The base size of the symmetric group

Coen del Valle
Joint work with Colva Roney-Dougal

22 May 2024

University of St Andrews

G-congruences

Let G be a group acting faithfully on a set Ω.

G-congruences

Let G be a group acting faithfully on a set Ω. An equivalence relation, $\sim$, is called a *G-congruence* if for every $g \in G$ and every $\alpha, \beta \in \Omega$,

University of St Andrews

G-congruences

Let G be a group acting faithfully on a set Ω. An equivalence relation, $\sim$, is called a *G-congruence* if for every $g \in G$ and every $\alpha, \beta \in \Omega$,

$$\alpha^g \sim \beta^g \Leftrightarrow \alpha \sim \beta.$$

G-congruences

Let G be a group acting faithfully on a set Ω. An equivalence relation, $\sim$, is called a *G-congruence* if for every $g \in G$ and every $\alpha, \beta \in \Omega$,

$$\alpha^g \sim \beta^g \Leftrightarrow \alpha \sim \beta.$$

We call (the action of) G *primitive* if

G-congruences

Let G be a group acting faithfully on a set Ω. An equivalence relation, $\sim$, is called a *G-congruence* if for every $g \in G$ and every $\alpha, \beta \in \Omega$,

$$\alpha^g \sim \beta^g \Leftrightarrow \alpha \sim \beta.$$

We call (the action of) G *primitive* if

- G is transitive; and

University of St Andrews

G-congruences

Let G be a group acting faithfully on a set Ω. An equivalence relation, $\sim$, is called a *G-congruence* if for every $g \in G$ and every $\alpha, \beta \in \Omega$,

$$\alpha^g \sim \beta^g \Leftrightarrow \alpha \sim \beta.$$

We call (the action of) G *primitive* if

- G is transitive; and
- G admits no nontrivial G-congruences.

University of St Andrews

Examples

- The symmetric group S_n acting on $[n] := \{1, 2, \ldots, n\}$.

University of St Andrews

Examples

- The symmetric group S_n acting on $[n] := \{1, 2, \ldots, n\}$.
- Any k-transitive group, $k \geq 2$.

University of St Andrews

Examples

- The symmetric group S_n acting on $[n] := \{1, 2, \ldots, n\}$.
- Any k-transitive group, $k \geq 2$.
- The symmetric group S_n acting on the set of r-subsets of $[n]$, $n > 2r$.

Examples

- The symmetric group S_n acting on $[n] := \{1, 2, \ldots, n\}$.
- Any k-transitive group, $k \geq 2$.
- The symmetric group S_n acting on the set of r-subsets of $[n]$, $n > 2r$.
- The projective general linear group $\mathrm{PGL}_d(q)$ acting on m-dimensional subspaces of $\mathrm{GF}(q)^d$, $d > 2m$.

University of St Andrews

The O'Nan-Scott theorem

The O'Nan-Scott theorem classifies all primitive permutation groups; we summarise a condensed version for the actions of S_n and A_n.

University of St Andrews

The O'Nan-Scott theorem

The O'Nan-Scott theorem classifies all primitive permutation groups; we summarise a condensed version for the actions of S_n and A_n.

Theorem: Up to equivalence, the primitive actions of $G \in \{\mathrm{S}_n, \mathrm{A}_n\}$ are the actions on:

(i) r-subsets of $[n]$, $n > 2r$;

University of St Andrews

The O'Nan-Scott theorem

The O'Nan-Scott theorem classifies all primitive permutation groups; we summarise a condensed version for the actions of S_n and A_n.

Theorem: Up to equivalence, the primitive actions of $G \in \{\mathrm{S}_n, \mathrm{A}_n\}$ are the actions on:

(i) r-subsets of $[n]$, $n > 2r$;

(ii) partitions of $[n]$ into k parts each of size l ($n = kl$);

University of St Andrews

The O'Nan-Scott theorem

The O'Nan-Scott theorem classifies all primitive permutation groups; we summarise a condensed version for the actions of S_n and A_n.

Theorem: Up to equivalence, the primitive actions of $G \in \{\mathrm{S}_n, \mathrm{A}_n\}$ are the actions on:

(i) r-subsets of $[n]$, $n > 2r$;

(ii) partitions of $[n]$ into k parts each of size l ($n = kl$);

(iii) subspaces of a vector space (when G is isomorphic to an almost simple classical group); and

University of
St Andrews

The O'Nan-Scott theorem

The O'Nan-Scott theorem classifies all primitive permutation groups; we summarise a condensed version for the actions of S_n and A_n.

Theorem: Up to equivalence, the primitive actions of $G \in \{\mathrm{S}_n, \mathrm{A}_n\}$ are the actions on:

(i) r-subsets of $[n]$, $n > 2r$;

(ii) partitions of $[n]$ into k parts each of size l ($n = kl$);

(iii) subspaces of a vector space (when G is isomorphic to an almost simple classical group); and

(iv) something else (known precisely).

University of St Andrews

The O'Nan-Scott theorem

The O'Nan-Scott theorem classifies all primitive permutation groups; we summarise a condensed version for the actions of S_n and A_n.

Theorem: Up to equivalence, the primitive actions of $G \in \{\mathrm{S}_n, \mathrm{A}_n\}$ are the actions on:

(i) r-subsets of $[n]$, $n > 2r$;

(ii) partitions of $[n]$ into k parts each of size l ($n = kl$);

(iii) subspaces of a vector space (when G is isomorphic to an almost simple classical group); and

(iv) something else (known precisely).

(i)–(iii) are called *standard* actions, and (iv) *non-standard*.

University of St Andrews

A computational problem

Let G be a permutation group acting faithfully on an n-set Ω.

A computational problem

Let G be a permutation group acting faithfully on an n-set Ω.

Problem: How can we store each permutation $g \in G$?

University of St Andrews

A computational problem

Let G be a permutation group acting faithfully on an n-set Ω.

Problem: How can we store each permutation $g \in G$?

Naïve approach: Store g as the n-tuple $(\alpha^g : \alpha \in \Omega)$.

University of St Andrews

A computational problem

Let G be a permutation group acting faithfully on an n-set Ω.

Problem: How can we store each permutation $g \in G$?

Naïve approach: Store g as the n-tuple $(\alpha^g : \alpha \in \Omega)$.

As the degree gets large, so does the length of these tuples (linearly), but much of their information is redundant.

University of St Andrews

Bases

We call a subset $\mathcal{B} = \{\beta_i : 1 \leq i \leq k\} \subseteq \Omega$, a *base* if

Bases

We call a subset $\mathcal{B} = \{\beta_i : 1 \leq i \leq k\} \subseteq \Omega$, a *base* if

$$G_{(\mathcal{B})} := \{g \in G : \beta_i^g = \beta_i, 1 \leq i \leq k\} = 1.$$

University of
St Andrews

Bases

We call a subset $\mathcal{B} = \{\beta_i : 1 \leq i \leq k\} \subseteq \Omega$, a *base* if

$$G_{(\mathcal{B})} := \{g \in G : \beta_i^g = \beta_i, 1 \leq i \leq k\} = 1.$$

If permutations g and h agree on $\mathcal{B}$, then $gh^{-1} \in G_{(\mathcal{B})} = 1$, so $g = h$. That is, each permutation is uniquely determined by $(\beta_i^g)_{i \leq k}$.

Bases

We call a subset $\mathcal{B} = \{\beta_i : 1 \leq i \leq k\} \subseteq \Omega$, a *base* if

$$G_{(\mathcal{B})} := \{g \in G : \beta_i^g = \beta_i, 1 \leq i \leq k\} = 1.$$

If permutations g and h agree on $\mathcal{B}$, then $gh^{-1} \in G_{(\mathcal{B})} = 1$, so $g = h$. That is, each permutation is uniquely determined by $(\beta_i^g)_{i \leq k}$.

We can store g as a tuple of (probably) much shorter length; call the minimum size of a base for G the *base size* of G, denoted $b(G)$.

University of St Andrews

Examples and bounds

- Any $(n-1)$ set is a base for S_n acting on $[n]$, but any set of size less than $n-1$ has a stabiliser containing a transposition hence cannot be a base. Thus $b(G) = n-1$.

University of St Andrews

Examples and bounds

- Any $(n-1)$ set is a base for S_n acting on $[n]$, but any set of size less than $n-1$ has a stabiliser containing a transposition hence cannot be a base. Thus $b(G) = n-1$.
- Let $e_1, e_2, \ldots, e_d$ be a basis for $GF(q)^d$. Then $\{\langle e_1\rangle, \langle e_2\rangle, \ldots, \langle e_d\rangle, \langle e_1 + e_2 + \cdots + e_d\rangle\}$ is a base of size $d+1$ for $\mathrm{PGL}_d(q)$ acting on 1-spaces.

University of St Andrews

Examples and bounds

- Any $(n-1)$ set is a base for S_n acting on $[n]$, but any set of size less than $n-1$ has a stabiliser containing a transposition hence cannot be a base. Thus $b(G) = n-1$.
- Let $e_1, e_2, \ldots, e_d$ be a basis for $GF(q)^d$. Then $\{\langle e_1\rangle, \langle e_2\rangle, \ldots, \langle e_d\rangle, \langle e_1 + e_2 + \cdots + e_d\rangle\}$ is a base of size $d+1$ for $\mathrm{PGL}_d(q)$ acting on 1-spaces.
- For any permutation group G of degree n, $(\log|G|)/(\log n) \leq b(G) \leq \log|G|$.

University of St Andrews

Base size of S_n and A_n

Theorem: (Burness+Guralnick+Saxl, 2011) All non-standard actions of S_n and A_n have base size 2 or 3, and actions of type (iii) (there are finitely many of these) have base size at most 5.

University of St Andrews

Base size of S_n and A_n

Theorem: (Burness+Guralnick+Saxl, 2011) All non-standard actions of S_n and A_n have base size 2 or 3, and actions of type (iii) (there are finitely many of these) have base size at most 5.

Theorem: (Morris+Spiga, 2021) Let $k \geq 2$, $l \geq 2$ and let $\mathrm{S}_{k \times l}$ denote S_{kl} acting on partitions of $[kl]$ into k parts of size l then

University of St Andrews

Base size of S_n and A_n

Theorem: (Burness+Guralnick+Saxl, 2011) All non-standard actions of S_n and A_n have base size 2 or 3, and actions of type (iii) (there are finitely many of these) have base size at most 5.

Theorem: (Morris+Spiga, 2021) Let $k \geq 2$, $l \geq 2$ and let $\mathrm{S}_{k\times l}$ denote S_{kl} acting on partitions of $[kl]$ into k parts of size l then

1. $b(\mathrm{S}_{2\times 2})$ is undefined, $b(\mathrm{S}_{3\times 2}) = 4$ and $b(\mathrm{S}_{k\times 2}) = 3$ for $k \geq 4$;
2. $b(\mathrm{S}_{2\times 4}) = 5$, $b(\mathrm{S}_{2\times l}) = \lceil \log_2(l+3)\rceil + 1$ for $l \notin \{2,4\}$;
3. $b(\mathrm{S}_{6\times 3}) = b(\mathrm{S}_{7\times 3}) = b(\mathrm{S}_{7\times 4}) = 3$, $b(\mathrm{S}_{3\times 7}) = 4$, and $b(\mathrm{S}_{(l+2)\times l}) = 3$ for $l \geq 3$; and
4. $b(\mathrm{S}_{k\times l}) = \lceil \log_k(l+2)\rceil + 1$ otherwise.

University of St Andrews

Base size of S_n and A_n

Theorem: (Burness+Guralnick+Saxl, 2011) All non-standard actions of S_n and A_n have base size 2 or 3, and actions of type (iii) (there are finitely many of these) have base size at most 5.

Theorem: (Morris+Spiga, 2021) Let $k \geq 2$, $l \geq 2$ and let $\mathrm{S}_{k \times l}$ denote S_{kl} acting on partitions of $[kl]$ into k parts of size l then

1. $b(\mathrm{S}_{2\times 2})$ is undefined, $b(\mathrm{S}_{3\times 2}) = 4$ and $b(\mathrm{S}_{k\times 2}) = 3$ for $k \geq 4$;
2. $b(\mathrm{S}_{2\times 4}) = 5$, $b(\mathrm{S}_{2\times l}) = \lceil \log_2(l+3) \rceil + 1$ for $l \notin \{2, 4\}$;
3. $b(\mathrm{S}_{6\times 3}) = b(\mathrm{S}_{7\times 3}) = b(\mathrm{S}_{7\times 4}) = 3$, $b(\mathrm{S}_{3\times 7}) = 4$, and $b(\mathrm{S}_{(l+2)\times l}) = 3$ for $l \geq 3$; and
4. $b(\mathrm{S}_{k\times l}) = \lceil \log_k(l+2) \rceil + 1$ otherwise.

They show a similar result for A_n — remains to consider r-subsets.

University of St Andrews

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$.

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$. We will be discussing the base size problem for G, which is equivalent to a purely graph-theoretic problem:

University of St Andrews

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$. We will be discussing the base size problem for G, which is equivalent to a purely graph-theoretic problem:

The *determining number* $\mathrm{Det}(\Gamma)$, of a graph $\Gamma = (V, E)$ is the minimum cardinality of a set $S \subseteq V$ such that $\mathrm{Aut}(\Gamma)_{(S)} = 1$.

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$. We will be discussing the base size problem for G, which is equivalent to a purely graph-theoretic problem:

The *determining number* $\mathrm{Det}(\Gamma)$, of a graph $\Gamma = (V, E)$ is the minimum cardinality of a set $S \subseteq V$ such that $\mathrm{Aut}(\Gamma)_{(S)} = 1$. Given positive integers $n \geq 2r$, the *Kneser graph*, $K_{n:r}$, has vertex set $V = \{A \subseteq [n] : |A| = r\}$, where sets are adjacent if and only if they are disjoint.

University of St Andrews

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$. We will be discussing the base size problem for G, which is equivalent to a purely graph-theoretic problem:

The *determining number* $\mathrm{Det}(\Gamma)$, of a graph $\Gamma = (V, E)$ is the minimum cardinality of a set $S \subseteq V$ such that $\mathrm{Aut}(\Gamma)_{(S)} = 1$. Given positive integers $n \geq 2r$, the *Kneser graph*, $K_{n:r}$, has vertex set $V = \{A \subseteq [n] : |A| = r\}$, where sets are adjacent if and only if they are disjoint. Hence, $\mathrm{Det}(K_{n:r}) = b(\mathrm{S}_{n,r})$.

University of St Andrews

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$. We will be discussing the base size problem for G, which is equivalent to a purely graph-theoretic problem:

The *determining number* $\mathrm{Det}(\Gamma)$, of a graph $\Gamma = (V, E)$ is the minimum cardinality of a set $S \subseteq V$ such that $\mathrm{Aut}(\Gamma)_{(S)} = 1$. Given positive integers $n \geq 2r$, the *Kneser graph*, $K_{n:r}$, has vertex set $V = \{A \subseteq [n] : |A| = r\}$, where sets are adjacent if and only if they are disjoint. Hence, $\mathrm{Det}(K_{n:r}) = b(\mathrm{S}_{n,r})$.

Theorem: (Halasi, 2012) If $n \geq (r^2 + r)/2$, then $b(G) = \left\lceil \frac{2n-2}{r+1} \right\rceil$.

University of St Andrews

r-sets and the determining number

Denote by $\mathrm{S}_{n,r}$, and $\mathrm{A}_{n,r}$ the symmetric and alternating groups S_n and A_n acting on r-subsets of $[n]$. We will be discussing the base size problem for G, which is equivalent to a purely graph-theoretic problem:

The *determining number* $\mathrm{Det}(\Gamma)$, of a graph $\Gamma = (V, E)$ is the minimum cardinality of a set $S \subseteq V$ such that $\mathrm{Aut}(\Gamma)_{(S)} = 1$. Given positive integers $n \geq 2r$, the *Kneser graph*, $K_{n:r}$, has vertex set $V = \{A \subseteq [n] : |A| = r\}$, where sets are adjacent if and only if they are disjoint. Hence, $\mathrm{Det}(K_{n:r}) = b(\mathrm{S}_{n,r})$.

Theorem: (Halasi, 2012) If $n \geq (r^2 + r)/2$, then $b(G) = \left\lceil \frac{2n-2}{r+1} \right\rceil$.

University of St Andrews

Main result

Given $l, k, r \in \mathbb{N}$ set $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

University of St Andrews

Main result

Given $l, k, r \in \mathbb{N}$ set $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Theorem: (dV+Roney-Dougal, 2023) Let $n \geq 2r$ be fixed and let l be minimal such that there exists some $k \leq l+1$ satisfying $0 \leq m_r(l,k) \leq \binom{l}{k}$ and $\sum_{i=0}^{k-1}\binom{l}{i} + m_r(l,k) \geq n$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{A}_{n+1,r}) = l$.

University of St Andrews

Main result

Given $l, k, r \in \mathbb{N}$ set $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Theorem: (dV+Roney-Dougal, 2023) Let $n \geq 2r$ be fixed and let l be minimal such that there exists some $k \leq l+1$ satisfying $0 \leq m_r(l,k) \leq \binom{l}{k}$ and $\sum_{i=0}^{k-1}\binom{l}{i} + m_r(l,k) \geq n$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{A}_{n+1,r}) = l$.

A similar result was obtained independently by Mecenero+Spiga, although it takes a surprisingly different form.

University of St Andrews

Main result

Given $l, k, r \in \mathbb{N}$ set $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Theorem: (dV+Roney-Dougal, 2023) Let $n \geq 2r$ be fixed and let l be minimal such that there exists some $k \leq l+1$ satisfying $0 \leq m_r(l,k) \leq \binom{l}{k}$ and $\sum_{i=0}^{k-1}\binom{l}{i} + m_r(l,k) \geq n$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{A}_{n+1,r}) = l$.

A similar result was obtained independently by Mecenero+Spiga, although it takes a surprisingly different form.

Corollary: Every almost simple primitive permutation group with alternating socle has known base size.

University of St Andrews

Consequences of the main result

Corollary: Let n and r be positive integers satisfying $\frac{r^2+r}{2} > n \geq r^{3/2} + \frac{r}{2} + 1$. Then

$$b(\mathrm{S}_{n,r}) = \left\lceil \left(3\left(2n + r - \frac{5}{4}\right) + r^2\right)^{\frac{1}{2}} - r - \frac{3}{2} \right\rceil .$$

University of St Andrews

Consequences of the main result

Corollary: Let n and r be positive integers satisfying $\frac{r^2+r}{2} > n \geq r^{3/2} + \frac{r}{2} + 1$. Then

$$b(\mathrm{S}_{n,r}) = \left\lceil \left(3\left(2n + r - \frac{5}{4}\right) + r^2\right)^{\frac{1}{2}} - r - \frac{3}{2} \right\rceil .$$

Corollary: Let $s \in (0,1]$. Then $b(\mathrm{S}_{r^{1+s},r}) = \Theta(r^s)$, that is, there exist $c, C > 0$ such that

$$cr^s \leq b(\mathrm{S}_{r^{1+s},r}) \leq Cr^s,$$

for all r.

University of St Andrews

Ingredients of the proof

Let $\mathrm{S}_{n,\leq r}$ denote S_n with its action on all subsets of $[n]$ of size at most r.

University of St Andrews

Ingredients of the proof

Let $\mathrm{S}_{n,\leq r}$ denote S_n with its action on all subsets of $[n]$ of size at most r.

Lemma: (Halasi, 2012) Fix $n \geq 2r$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{S}_{n,\leq r})$.

University of St Andrews

Ingredients of the proof

Let $\mathrm{S}_{n,\leq r}$ denote S_n with its action on all subsets of $[n]$ of size at most r.

Lemma: (Halasi, 2012) Fix $n \geq 2r$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{S}_{n,\leq r})$.

We can view a base for $\mathrm{S}_{n,\leq r}$ as a hypergraph on $[n]$ with hyperedges of size at most r.

Ingredients of the proof

Let $\mathrm{S}_{n,\leq r}$ denote S_n with its action on all subsets of $[n]$ of size at most r.

Lemma: (Halasi, 2012) Fix $n \geq 2r$. Then $b(\mathrm{S}_{n,r}) = b(\mathrm{S}_{n,\leq r})$.

We can view a base for $\mathrm{S}_{n,\leq r}$ as a hypergraph on $[n]$ with hyperedges of size at most r.

With such a framework, the notions of neighbourhoods, and duals become sensible.

University of St Andrews

Neighbourhoods

Given a hypergraph $H = (V, E)$ and $v \in V$, define the *neighbourhood* of v to be the set

$$N_H(v) := \{e \in E(H) : v \in e\}.$$

University of
St Andrews

Neighbourhoods

Given a hypergraph $H = (V, E)$ and $v \in V$, define the *neighbourhood* of v to be the set

$$N_H(v) := \{e \in E(H) : v \in e\}.$$

Lemma: Let n and r be positive integers with $n \geq 2r$, and $\mathcal{B}$ a base for $\mathrm{S}_{n,r}$ with $|\mathcal{B}| = l$. Then $lr = \sum_{x \in [n]} |N_{\mathcal{B}}(x)|$.

University of St Andrews

Neighbourhoods

Given a hypergraph $H = (V, E)$ and $v \in V$, define the *neighbourhood* of v to be the set

$$N_H(v) := \{e \in E(H) : v \in e\}.$$

Lemma: Let n and r be positive integers with $n \geq 2r$, and $\mathcal{B}$ a base for $\mathrm{S}_{n,r}$ with $|\mathcal{B}| = l$. Then $lr = \sum_{x \in [n]} |N_{\mathcal{B}}(x)|$.

Neighbourhoods also give us a nice combinatorial description of a base:

University of
St Andrews

Neighbourhoods

Given a hypergraph $H = (V, E)$ and $v \in V$, define the *neighbourhood* of v to be the set

$$N_H(v) := \{e \in E(H) : v \in e\}.$$

Lemma: Let n and r be positive integers with $n \geq 2r$, and $\mathcal{B}$ a base for $\mathrm{S}_{n,r}$ with $|\mathcal{B}| = l$. Then $lr = \sum_{x \in [n]} |N_{\mathcal{B}}(x)|$.

Neighbourhoods also give us a nice combinatorial description of a base: a collection $\mathcal{B}$ of $(\leq)r$-subsets of $[n]$ is a base for $\mathrm{S}_{n,(\leq)r}$ if and only if no two points share a common neighbourhood.

University of St Andrews

Interpretation of $m_r(l, k)$

Recall $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

University of St Andrews

Interpretation of $m_r(l, k)$

Recall $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Given $\mathcal{B}, k$, set $A_1 := \{x \in [n] : |N_{\mathcal{B}}(x)| < k\}$ and $A_2 := \{x \in [n] : |N_{\mathcal{B}}(x)| \geq k\}$. Then $\sum_{x \in A_2} |N_{\mathcal{B}}(x)| = lr - \left(\sum_{x \in A_1} |N_{\mathcal{B}}(x)|\right)$.

University of St Andrews

Interpretation of $m_r(l, k)$

Recall $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Given $\mathcal{B}, k$, set $A_1 := \{x \in [n] : |N_{\mathcal{B}}(x)| < k\}$ and $A_2 := \{x \in [n] : |N_{\mathcal{B}}(x)| \geq k\}$. Then $\sum_{x\in A_2} |N_{\mathcal{B}}(x)| = lr - \left(\sum_{x\in A_1} |N_{\mathcal{B}}(x)|\right)$. There are at most $\binom{l}{i}$ distinct neighbourhoods of size i, so $lr - \left(\sum_{x\in A_1} |N_{\mathcal{B}}(x)|\right)$ is minimally $lr - \sum_{i=1}^{k-1} i\binom{l}{i} = km_r(l,k)$.

University of St Andrews

Interpretation of $m_r(l, k)$

Recall $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Given $\mathcal{B}, k$, set $A_1 := \{x \in [n] : |N_{\mathcal{B}}(x)| < k\}$ and $A_2 := \{x \in [n] : |N_{\mathcal{B}}(x)| \geq k\}$. Then $\sum_{x \in A_2} |N_{\mathcal{B}}(x)| = lr - \left(\sum_{x \in A_1} |N_{\mathcal{B}}(x)|\right)$. There are at most $\binom{l}{i}$ distinct neighbourhoods of size i, so $lr - \left(\sum_{x \in A_1} |N_{\mathcal{B}}(x)|\right)$ is minimally $lr - \sum_{i=1}^{k-1} i\binom{l}{i} = km_r(l,k)$. On the other hand $k|A_2| \leq \sum_{x \in A_2} |N_{\mathcal{B}}(x)|$.

University of St Andrews

Interpretation of $m_r(l, k)$

Recall $m_r(l,k) := \frac{1}{k}\left(lr - \sum_{i=1}^{k-1} i\binom{l}{i}\right)$.

Given $\mathcal{B}, k$, set $A_1 := \{x \in [n] : |N_{\mathcal{B}}(x)| < k\}$ and $A_2 := \{x \in [n] : |N_{\mathcal{B}}(x)| \geq k\}$. Then $\sum_{x \in A_2} |N_{\mathcal{B}}(x)| = lr - \left(\sum_{x \in A_1} |N_{\mathcal{B}}(x)|\right)$. There are at most $\binom{l}{i}$ distinct neighbourhoods of size i, so $lr - \left(\sum_{x \in A_1} |N_{\mathcal{B}}(x)|\right)$ is minimally $lr - \sum_{i=1}^{k-1} i\binom{l}{i} = km_r(l,k)$. On the other hand $k|A_2| \leq \sum_{x \in A_2} |N_{\mathcal{B}}(x)|$. Thus $m_r(l,k)$ estimates the minimum number of points of $[n]$ which have neighbourhoods of size at least k.

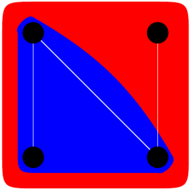
Making a small base

Let H be a hypergraph. The *dual* of H, denoted $H^{\perp}$, is the hypergraph with vertex set identified with the hyperedges of H, and hyperedges identified with vertices of H, where the incidence relations of $H^{\perp}$ are the reverse of those of H.

University of St Andrews

Making a small base

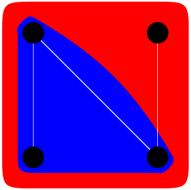
Let H be a hypergraph. The *dual* of H, denoted $H^{\perp}$, is the hypergraph with vertex set identified with the hyperedges of H, and hyperedges identified with vertices of H, where the incidence relations of $H^{\perp}$ are the reverse of those of H.



$$\mapsto \{\{1,2,4,5\},\{3,5\},\{2,3,4,5\},\{1,4,5\}\}$$

Making a small base

Let H be a hypergraph. The *dual* of H, denoted $H^{\perp}$, is the hypergraph with vertex set identified with the hyperedges of H, and hyperedges identified with vertices of H, where the incidence relations of $H^{\perp}$ are the reverse of those of H.

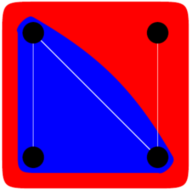


$\mapsto \{\{1,2,4,5\},\{3,5\},\{2,3,4,5\},\{1,4,5\}\}$

Edges become vertices and neighbourhoods become edges.

Making a small base

Let H be a hypergraph. The *dual* of H, denoted $H^{\perp}$, is the hypergraph with vertex set identified with the hyperedges of H, and hyperedges identified with vertices of H, where the incidence relations of $H^{\perp}$ are the reverse of those of H.



$\mapsto \{\{1,2,4,5\},\{3,5\},\{2,3,4,5\},\{1,4,5\}\}$

Edges become vertices and neighbourhoods become edges. Thus to make a small base it suffices to make its dual — a hypergraph with n (distinct) edges and as few vertices as possible so that no vertex is contained in more than r edges.

University of St Andrews

Example

Suppose we wish to construct a minimum base for $\mathrm{S}_{18,7}$.

University of
St Andrews

Example

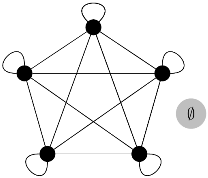
Suppose we wish to construct a minimum base for $\mathrm{S}_{18,7}$.

$(l, k) = (5, 3)$ satisfy the conditions of the theorem with l minimal. Since $k = 3$ we start with K_5 adorned with all loops and the empty edge.

Example

Suppose we wish to construct a minimum base for $\mathrm{S}_{18,7}$.

$(l, k) = (5, 3)$ satisfy the conditions of the theorem with l minimal. Since $k = 3$ we start with K_5 adorned with all loops and the empty edge.

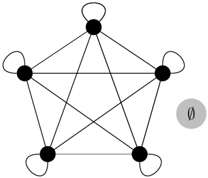


University of
St Andrews

Example

Suppose we wish to construct a minimum base for $\mathrm{S}_{18,7}$.

$(l, k) = (5, 3)$ satisfy the conditions of the theorem with l minimal. Since $k = 3$ we start with K_5 adorned with all loops and the empty edge.



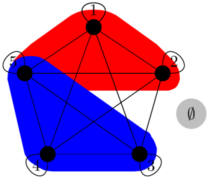
We now add hyperedges of size three until the hypergraph has 18 edges, being careful that no vertex ends up with neighbourhood bigger than 7.

University of St Andrews

Example

Suppose we wish to construct a minimum base for $\mathrm{S}_{18,7}$.

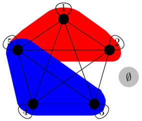
$(l, k) = (5, 3)$ satisfy the conditions of the theorem with l minimal. Since $k = 3$ we start with K_5 adorned with all loops and the empty edge.



We now add hyperedges of size three until the hypergraph has 18 edges, being careful that no vertex ends up with neighbourhood bigger than 7.

University of
St Andrews

Example cont'd

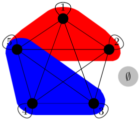


Taking the dual gives

$$\{\{2,7,8,9,10,17\},\{3,7,11,12,13,17\},\{4,8,11,14,15,18\},$$
$$\{5,9,12,14,16,18\},\{6,10,13,15,16,17,18\}\}$$

as a minimum base for $\mathrm{S}_{18,\leq 7}$

Example cont'd



Taking the dual gives

$$\{\{2,7,8,9,10,17\},\{3,7,11,12,13,17\},\{4,8,11,14,15,18\},\\ \{5,9,12,14,16,18\},\{6,10,13,15,16,17,18\}\}$$

as a minimum base for $\mathrm{S}_{18,\leq 7}$

Applying Halasi's algorithm yields

$$\{\{2,7,8,9,10,17,18\},\{3,7,11,12,13,17,18\},\\ \{4,8,11,14,15,17,18\},\{5,7,9,12,14,16,18\},\\ \{6,10,13,15,16,17,18\}\}$$

University of St Andrews

a minimum base for $\mathrm{S}_{18,7}$.

Thanks for listening!

University of
St Andrews