

AustMS ECR Workshop
Adelaide, 29092009

Three combinatorial dual identities and their proximity to something useful

Thomas Britz*

*University of New South Wales
Funded by an ARC Discovery Grant

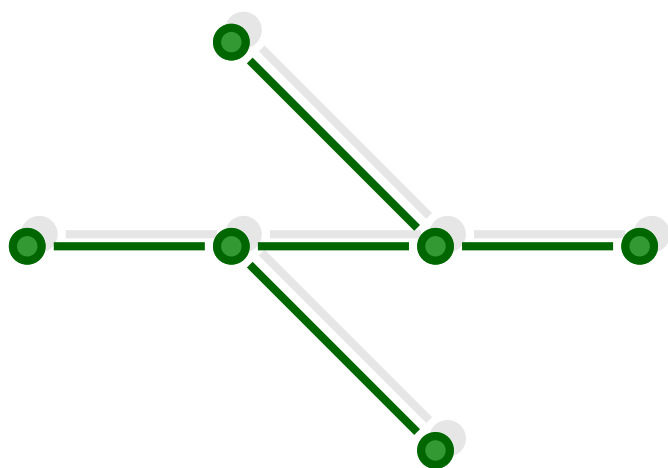


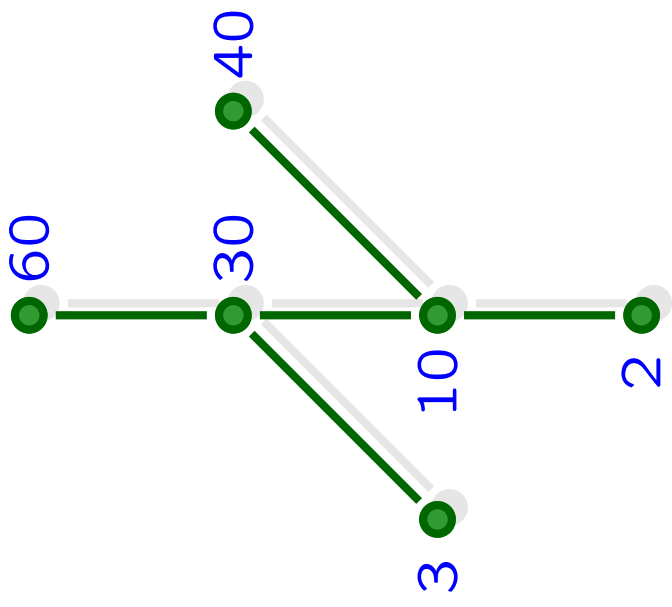
G.H. Hardy
(1877-1947)

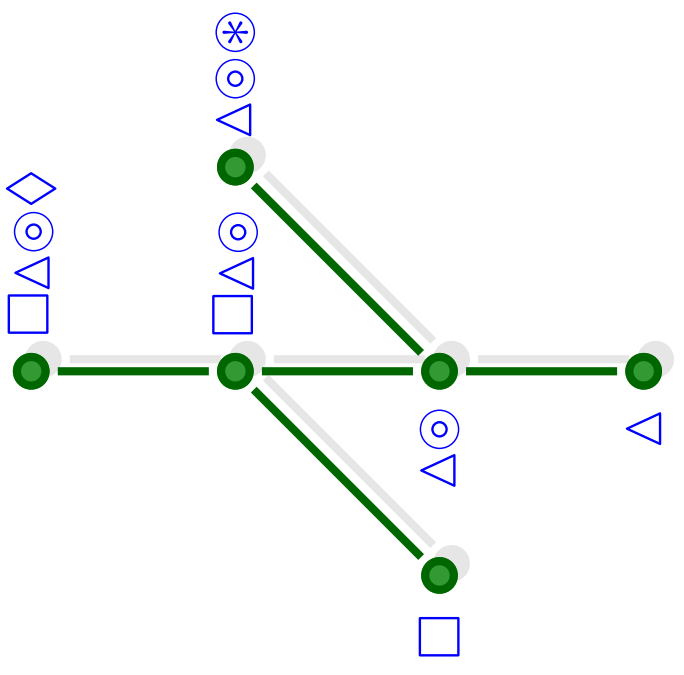
*“I have never done anything ‘useful’.
No discovery of mine has made, or is likely to make,
directly or indirectly, for good or ill,
the least difference to the amenity of the world.”*

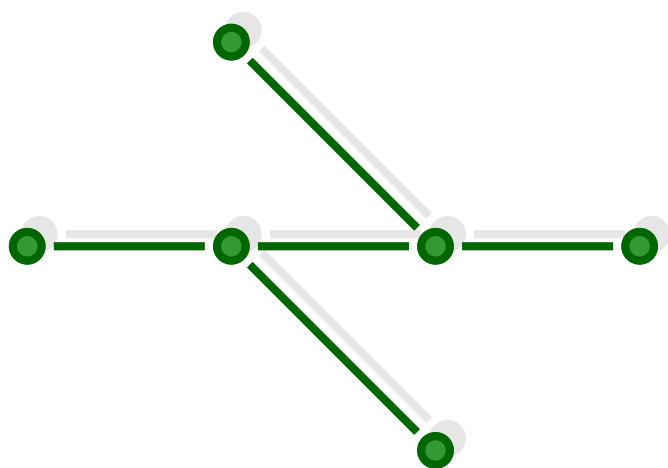
*“Mathematicians may be justified in rejoicing
that there is one science at any rate, and that their own,
whose very remoteness from ordinary human activities
should keep it gentle and clean”*

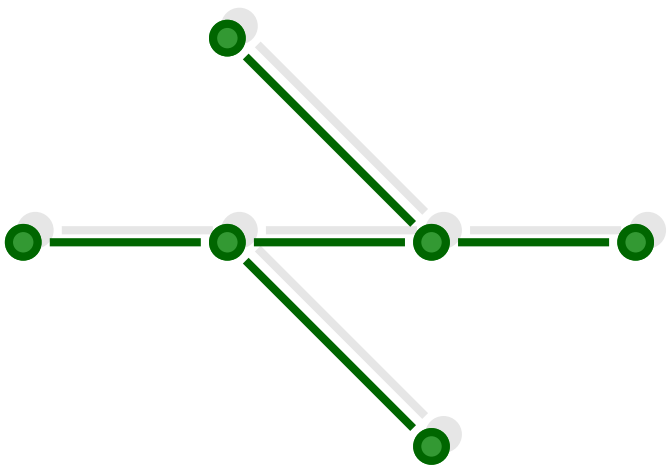
Duality Theorem 1:
Greene's Theorem







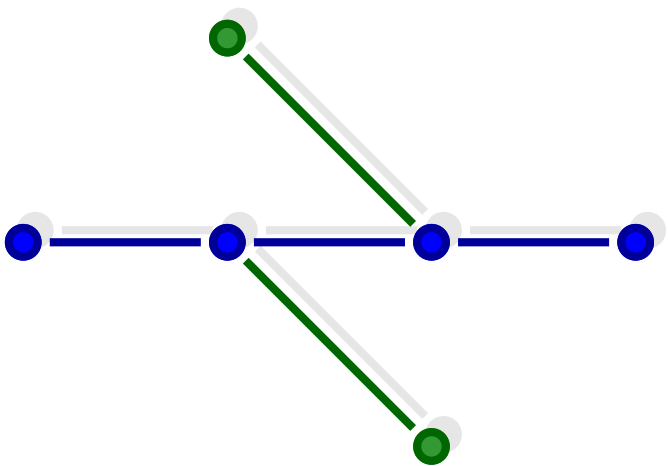




chain



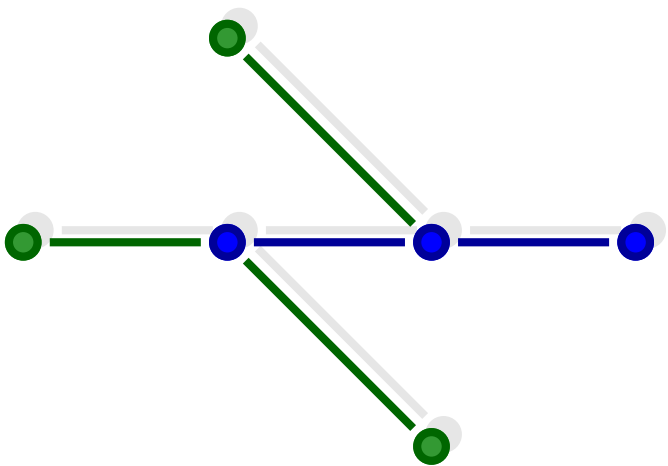
antichain



chain



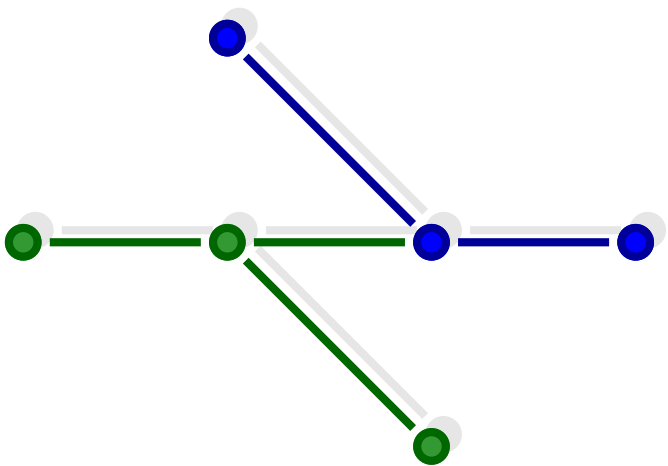
antichain



chain



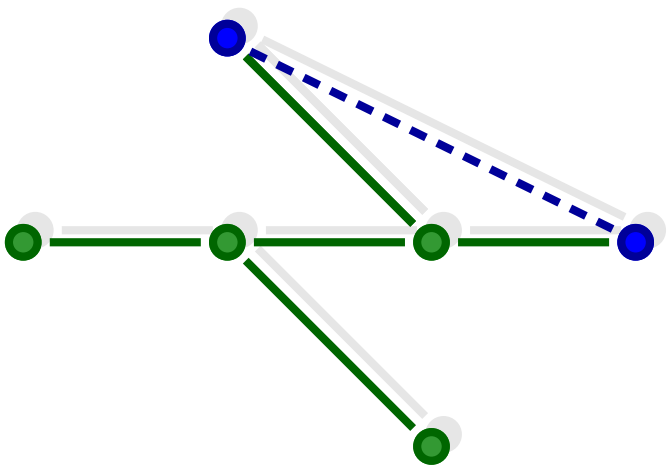
antichain



chain



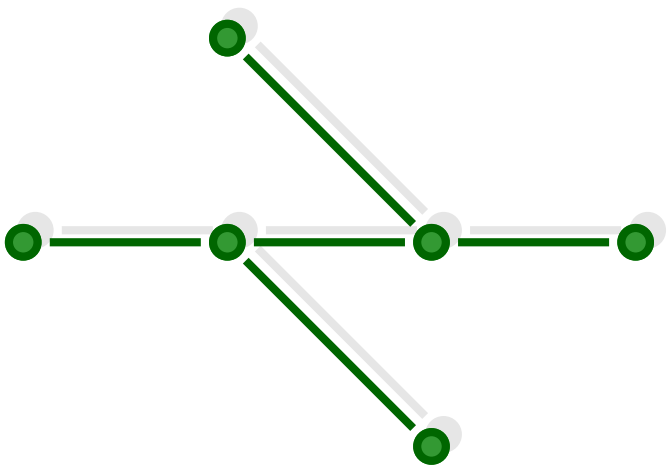
antichain



chain



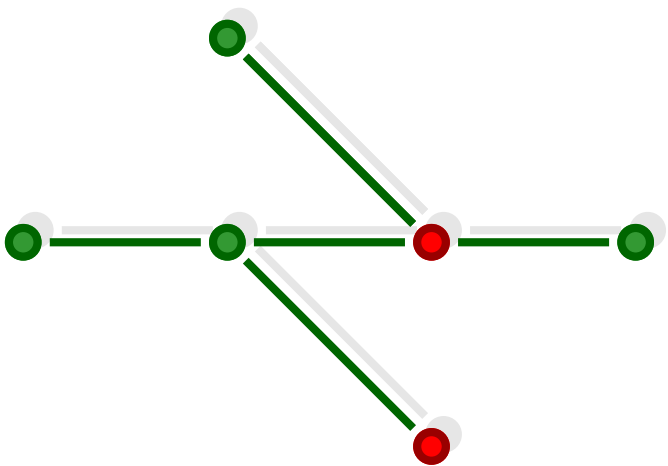
antichain



chain



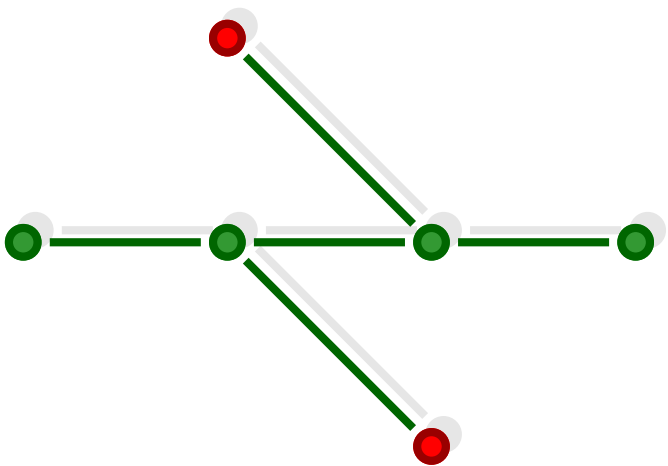
antichain



chain



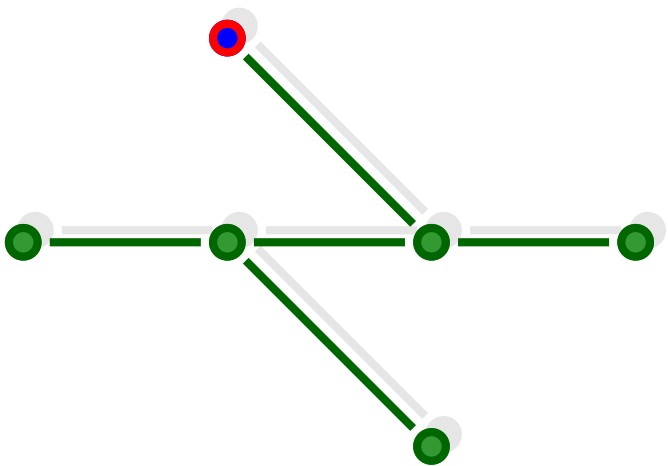
antichain



chain



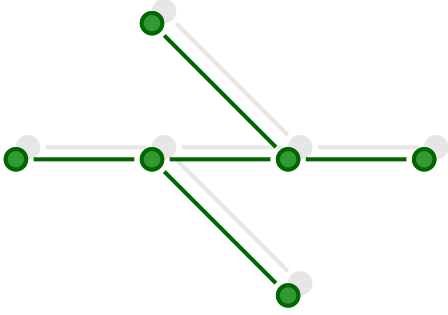
antichain



chain



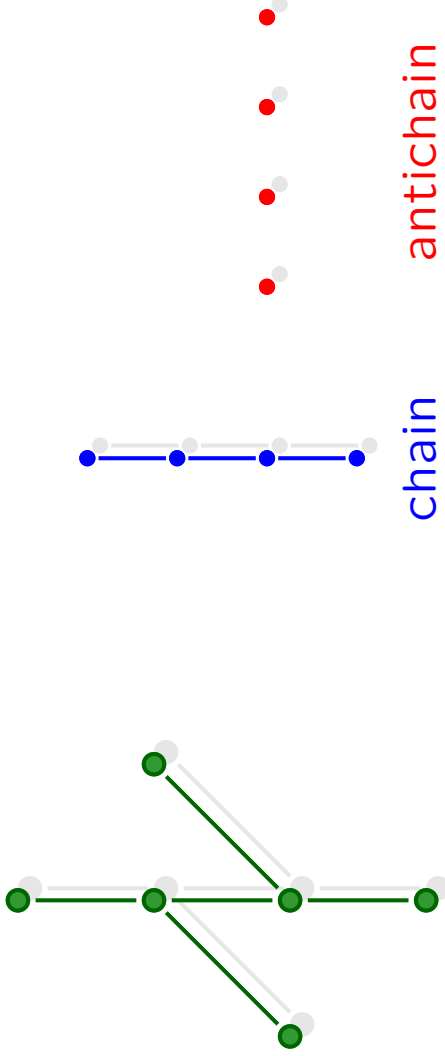
antichain



chain

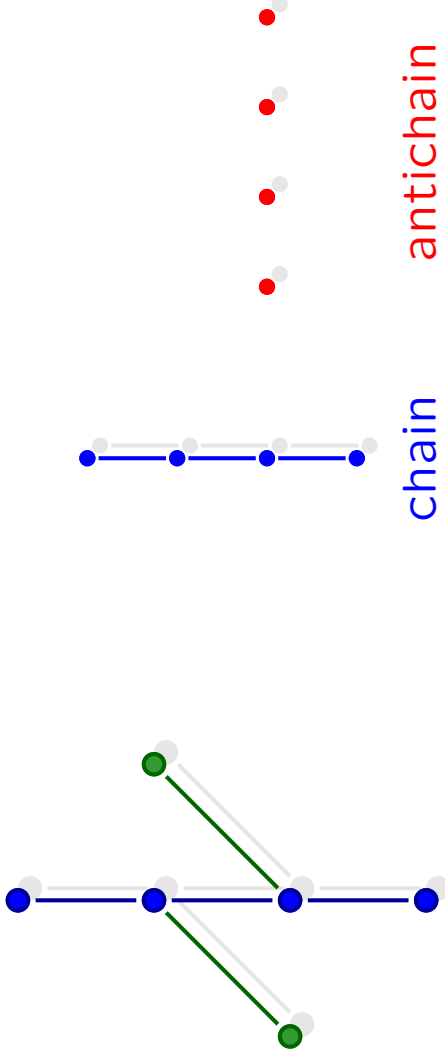


antichain

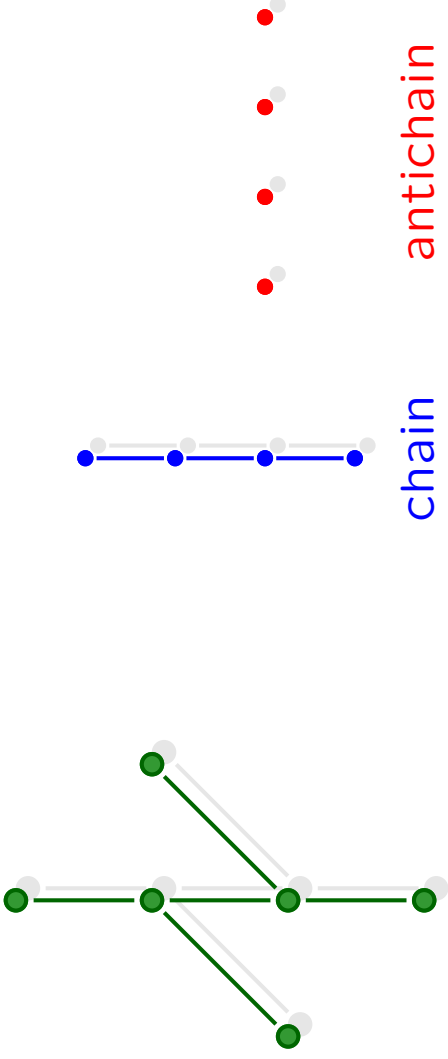


chain antichain

c_1 = maximal size of 1 chain =

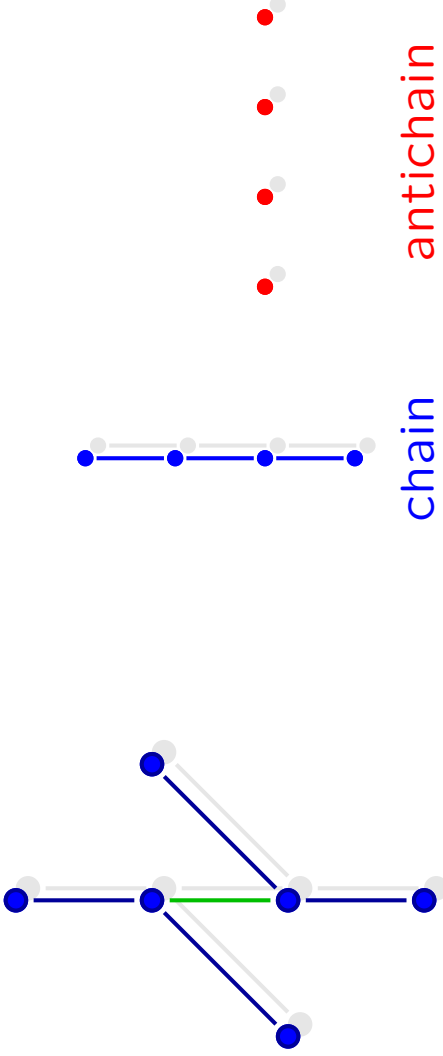


$c_1 = \text{maximal size of 1 chain} = 4$



c_1 = maximal size of 1 chain = 4

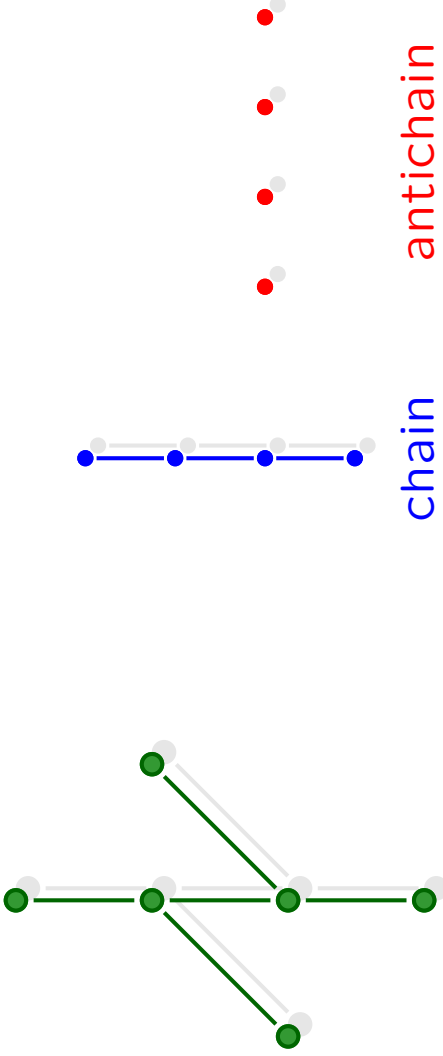
c_2 = maximal size of 2 chains =



chain antichain

$c_1 =$ maximal size of 1 chain $= 4$

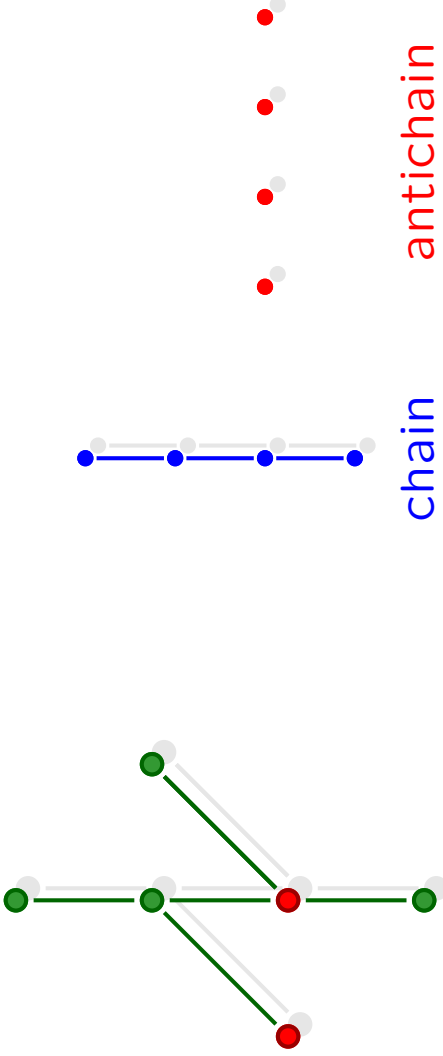
$c_2 =$ maximal size of 2 chains $= 6$



$c_1 =$ maximal size of 1 chain = 4

$c_2 =$ maximal size of 2 chains = 6

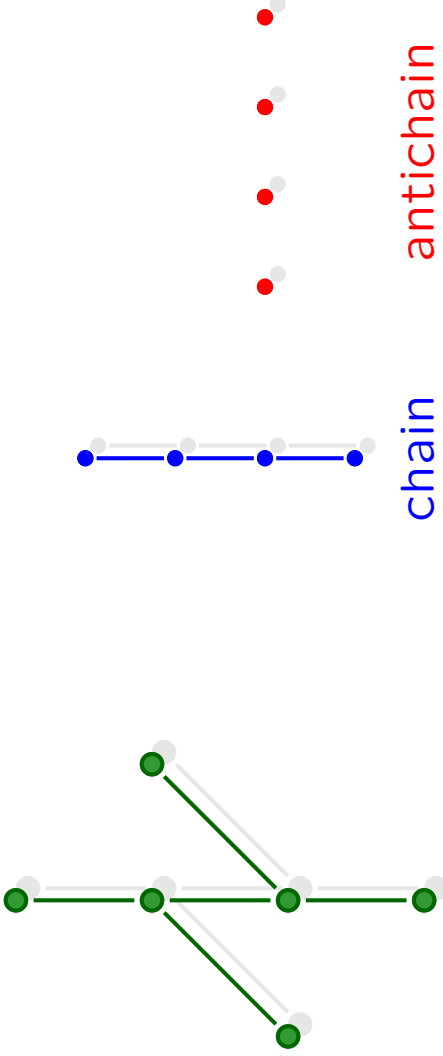
$a_1 =$ maximal size of 1 antichain =



$c_1 = \text{maximal size of 1 chain} = 4$

$c_2 = \text{maximal size of 2 chains} = 6$

$a_1 = \text{maximal size of 1 antichain} = 2$

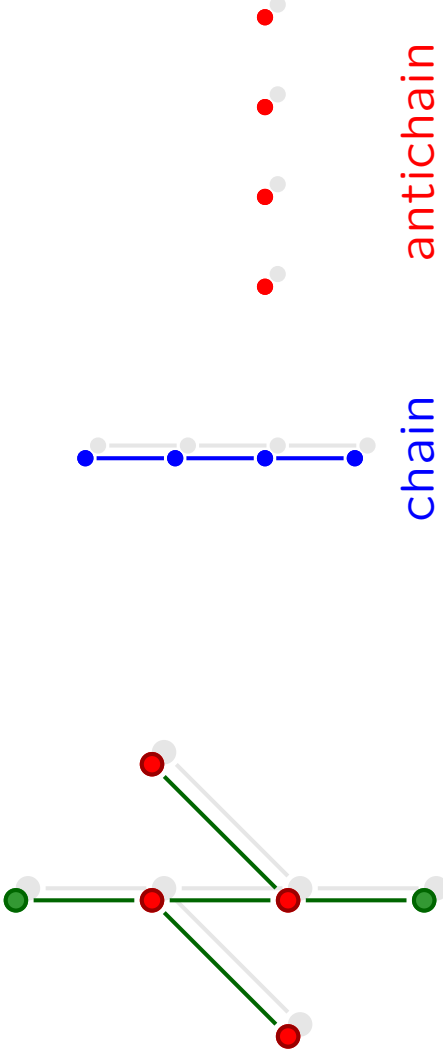


$c_1 =$ maximal size of 1 chain = 4

$c_2 =$ maximal size of 2 chains = 6

$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains =

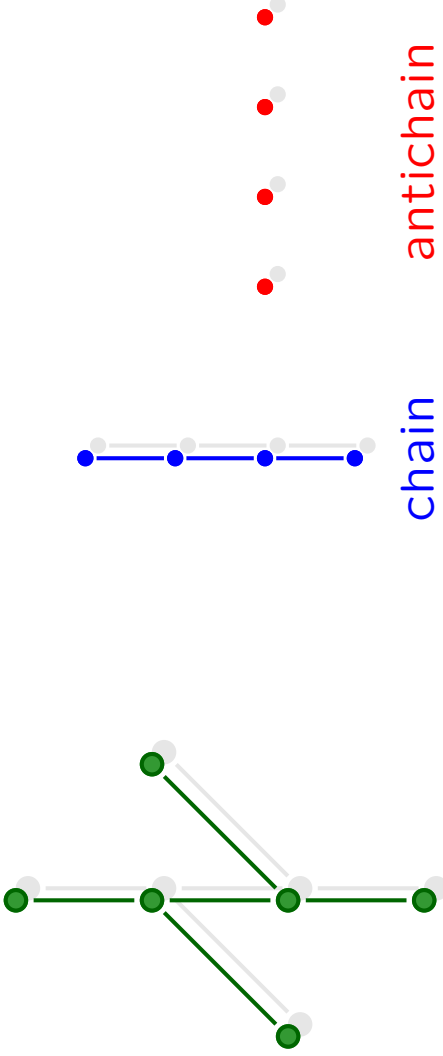


$c_1 =$ maximal size of 1 chain = 4

$c_2 =$ maximal size of 2 chains = 6

$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains = 4



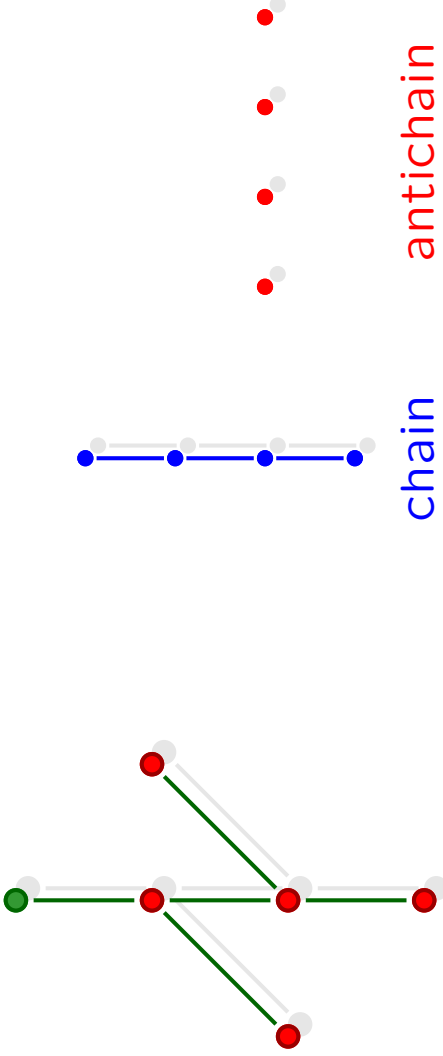
$c_1 =$ maximal size of 1 chain = 4

$c_2 =$ maximal size of 2 chains = 6

$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains = 4

$a_3 =$ maximal size of 3 antichains =



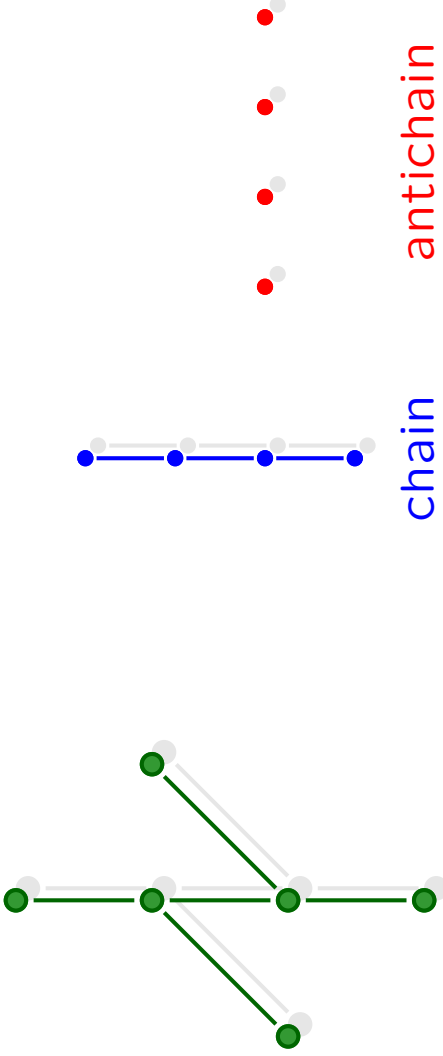
$c_1 = \text{maximal size of 1 chain} = 4$

$c_2 = \text{maximal size of 2 chains} = 6$

$a_1 = \text{maximal size of 1 antichain} = 2$

$a_2 = \text{maximal size of 2 antichains} = 4$

$a_3 = \text{maximal size of 3 antichains} = 5$



$c_1 =$ maximal size of 1 chain = 4

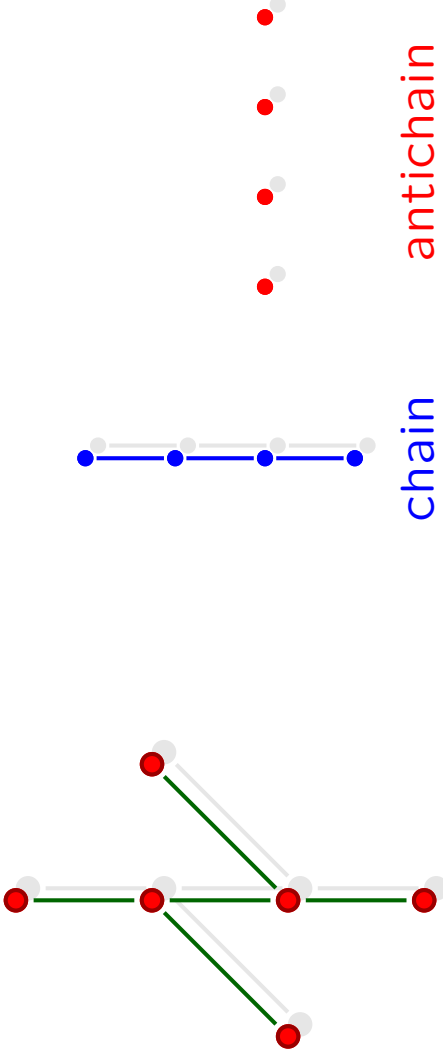
$c_2 =$ maximal size of 2 chains = 6

$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains = 4

$a_3 =$ maximal size of 3 antichains = 5

$a_4 =$ maximal size of 4 antichains =



$c_1 =$ maximal size of 1 chain = 4

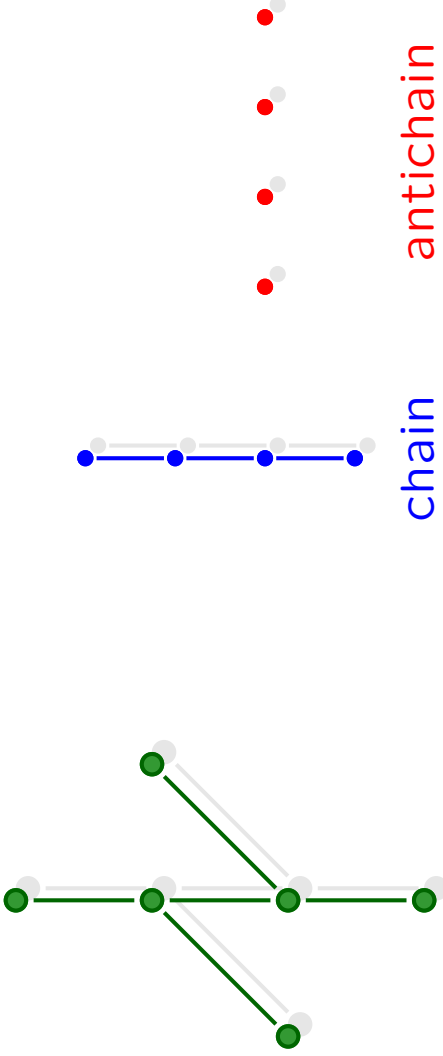
$c_2 =$ maximal size of 2 chains = 6

$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains = 4

$a_3 =$ maximal size of 3 antichains = 5

$a_4 =$ maximal size of 4 antichains = 6



$c_1 =$ maximal size of 1 chain = 4

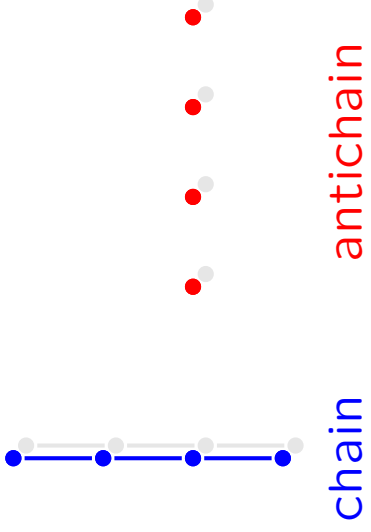
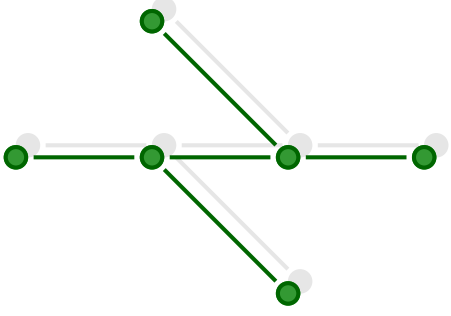
$c_2 =$ maximal size of 2 chains = 6

$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains = 4

$a_3 =$ maximal size of 3 antichains = 5

$a_4 =$ maximal size of 4 antichains = 6



$c_1 = \text{maximal size of 1 chain} = 4$

$c_2 = \text{maximal size of 2 chains} = 6$

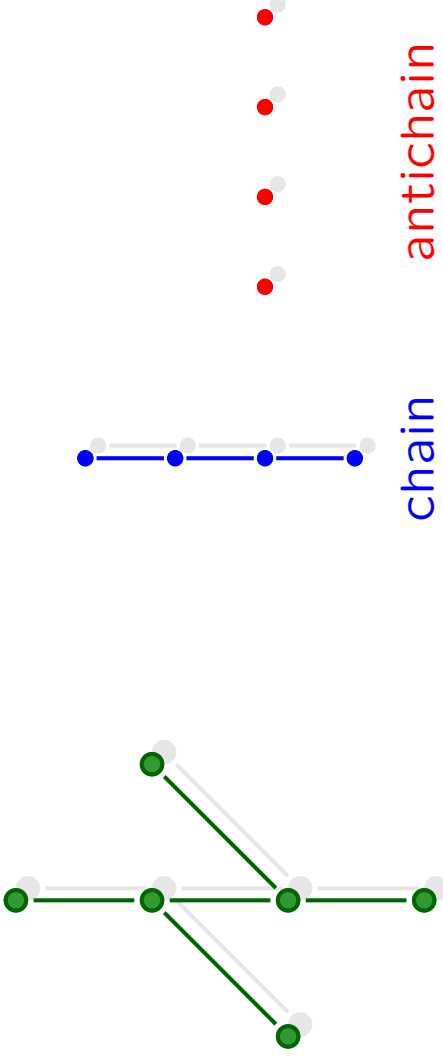
$a_1 = \text{maximal size of 1 antichain} = 4$

$a_2 = \text{maximal size of 2 antichains} = 5$

$a_3 = \text{maximal size of 3 antichains} = 6$

$a_4 = \text{maximal size of 4 antichains} = 8$





$c_1 =$ maximal size of 1 chain = 4

$c_2 =$ maximal size of 2 chains = 6

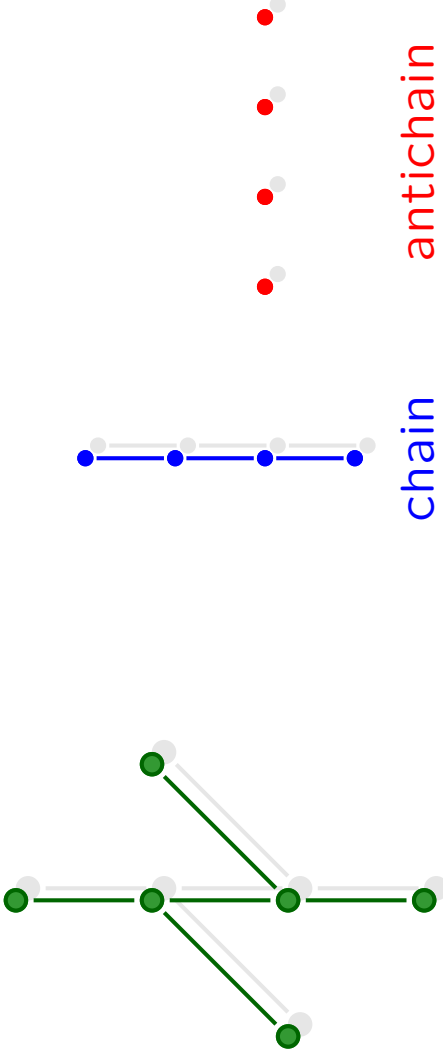
$a_1 =$ maximal size of 1 antichain = 2

$a_2 =$ maximal size of 2 antichains = 4

$a_3 =$ maximal size of 3 antichains = 5

$a_4 =$ maximal size of 4 antichains = 6





$c_1 = \text{maximal size of 1 chain} = 4$

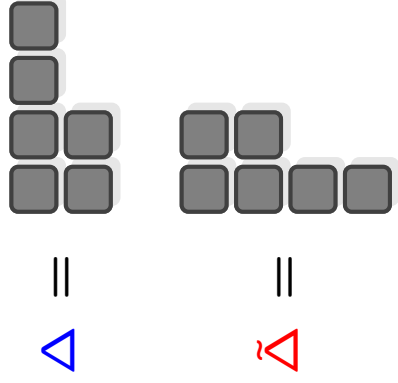
$c_2 = \text{maximal size of 2 chains} = 6$

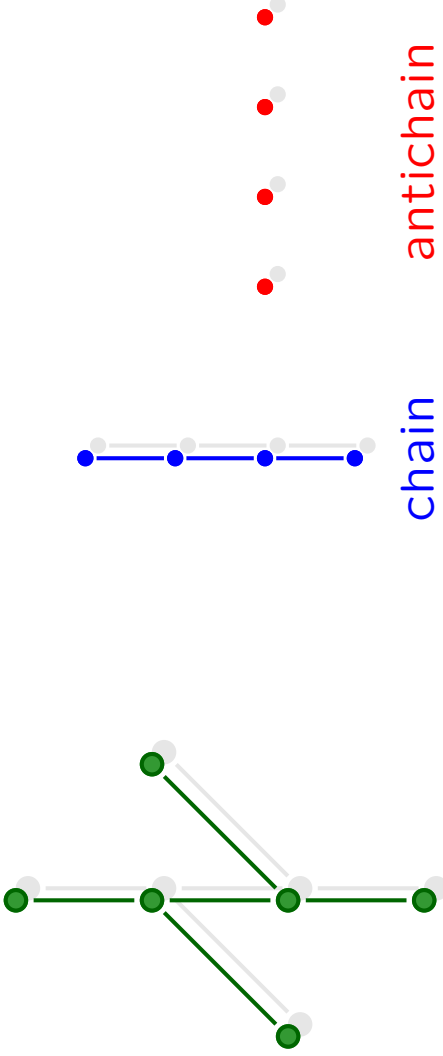
$a_1 = \text{maximal size of 1 antichain} = 2$

$a_2 = \text{maximal size of 2 antichains} = 4$

$a_3 = \text{maximal size of 3 antichains} = 5$

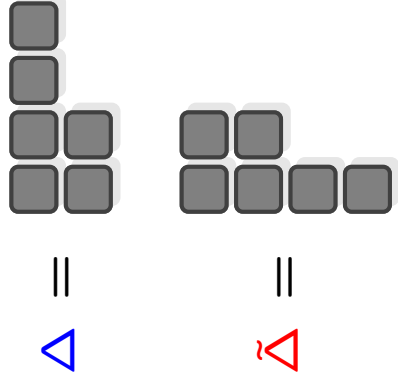
$a_4 = \text{maximal size of 4 antichains} = 6$



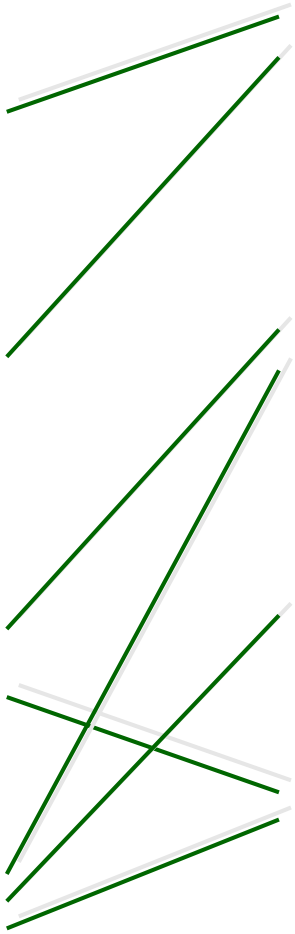
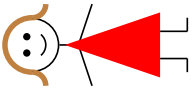
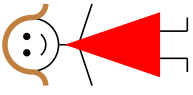
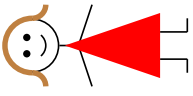
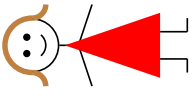
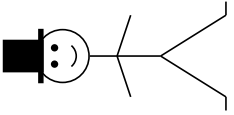
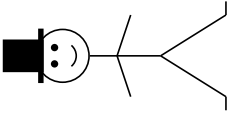
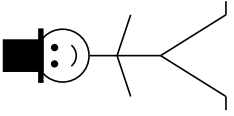
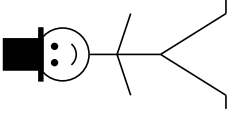
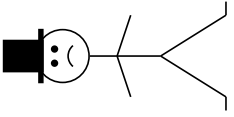


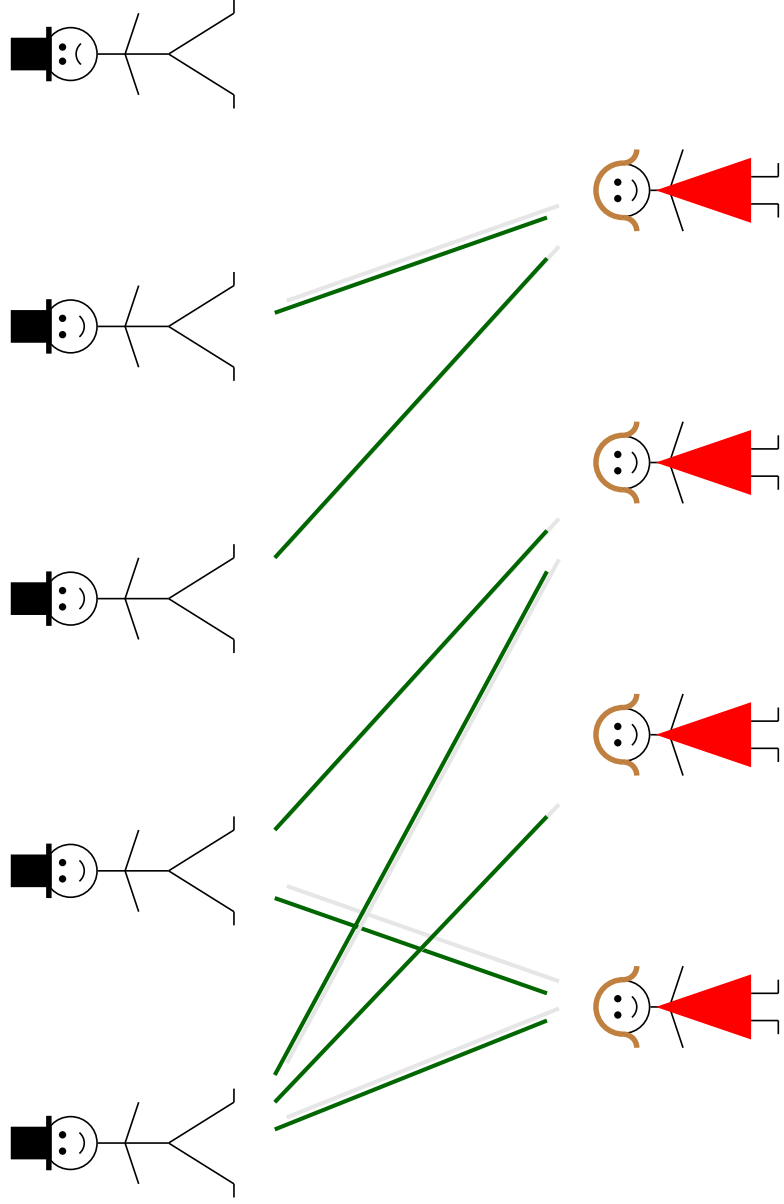
$c_1 = \text{maximal size of 1 chain} = 4$
 $c_2 = \text{maximal size of 2 chains} = 6$

$a_1 = \text{maximal size of 1 antichain} = 2$
 $a_2 = \text{maximal size of 2 antichains} = 4$
 $a_3 = \text{maximal size of 3 antichains} = 5$
 $a_4 = \text{maximal size of 4 antichains} = 6$



Greene's Theorem : $\Delta = \tilde{\Delta}^T$





The Marriage Theorem

The girls can all get a boy (each)

if and only if

k girls together like at least k boys ($\forall k \geq 1$).

Duality Theorem 2:
The MacWilliams Identity

\mathbb{F} = a field

$E = \{e_1, \dots, e_n\}$

A subspace $C \subseteq \mathbb{F}^E$ is also called a *linear code*.

\mathbb{F} = a field

$$E = \{e_1, \dots, e_n\}$$

A subspace $C \subseteq \mathbb{F}^E$ is also called a *linear code*.

Hamming distance: $d(u, v) = \#\{e \in E : u_e \neq v_e\}$

Hamming weight: $w(v) = d(v, 0)$

Support: $S(v) = \{e \in E : v_e \neq 0\}$

\mathbb{F} = a field

$$E = \{e_1, \dots, e_n\}$$

A subspace $C \subseteq \mathbb{F}^E$ is also called a *linear code*.

Hamming distance: $d(u, v) = \#\{e \in E : u_e \neq v_e\}$

Hamming weight: $w(v) = d(v, 0)$ $w(v) = 3$

Support: $S(v) = \{e \in E : v_e \neq 0\}$ $S(v) = \{e_2, e_3, e_5\}$

e_2 e_3 e_5

$$v = (0 \mathbf{1} \mathbf{2} 0 \mathbf{-1})$$

$C \subseteq \mathbb{F}_q^E$ = a linear code with dimension k .

$$A_i = \#\{v \in C : w(v) = i\}$$

The weight enumerator $W_C(x, y)$ of C :
$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$$

$C \subseteq \mathbb{F}_q^E$ = a linear code with dimension k .

$$A_i = \#\{v \in C : w(v) = i\}$$

The weight enumerator $W_C(x, y)$ of C :
$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\begin{aligned} & (0 \ 0 \ 0 \ 0 \ 0) \\ & (1 \ 0 \ 1 \ 0 \ 0) \\ & (0 \ 1 \ 1 \ 0 \ 0) \\ & (0 \ 0 \ 0 \ 1 \ 1) \\ & (1 \ 1 \ 0 \ 0 \ 0) \\ & (1 \ 0 \ 1 \ 1 \ 1) \\ & (0 \ 1 \ 1 \ 1 \ 1) \\ & (1 \ 1 \ 0 \ 1 \ 1) \end{aligned}$$

$$W_C(x, y) = x^5 + 4x^3y^2 + 3xy^4$$

$C \subseteq \mathbb{F}_q^E$ = a linear code with dimension k .

$$A_i = \#\{v \in C : w(v) = i\}$$

The weight enumerator $W_C(x, y)$ of C :
$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$$

The MacWilliams Identity

$$W_{C^\perp}(x, y) = \frac{1}{q^k} W_C(x + (q-1)y, x - y)$$

$C \subseteq \mathbb{F}_q^E$ = a linear code with dimension k .

$$A_i = \#\{v \in C : w(v) = i\}$$

The weight enumerator $W_C(x, y)$ of C : $W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$

The MacWilliams Identity

$$W_{C^\perp}(x, y) = \frac{1}{q^k} W_C(x + (q-1)y, x - y)$$



$C \subseteq \mathbb{F}_q^E$ = a linear code with dimension k .

$$A_i = \#\{v \in C : w(v) = i\}$$

The weight enumerator $W_C(x, y)$ of C :
$$W_C(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i$$

The MacWilliams Identity

$$W_{C^\perp}(x, y) = \frac{1}{q^k} W_C(x + (q-1)y, x-y)$$



$M = (E, \rho)$ is a matroid if and only if, for all $X \subseteq Y \subseteq E$,

- $0 \leq \rho(X) \leq \rho(Y) \leq |Y|$
- $\rho(X) \cap \rho(Y) + \rho(X) \cup \rho(Y) \leq \rho(X) + \rho(Y)$

$C \subseteq \mathbb{F}_q^E$ = a linear code

$A_i^{(r)}$ = # r -dimensional subcodes $D \subseteq C$ with $|\cup_{v \in D} S(v)| = i$

The r th higher weight enumerator of C : $W_C^{(r)}(z) = \sum_{i=0}^n A_i^{(r)} z^i$

$C \subseteq \mathbb{F}_q^E$ = a linear code

$A_i^{(r)}$ = # r -dimensional subcodes $D \subseteq C$ with $|U_{v \in D} S(v)| = i$

The r th higher weight enumerator of C : $W_C^{(r)}(z) = \sum_{i=0}^n A_i^{(r)} z^i$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$W_C^{(2)}(z) = 3z^5 + 3z^4 + z^3$$

$$\begin{array}{cccccc} [11000] & [11000] & [10100] & [01100] & [11000] & [10100] & [01100] \\ [10100] & [11111] & [11111] & [11111] & [01011] & [00111] & [00111] \\ 3 & 5 & 5 & 5 & 4 & 4 & 4 \end{array}$$

$C \subseteq \mathbb{F}_q^E$ = a linear code

$A_i^{(r)}$ = # r -dimensional subcodes $D \subseteq C$ with $|\cup_{v \in D} S(v)| = i$

The r th higher weight enumerator of C : $W_C^{(r)}(z) = \sum_{i=0}^n A_i^{(r)} z^i$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$W_C^{(2)}(z) = 3z^5 + 3z^4 + z^3$$

$$\begin{array}{llll} [11000] & [11000] & [10100] & [01100] & [11000] & [10100] & [01100] \\ [10100] & [11111] & [11111] & [11111] & [01011] & [00111] & [00111] \\ 3 & 5 & 5 & 5 & 4 & 4 & 4 \end{array}$$

Problem: Calculate these enumerators for interesting linear codes

The extremal doubly-even, self-dual binary codes:

1 × [24, 12, 8] code (the extended binary Golay code)

5 × [32, 16, 8] codes

1 × [48, 24, 12] code

At most 1 × [72, 36, 16] code

At least 12579 × [40, 20, 8] codes

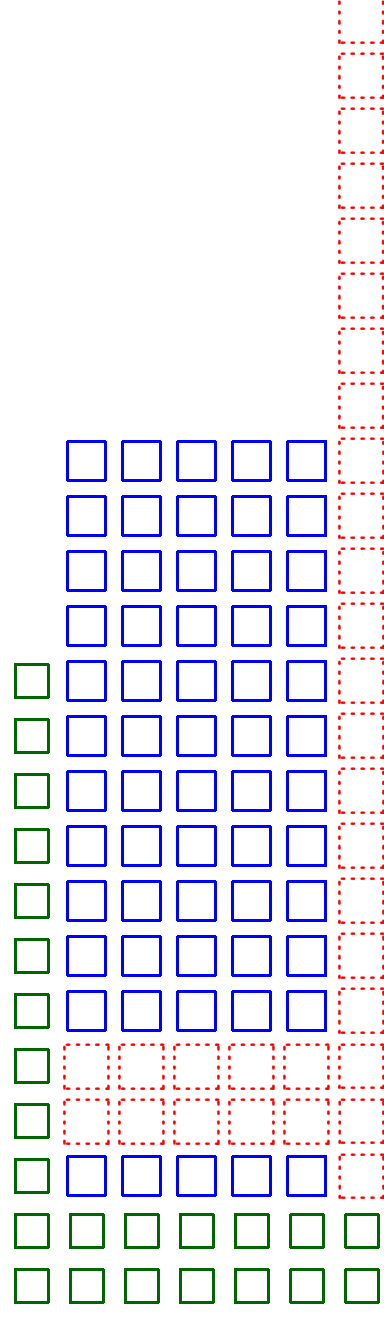
etc.

The extremal doubly-even, self-dual binary codes:

1 × [24, 12, 8] code

5 × [32, 16, 8] codes

1 × [48, 24, 12] code



$W_C^{(r)}(z)$:

□ : [Dougherty and Gulliver 2001]

□ : [Milenkovic, Coffey and Compton 2003]

□ : missing

The *Tutte polynomial* of a matroid $M = (E, \rho)$:

$$T_M(x, y) = \sum_{X \subseteq E} (x - 1)^{\rho_M(E) - \rho_M(X)} (y - 1)^{|X| - \rho_M(X)}$$

The *Tutte polynomial* of a matroid $M = (E, \rho)$:

$$T_M(x, y) = \sum_{X \subseteq E} (x - 1)^{\rho_M(E) - \rho_M(X)} (y - 1)^{|X| - \rho_M(X)}$$

Britz 2005: For a linear code $C \subseteq \mathbb{F}_q^E$ of dimension k ,

$$W_C^{(r)}(z) = z^{n-k} (1-z)^k \sum_{i=0}^r \frac{(-1)^{r-i}}{[r]_r} q^{\binom{r-i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} T_{M_C} \left(\frac{1 + (q^i - 1)z}{1-z}, \frac{1}{z} \right)$$

The *Tutte polynomial* of a matroid $M = (E, \rho)$:

$$T_M(x, y) = \sum_{X \subseteq E} (x - 1)^{\rho_M(E) - \rho_M(X)} (y - 1)^{|X| - \rho_M(X)}$$

Britz 2005: For a linear code $C \subseteq \mathbb{F}_q^E$ of dimension k ,

$$W_C^{(r)}(z) = z^{n-k} (1-z)^k \sum_{i=0}^r \frac{(-1)^{r-i}}{[r]_r} q^{\binom{r-i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} T_{M_C} \left(\frac{1 + (q^i - 1)z}{1-z}, \frac{1}{z} \right)$$

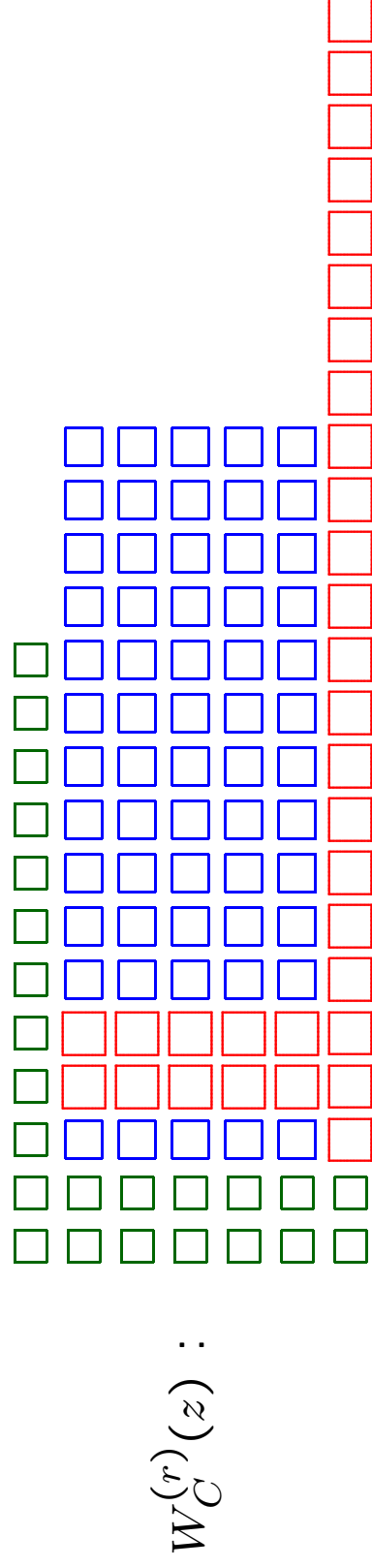
$$T_M(x, y) = \begin{cases} y T_{M/e}(x, y), & \rho_M(e) = 0; \\ x T_{M/e}(x, y), & \rho_{M^*}(e) = 0; \\ T_{M \setminus e}(x, y) + T_{M/e}(x, y), & \text{otherwise.} \end{cases}$$

The extremal doubly-even, self-dual binary codes:

1 × [24, 12, 8] code

5 × [32, 16, 8] codes

1 × [48, 24, 12] code



□ : [Dougherty and Gulliver 2001]

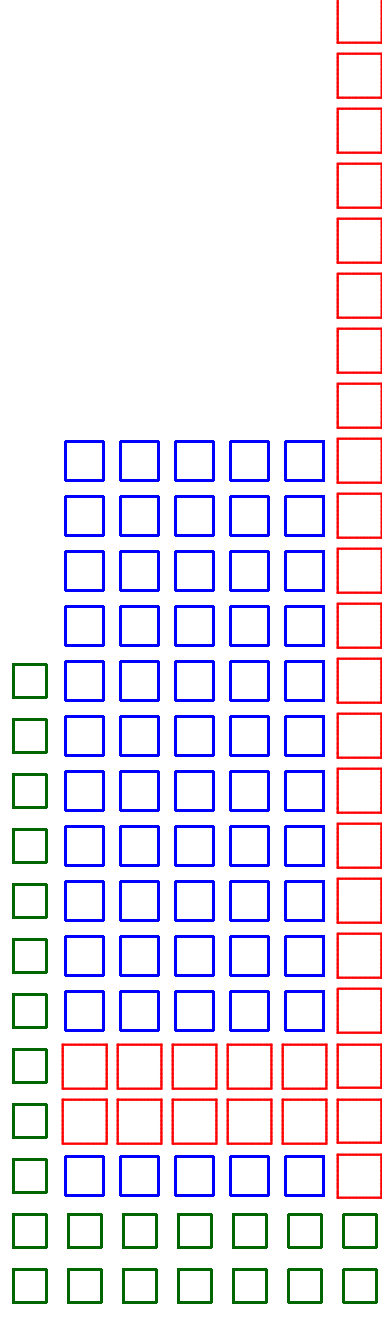
□ : [Milenkovic, Coffey and Compton 2003]

□ : [Britz, Britz, Shiromoto, and Sørensen 2007]

The extremal doubly-even, self-dual binary codes:

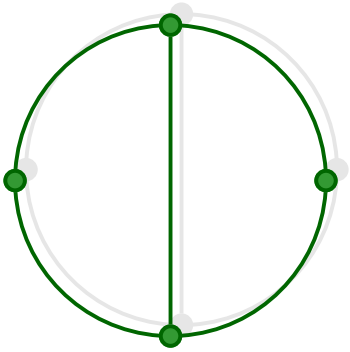
- 1 sec 1 × [24, 12, 8] code
- 40 sec 5 × [32, 16, 8] codes
- 800 hours 1 × [48, 24, 12] code

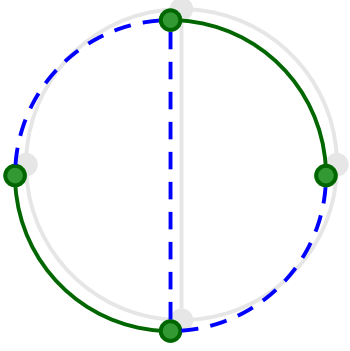
$W_C^{(r)}(z)$:



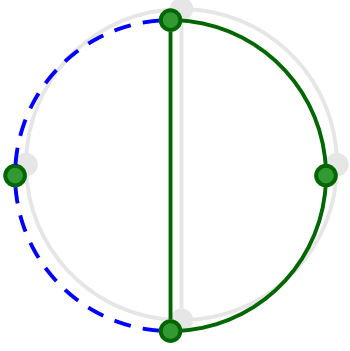
- : [Dougherty and Gulliver 2001]
- : [Milenkovic, Coffey and Compton 2003]
- : [Britz, Britz, Shiromoto, and Sørensen 2007]

Duality Theorem 3:
Wei's Duality Theorem

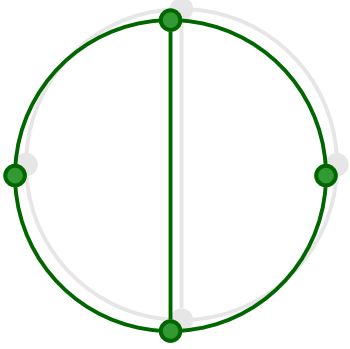




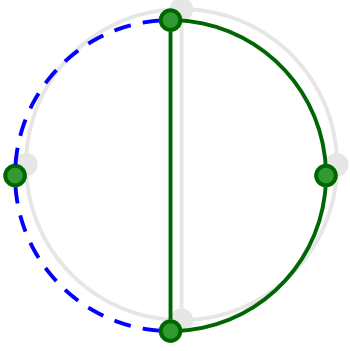
Bond = minimal cutset



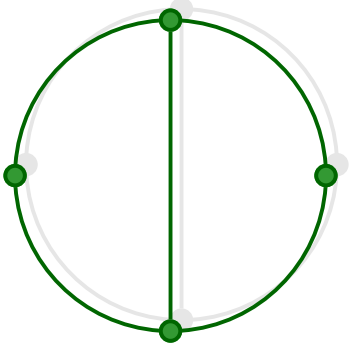
Bond = minimal cutset



b_1 = minimal size of a bond

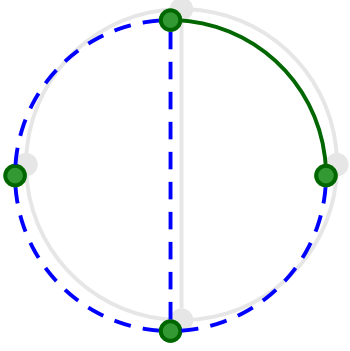


$b_1 = \text{minimal size of a bond} = 2$



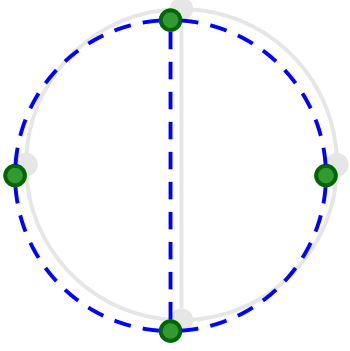
b_1 = minimal size of a bond = 2

b_2 = min. # edges in 2 distinct bonds =



$b_1 = \text{minimal size of a bond} = 2$

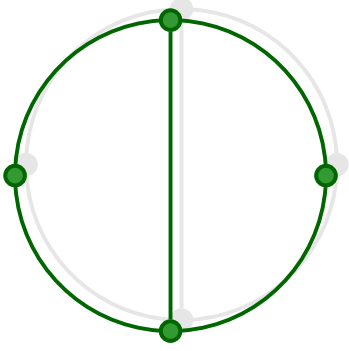
$b_2 = \text{min. \# edges in 2 distinct bonds} = 4$



$b_1 = \text{minimal size of a bond} = 2$

$b_2 = \text{min. \# edges in 2 distinct bonds} = 4$

$b_3 = \text{min. \# edges in 3 distinct bonds } B_1, B_2, B_3, B_3 \notin B_1 \cup B_2 = 5$

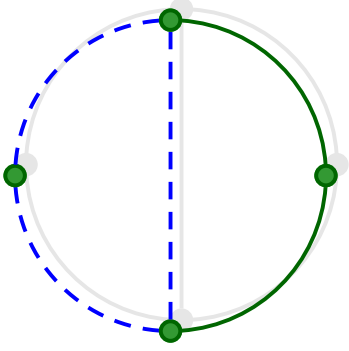


b_1 = minimal size of a bond = 2

b_2 = min. # edges in 2 distinct bonds = 4

b_3 = min. # edges in 3 distinct bonds B_1, B_2, B_3 , $B_3 \not\subseteq B_1 \cup B_2$ = 5

c_1 = minimal size of a cycle =

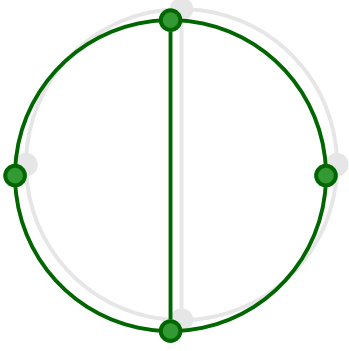


b_1 = minimal size of a bond = 2

b_2 = min. # edges in 2 distinct bonds = 4

b_3 = min. # edges in 3 distinct bonds B_1, B_2, B_3 , $B_3 \not\subseteq B_1 \cup B_2$ = 5

c_1 = minimal size of a cycle = 3



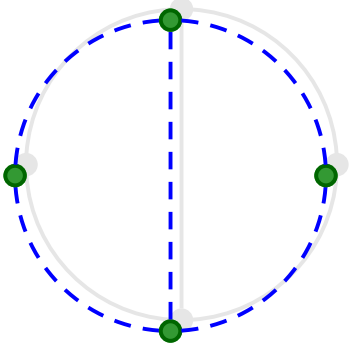
b_1 = minimal size of a bond = 2

b_2 = min. # edges in 2 distinct bonds = 4

b_3 = min. # edges in 3 distinct bonds B_1, B_2, B_3 , $B_3 \not\subseteq B_1 \cup B_2$ = 5

c_1 = minimal size of a cycle = 3

c_2 = min. # edges in 2 distinct cycles =



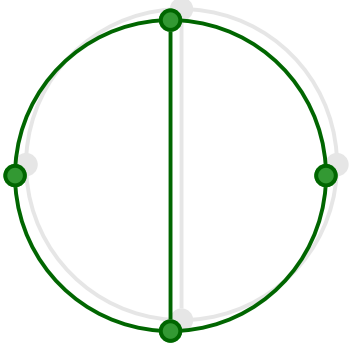
b_1 = minimal size of a bond = 2

b_2 = min. # edges in 2 distinct bonds = 4

b_3 = min. # edges in 3 distinct bonds B_1, B_2, B_3 , $B_3 \not\subseteq B_1 \cup B_2$ = 5

c_1 = minimal size of a cycle = 3

c_2 = min. # edges in 2 distinct cycles = 5



$b_1 =$ minimal size of a bond $= 2$

$b_2 =$ min. # edges in 2 distinct bonds $= 4$

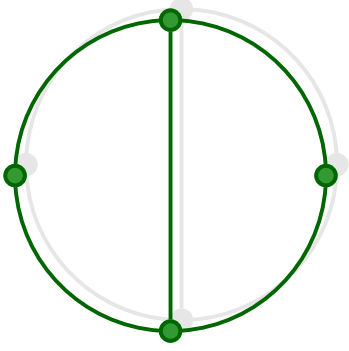
$b_3 =$ min. # edges in 3 distinct bonds B_1, B_2, B_3 , $B_3 \not\subseteq B_1 \cup B_2 = 5$

$c_1 =$ minimal size of a cycle $= 3$

$c_2 =$ min. # edges in 2 distinct cycles $= 5$

Set $U = \{b_1, b_2, b_3\} = \{2, 4, 5\}$

and $V = \{5 + 1 - c_2, 5 + 1 - c_1\} = \{1, 3\}$.



b_1 = minimal size of a bond = 2

b_2 = min. # edges in 2 distinct bonds = 4

b_3 = min. # edges in 3 distinct bonds B_1, B_2, B_3 , $B_3 \not\subseteq B_1 \cup B_2$ = 5

c_1 = minimal size of a cycle = 3

c_2 = min. # edges in 2 distinct cycles = 5

Set $U = \{b_1, b_2, b_3\} = \{2, 4, 5\}$

and $V = \{5 + 1 - c_2, 5 + 1 - c_1\} = \{1, 3\}$.

$$U \cup V = \{1, 2, 3, 4, 5\} \quad \text{and} \quad U \cap V = \emptyset$$

G = a multigraph on n edges

Define

k = # edges in a spanning forest of G

b_i = min. # edges in i bonds, none contained in the union of the others

c_j = min. # edges in j cycles, none contained in the union of the others

$$U = \{b_1, \dots, b_k\}$$

$$V = \{n + 1 - c_{n-k}, \dots, n + 1 - c_1\}.$$

Britz 2007: $U \cup V = \{1, \dots, n\}$ and $U \cap V = \emptyset$.

M = a matroid of rank k on n elements

Define

f_i = maximal size of an i -rank set in M

f_j^* = maximal size of an j -rank set in M^*

$$U = \{f_0 + 1, \dots, f_{k-1} + 1\}$$

$$V = \{n - f_{n-k-1}^*, \dots, n - f_0^*\}.$$

Britz et al.: $U \cup V = \{1, \dots, n\}$ and $U \cap V = \emptyset$.

M = a matroid of rank k on n elements

Define

f_i = maximal size of an i -rank set in M

f_j^* = maximal size of an j -rank set in M^*

$$U = \{f_0 + 1, \dots, f_{k-1} + 1\}$$

$$V = \{n - f_{n-k-1}^*, \dots, n - f_0^*\}.$$

Britz et al.: $U \cup V = \{1, \dots, n\}$ and $U \cap V = \emptyset$.

Proof. Assume that the theorem is false.

Then $f_i + 1 = n - f_j^*$ for some i, j .

Let $A \subseteq E$ satisfy $|A| = f_j^*$ and $r_{M^*}(A) = j$.

Then $|E - A| = f_i + 1$, so $r_M(E - A) \geq i + 1$.

Since $|E - A| + r_{M^*}(A) - r(M^*) = r_M(E - A)$,

$$-f_j^* + j + r \geq i + 1.$$

Similarly,

$$n - f_i + i - r \geq j + 1.$$

Hence, $1 = n - f_i - f_j^* \geq 2$, a contradiction. \square

M = a matroid of rank k on n elements

Define

f_i = maximal size of an i -rank set in M

f_j^* = maximal size of an j -rank set in M^*

$$U = \{f_0 + 1, \dots, f_{k-1} + 1\}$$

$$V = \{n - f_{n-k-1}^*, \dots, n - f_0^*\}.$$

Britz et al.: $U \cup V = \{1, \dots, n\}$ and $U \cap V = \emptyset$.

Britz et al.: Further generalizations.

Britz et al.: Applications to graphs, codes, modules, and matchings.

M = a matroid of rank k on n elements

Define

f_i = maximal size of an i -rank set in M

f_j^* = maximal size of an j -rank set in M^*

$$U = \{f_0 + 1, \dots, f_{k-1} + 1\}$$

$$V = \{n - f_{n-k-1}^*, \dots, n - f_0^*\}.$$

Britz et al.: $U \cup V = \{1, \dots, n\}$ and $U \cap V = \emptyset$.

Britz et al.: Further generalizations.

Britz et al.: Applications to graphs, codes, modules, and matchings.

Wei's Duality Theorem

M = a matroid of rank k on n elements

Define

f_i = maximal size of an i -rank set in M

f_j^* = maximal size of an j -rank set in M^*

$$U = \{f_0 + 1, \dots, f_{k-1} + 1\}$$

$$V = \{n - f_{n-k-1}^*, \dots, n - f_0^*\}.$$

Britz et al.: $U \cup V = \{1, \dots, n\}$ and $U \cap V = \emptyset$.

Britz et al.: Further generalizations.

Britz et al.: Applications to graphs, codes, modules, and matchings.

Wei's Duality Theorem



Thank you!