Formalization of some central theorems in combinatorics of finite sets

Short Presentations (LPAR-21)

Abhishek Kr Singh

School of Technology and Computer Science
Tata Institute of Fundamental Research, Mumbai.

International Conference on Logic for Programming, Artificial Intelligence and Reasoning, 2017

Overview.

- Theorems and the connection between them
  - Dilworth's Decomposition Theorem
  - Mirsky's Theorem
  - Hall's Marriage theorem
  - Erdős-Szekeres Theorem
- The Coq Formalization of these theorems
  - Formal statement of these theorems
  - The proof ideas.
- Scope for Future Work

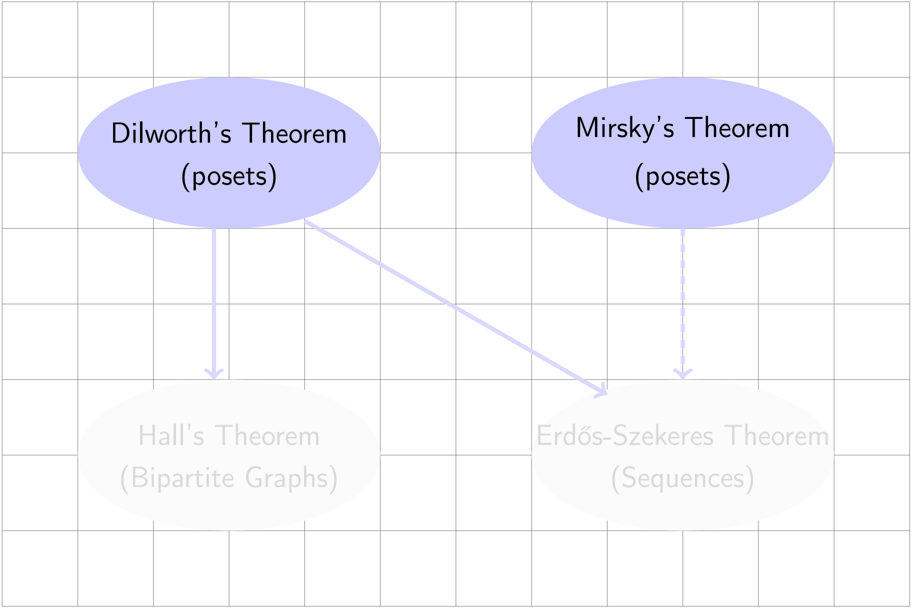
Overview.

- Theorems and the connection between them
  - Dilworth's Decomposition Theorem
  - Mirsky's Theorem
  - Hall's Marriage theorem
  - Erdős-Szekeres Theorem
- The Coq Formalization of these theorems
  - Formal statement of these theorems
  - The proof ideas.
- Scope for Future Work

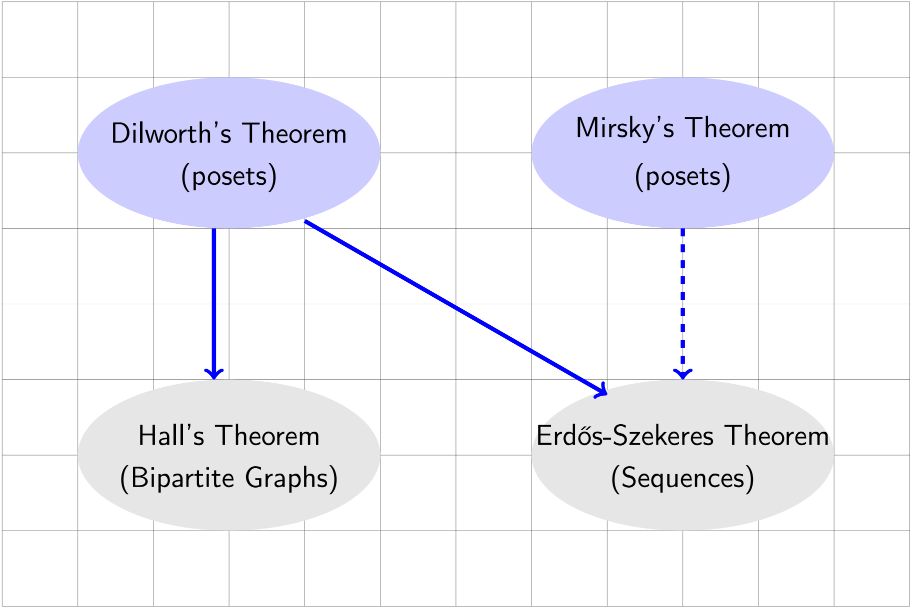
Overview.

- Theorems and the connection between them
  - Dilworth's Decomposition Theorem
  - Mirsky's Theorem
  - Hall's Marriage theorem
  - Erdős-Szekeres Theorem
- The Coq Formalization of these theorems
  - Formal statement of these theorems
  - The proof ideas.
- Scope for Future Work

Theorems and the connection between them



Theorems and the connection between them

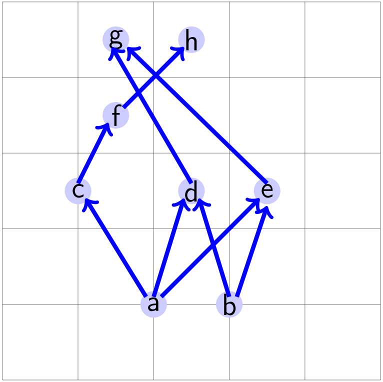


Dilworth's Decomposition Theorem

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- Partially Ordered Set (P,<).
- Chain.
- Antichain.
- Chain cover.
- Antichain cover.
- Height.
- Width.

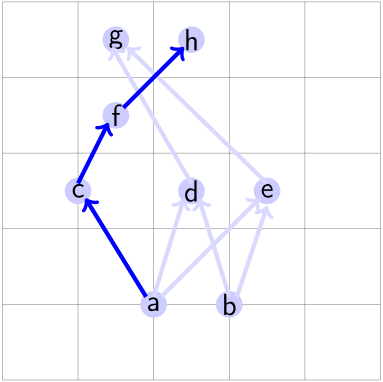


Dilworth's Decomposition Theorem

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- Partially Ordered Set (P,<).
- Chain.
- Antichain.
- Chain cover.
- Antichain cover.
- Height.
- Width.

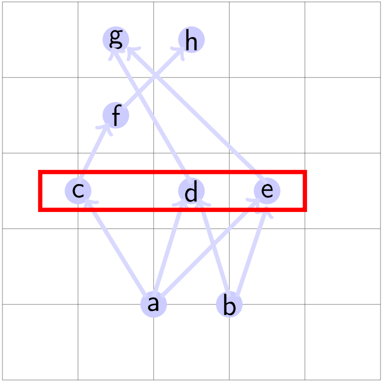


Dilworth's Decomposition Theorem

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- Partially Ordered Set (P,<).
- Chain.
- Antichain.
- Chain cover.
- Antichain cover.
- Height.
- Width.

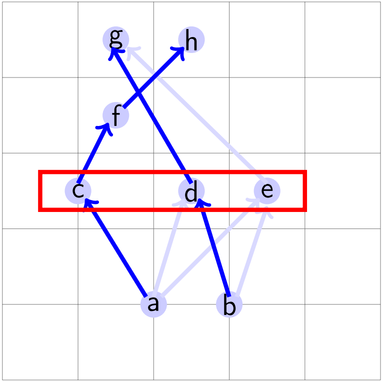


Dilworth's Decomposition Theorem

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- Partially Ordered Set (P,<).
- Chain.
- Antichain.
- Chain cover.
- Antichain cover.
- Height.
- Width.

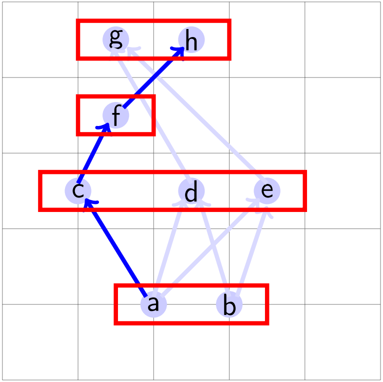


Dilworth's Decomposition Theorem

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- Partially Ordered Set (P,<).
- Chain.
- Antichain.
- Chain cover.
- Antichain cover.
- Height.
- Width.



Dilworth's Decomposition Theorem

Formal Statement in Coq

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- let m be the size of a largest antichain (i.e., width of a poset).
- let n be the number of chains in a smallest chain cover.
- then m=n.

Theorem (Dilworth_Thm: Formal statement)

∀ (P: FPO U)(m n: nat), (Is_width P m) → (∃ C, (Is_a_smallest_chain_cover P C) ∧ (cardinal C n)) → m=n.

Dilworth's Decomposition Theorem

Formal Statement in Coq

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- let m be the size of a largest antichain (i.e., width of a poset).
- let n be the number of chains in a smallest chain cover.
- then m=n.

Theorem (Dilworth_Thm: Formal statement)

$\forall$ *(P: FPO U)(m n: nat), (Is_width P m)* $\rightarrow$ *(*$\exists$ *C, (Is_a_smallest_chain_cover P C)* $\wedge$ *(cardinal C n))* $\rightarrow$ *m=n.*

Dilworth's Decomposition Theorem

Formal Statement in Coq

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- let m be the size of a largest antichain (i.e., width of a poset).
- let n be the number of chains in a smallest chain cover.
- then m=n.

Theorem (Dilworth_Thm: Formal statement)

$\forall$ *(P: FPO U)(m n: nat), (Is_width P m)* $\rightarrow$ *(*$\exists$ *C, (Is_a_smallest_chain_cover P C)* $\wedge$ *(cardinal C n))* $\rightarrow$ *m=n.*

Dilworth's Decomposition Theorem

Formal Statement in Coq

Theorem

In any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same.

- let m be the size of a largest antichain (i.e., width of a poset).
- let n be the number of chains in a smallest chain cover.
- then m=n.

Theorem (Dilworth_Thm: Formal statement)

$\forall$ *(P: FPO U)(m n: nat), (Is_width P m)* $\rightarrow$ *(*$\exists$ *C,*
(Is_a_smallest_chain_cover P C) $\wedge$ *(cardinal C n))* $\rightarrow$ *m=n.*

Theorem

In any finite partially ordered set (poset), the size of a smallest antichain cover and a largest chain are the same.

- let m be the size of largest chain (i.e., height of a poset).
- let n be the number of antichains in a smallest antichain cover.
- then m=n.

Theorem (Dual_Dilworth: Formal statement)

$\forall$ *(P: FPO U)(m n: nat), (Is_height P m)* $\rightarrow$ *(*$\exists$ *C, (Is_a_smallest_antichain_cover P C)* $\wedge$ *(cardinal C n))* $\rightarrow$ *m=n.*

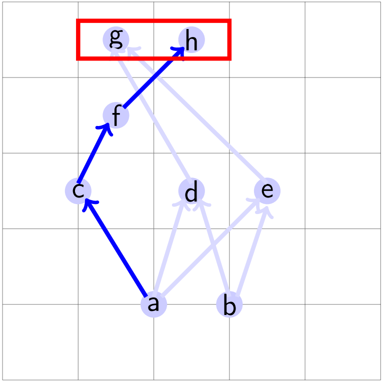
Mirsky's Theorem

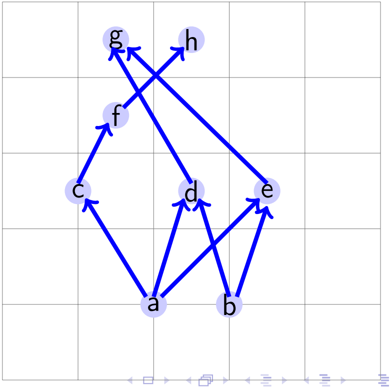
Proof Idea: Induction on the size of largest chain

If m is the size of a largest chain, then there cannot be an antichain cover of size less than m. Therefore it is sufficient to prove:

Lemma (Mirsky:)

If m is the size of a largest chain then there exists an antichain cover of size m.





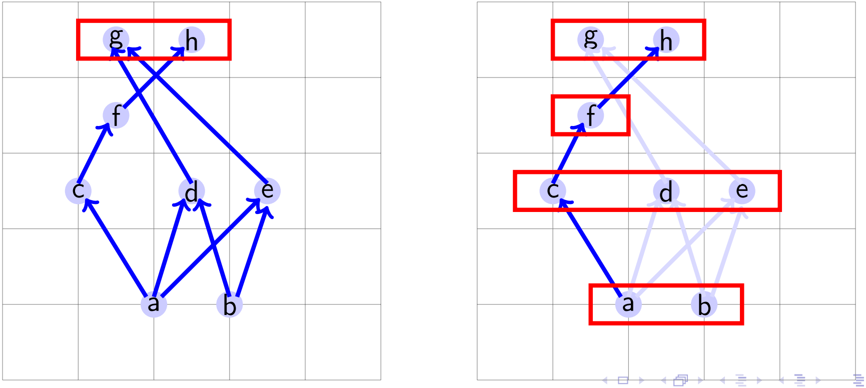
Mirsky's Theorem

Proof Idea: Induction on the size of largest chain

If m is the size of a largest chain, then there cannot be an antichain cover of size less than m. Therefore it is sufficient to prove:

Lemma (Mirsky:)

If m is the size of a largest chain then there exists an antichain cover of size m.



The key idea in the proof of Mirsky's theorem[5] is the following lemma

Lemma (Pre_Mirsky:)

There exists an antichain which intersects with every largest chain in the poset.

However, it is not easy to prove a similar lemma for Dilworth's theorem[2].

Lemma (Pre_Dilworth:)

There exists a chain which intersects with every largest antichain in the poset.

The key idea in the proof of Mirsky's theorem[5] is the following lemma

Lemma (Pre_Mirsky:)

There exists an antichain which intersects with every largest chain in the poset.

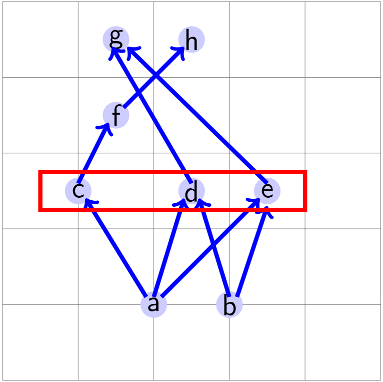
However, it is not easy to prove a similar lemma for Dilworth's theorem[2].

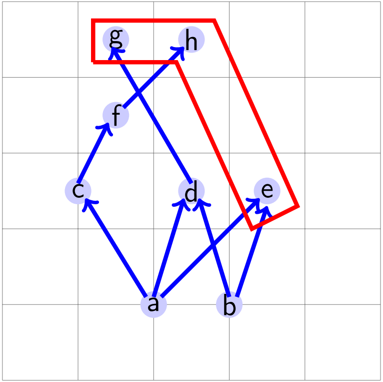
Lemma (Pre_Dilworth:)

There exists a chain which intersects with every largest antichain in the poset.

Dilworth's Theorem

Proof by Perles: Induction on the size of poset





Dilworth's Theorem: Other Variants

Disjoint Chain cover

Lemma (exists_disjoint_cover:)

If $\mathscr{C}_{\mathscr{V}}$ is a smallest chain cover of size m for P, then there also exists a disjoint chain cover $\mathscr{C}_{\mathscr{V}}'$ of size m for P.

This lemma can be used to obtain the following variant of Dilworth's theorem:

Theorem (Dilworth_Disj:)

In any poset if m is the size of a largest antichain then there exists a disjoint chain cover of size m.

Dilworth's Theorem: Other Variants

Disjoint Chain cover

Lemma (exists_disjoint_cover:)

If $\mathscr{C}_{\mathscr{V}}$ is a smallest chain cover of size m for P, then there also exists a disjoint chain cover $\mathscr{C}_{\mathscr{V}}{}'$ of size m for P.

This lemma can be used to obtain the following variant of Dilworth's theorem:

Theorem (Dilworth_Disj:)

In any poset if m is the size of a largest antichain then there exists a disjoint chain cover of size m.

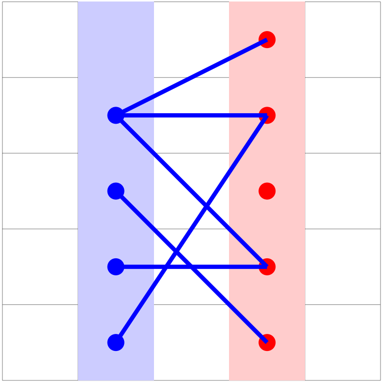
Hall's Marriage Theorem

Left Perfect matching in a Bipartite Graph

Theorem (Hall's Marriage Theorem [4]:)

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ if and only if $\exists$ an L-perfect matching.

- Matching.
- L-perfect matching.
- N(S) neighbour of a set S.



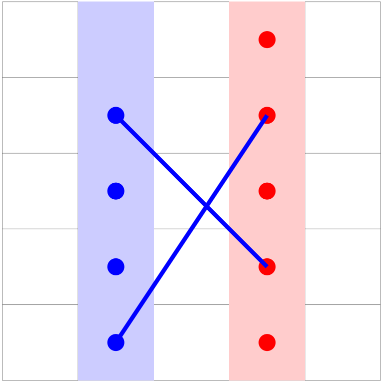
Hall's Marriage Theorem

Left Perfect matching in a Bipartite Graph

Theorem (Hall's Marriage Theorem [4]:)

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ if and only if $\exists$ an L-perfect matching.

- Matching.
- L-perfect matching.
- N(S) neighbour of a set S.



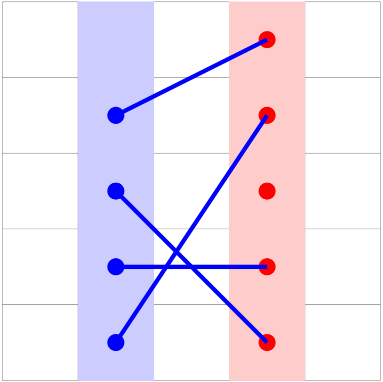
Hall's Marriage Theorem

Left Perfect matching in a Bipartite Graph

Theorem (Hall's Marriage Theorem [4]:)

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ *if and only if* $\exists$ *an L-perfect matching.*

- Matching.
- L-perfect matching.
- N(S) neighbour of a set S.



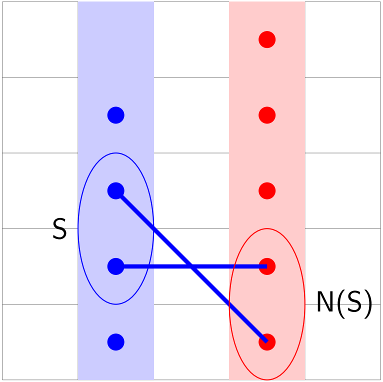
Hall's Marriage Theorem

Left Perfect matching in a Bipartite Graph

Theorem (Hall's Marriage Theorem [4]:)

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ if and only if $\exists$ an L-perfect matching.

- Matching.
- L-perfect matching.
- N(S) neighbour of a set S.



Hall's Marriage Theorem

Formal Statement in Coq

Theorem

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ *if and only if* $\exists$ *an L-perfect matching.*

Theorem (Halls_Thm: Formal statement)

($\forall$*S, Included S L* $\rightarrow$ *(*$\forall$ *m n, (cardinal S m* $\wedge$ *cardinal (N S) n)* $\rightarrow$ *m <=n))* $\leftrightarrow$ *(*$\exists$ *R:Relation U, Included_in_Edge R* $\wedge$ *Is_L_Perfect R).*

- We only need to prove the forward direction.
- We create a poset by giving directions to the edges.The set of Left and Right vertices becomes antichains in the poset.

Hall's Marriage Theorem

Formal Statement in Coq

Theorem

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ *if and only if* $\exists$ *an L-perfect matching.*

Theorem (Halls_Thm: Formal statement)

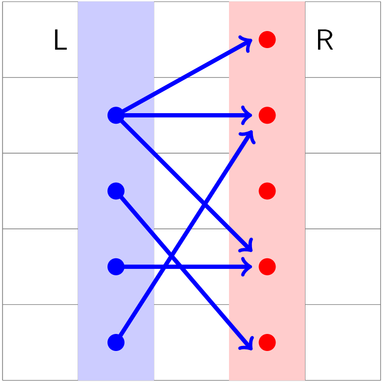
($\forall$S, Included S L $\rightarrow$ ($\forall$ m n, (cardinal S m $\wedge$ cardinal (N S) n) $\rightarrow$ m <=n)) $\leftrightarrow$ ($\exists$ R:Relation U, Included_in_Edge R $\wedge$ Is_L_Perfect R).

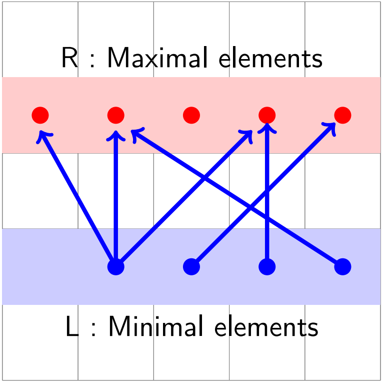
- We only need to prove the forward direction.
- We create a poset by giving directions to the edges.The set of Left and Right vertices becomes antichains in the poset.

Hall's Marriage Theorem

Disjoint Chain cover as an L-perfect matching

- Set of left (L) and right (R) vertices becomes minimal and maximal elements respectively.
- An L-perfect matching for the graph can be obtained from a disjoint chain cover for the poset.

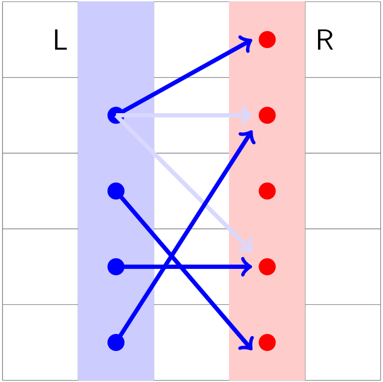


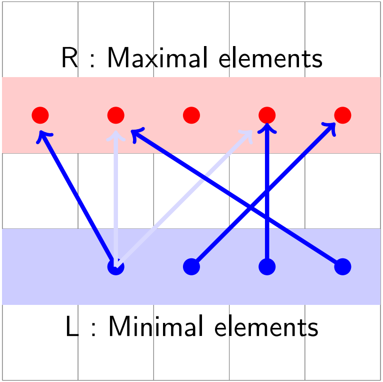


Hall's Marriage Theorem

Disjoint Chain cover as an L-perfect matching

- Set of left (L) and right (R) vertices becomes minimal and maximal elements respectively.
- An L-perfect matching for the graph can be obtained from a disjoint chain cover for the poset.





Hall's Marriage Theorem

Proof Idea: Bipartite graph as a poset

Theorem

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ if and only if $\exists$ an L-perfect matching.

- Assuming $\forall S \subset L, |N(S)| \geq |S|$ one can prove that R is the largest antichain in the poset.
- If m is the size of R then there exists a disjoint chain cover of size m for the poset.
- This disjoint chain cover for poset gives us an L-perfect matching for the Bipartite graph.

Hall's Marriage Theorem

Proof Idea: Bipartite graph as a poset

Theorem

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ if and only if $\exists$ an L-perfect matching.

- Assuming $\forall S \subset L, |N(S)| \geq |S|$ one can prove that R is the largest antichain in the poset.
- If m is the size of R then there exists a disjoint chain cover of size m for the poset.
- This disjoint chain cover for poset gives us an L-perfect matching for the Bipartite graph.

Hall's Marriage Theorem

Proof Idea: Bipartite graph as a poset

Theorem

For any Bipartite graph $G = (L, R, E), \forall S \subset L, |N(S)| \geq |S|$ if and only if $\exists$ an L-perfect matching.

- Assuming $\forall S \subset L, |N(S)| \geq |S|$ one can prove that R is the largest antichain in the poset.
- If m is the size of R then there exists a disjoint chain cover of size m for the poset.
- This disjoint chain cover for poset gives us an L-perfect matching for the Bipartite graph.

Sequences and The Erdős-Szekeres Theorem

Integer Sequences and Subsequences

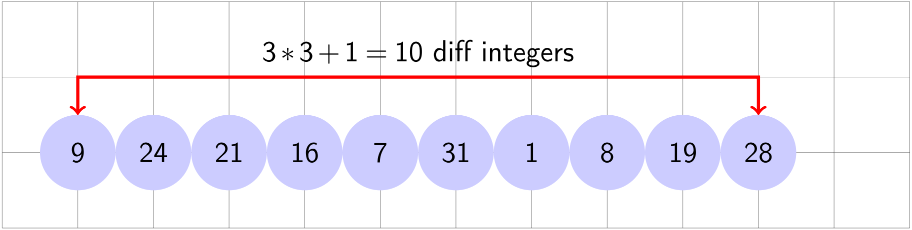
Theorem (The Erdős-Szekeres Theorem [3]:)

Every sequence of $m.n+1$ distinct integers contains an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$.

- increasing subsequence 9, 16, 19, 28.
- increasing subsequence 7, 8, 19, 28.
- decreasing subsequence 24, 21, 16, 7, 1.

Theorem (The Erdős-Szekeres Theorem [3]:)

Every sequence of $m.n+1$ distinct integers contains an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$.



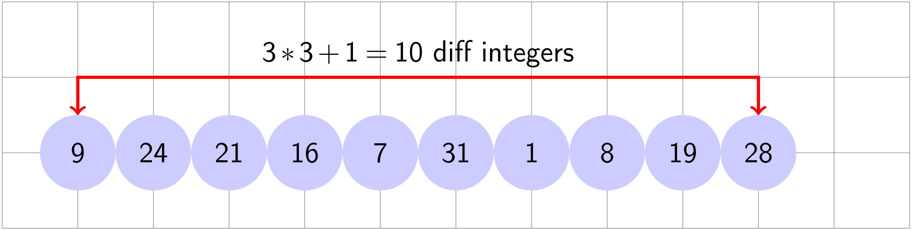
- increasing subsequence 9, 16, 19, 28.
- increasing subsequence 7, 8, 19, 28.
- decreasing subsequence 24, 21, 16, 7, 1.

Sequences and The Erdős-Szekeres Theorem

Integer Sequences and Subsequences

Theorem

Every sequence of $m.n+1$ distinct integers contains an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$.



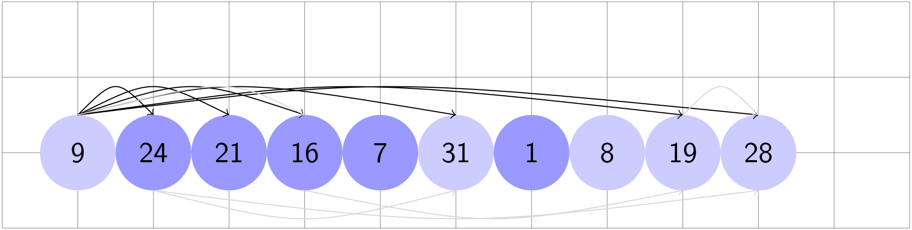
Theorem (Erdos_Szeker: Formal statement)

*∀ (s: Int_seq) m n, cardinal s (m*n+1) → ((∃ s1: Int_seq, sub_seq s1 s ∧ Is_increasing s1 ∧ cardinal s1 (m+1)) ∨ (∃ s2: Int_seq, sub_seq s2 s ∧ Is_decreasing s2 ∧ cardinal s2 (n+1))).*

Sequences and The Erdős-Szekeres Theorem

Proof Idea: Posets out of Integer Sequences

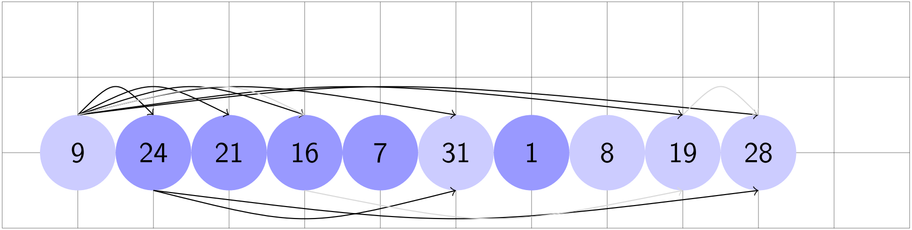
- We construct a poset $(s, \leq)$ where, for any two $x, y \in s$, $x \leq y$ iff x comes before y in the sequence s and x is less than y as numbers.
- A chain in this partial order $(s, \leq)$ is a monotonically increasing subsequence of the sequence s.
- An antichain in $(s, \leq)$ is a monotonically decreasing subsequence of the sequence s.



Sequences and The Erdős-Szekeres Theorem

Proof Idea: Posets out of Integer Sequences

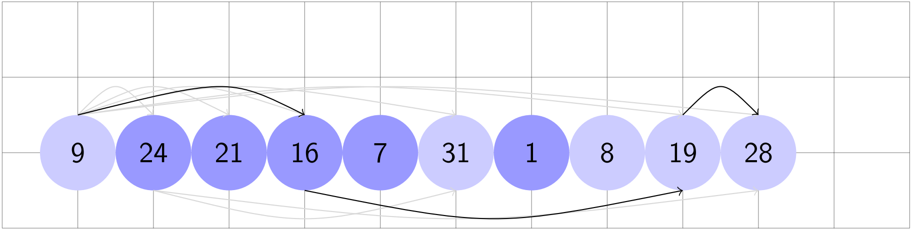
- We construct a poset $(s, \leq)$ where, for any two $x, y \in s$, $x \leq y$ iff x comes before y in the sequence s and x is less than y as numbers.
- A chain in this partial order $(s, \leq)$ is a monotonically increasing subsequence of the sequence s.
- An antichain in $(s, \leq)$ is a monotonically decreasing subsequence of the sequence s.



Sequences and The Erdős-Szekeres Theorem

Proof Idea: Posets out of Integer Sequences

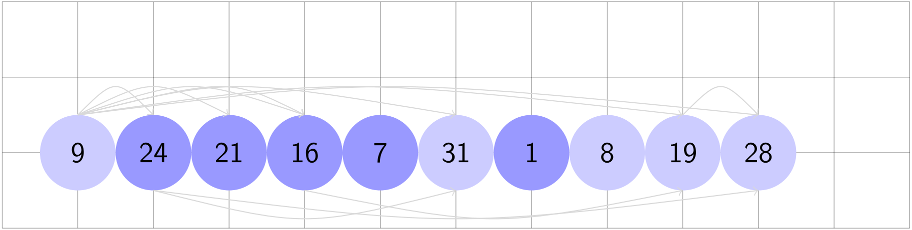
- We construct a poset $(s, \leq)$ where, for any two $x, y \in s$, $x \leq y$ iff x comes before y in the sequence s and x is less than y as numbers.
- A chain in this partial order $(s, \leq)$ is a monotonically increasing subsequence of the sequence s.
- An antichain in $(s, \leq)$ is a monotonically decreasing subsequence of the sequence s.



Sequences and The Erdős-Szekeres Theorem

Proof Idea: Posets out of Integer Sequences

- We construct a poset $(s, \leq)$ where, for any two $x, y \in s$, $x \leq y$ iff x comes before y in the sequence s and x is less than y as numbers.
- A chain in this partial order $(s, \leq)$ is a monotonically increasing subsequence of the sequence s.
- An antichain in $(s, \leq)$ is a monotonically decreasing subsequence of the sequence s.



Now, we can complete the proof of Erdős-Szekeres theorem by proving the following result on general posets,

Lemma (Pre_ES:)

If P is a poset with $m.n+1$ elements, then it has a chain of size at least $m+1$ or an antichain of size at least $n+1$.

- We prove this lemma using Dilworth's Decomposition theorem.

Future Work

- Removal of Excluded Middle (EM) and Choice axioms from the proofs.
  - Since all the structures involved are finite we can use decidable predicates.
  - Instead of using Ensemble Module of the Standard Library [1] one can use the Finite type and Finite set formalism of the Ssreflect library. It can be helpful in eliminating the use of EM and Choice Axioms.
- Mechanize other related results such as
  - Weak Perfect Graph Theorem and
  - Different forms of Konig's theorem on edge and vertex colouring of a Bipartite graph.

Future Work

- Removal of Excluded Middle (EM) and Choice axioms from the proofs.
  - Since all the structures involved are finite we can use decidable predicates.
  - Instead of using Ensemble Module of the Standard Library [1] one can use the Finite type and Finite set formalism of the Ssreflect library. It can be helpful in eliminating the use of EM and Choice Axioms.
- Mechanize other related results such as
  - Weak Perfect Graph Theorem and
  - Different forms of Konig's theorem on edge and vertex colouring of a Bipartite graph.

References

The Coq Standard Library.
https://coq.inria.fr/library/.

R. P. Dilworth.
A decomposition theorem for partially ordered sets.
In *Annals of Mathematics*, volume 51, pages 161–166, 1951.

P. Erdős and G. Szekeres.
A combinatorial problem in geometry.
In *Compositio Mathematica*, volume 2, pages 463–470, 1935.

Philip Hall.
On representations of subsets.
In *J. London Math. Soc.*, volume 10, pages 28–30, 1935.

Leon Mirsky.
A dual of Dilworth's decomposition theorem.
In *American Mathematical Monthly*, volume 78, pages 876–877, 1971.

Thank You