $\Gamma$  “ $\aleph_0$ -separable”?

## Some questions

- ▶ Given a finite group  $G$  (or infinite family of such), for which  $k$  is a base  $k$ -separable?
- ▶ What can we say about a group with a given  $k$ -separation defect?
- ▶ Separating infinite subsets: for a given infinite permutation group  $G$ , when is a subset  $\Gamma$  “ $\aleph_0$ -separable”?
- ▶ Solve the original “single-orbit” conjecture.....

THE END