Formal Proof of Dilworth's Theorem

Vivek Soorya Maadoori S. M. Meesum Shiv Pillai
T. V. H. Prathamesh Aditya Swami

March 25, 2025

Abstract

A *chain* is defined as a totally ordered subset of a partially ordered set. A *chain cover* refers to a collection of chains of a partially ordered set whose union equals the entire set. A *chain decomposition* is a chain cover consisting of pairwise disjoint sets. An *antichain* is a subset of elements of a partially ordered set in which no two elements are comparable.

In 1950, Dilworth proved that in any finite partially ordered set, the cardinality of a largest antichain equals the cardinality of a smallest chain decomposition.[2]

In this paper, we formalise a proof of the theorem above, also known as *Dilworth's theorem*, based on a proof by Perles (1963) [3]. Our formalisation draws on the formalisation of Dilworth's theorem for chain covers in Coq by Abhishek Kr. Singh [4], and builds on the AFP entry containing formalisation of minimal and maximal elements in a set by Martin Desharnais [1]. Our formalisation extends the prior work in Coq by including a formal proof of Dilworth's theorem for chain decomposition.

Contents

theory *Dilworth*
imports *Main HOL.Complete-Partial-Order HOL.Relation HOL.Order-Relation Min-Max-Least-Greatest.Min-Max-Least-Greatest-Set*
begin

Note: The Dilworth's theorem for chain cover is labelled Dilworth and the extension to chain decomposition is labelled Dilworth_Decomposition.

context *order*
begin

1 Definitions

definition *chain-on* :: - *set* ⇒ - *set* ⇒ *bool* **where**
chain-on A S ⟷ ((*A* ⊆ *S*) ∧ (*Complete-Partial-Order.chain* (≤) *A*))

definition *antichain* :: - *set* ⇒ *bool* **where**
antichain S ⟷ (∀ *x* ∈ *S*. ∀ *y* ∈ *S*. (*x* ≤ *y* ∨ *y* ≤ *x*) ⟶ *x* = *y*)

definition *antichain-on* :: - *set* ⇒ - *set* ⇒ *bool* **where**
(*antichain-on A S*) ⟷
(*partial-order-on A* (*relation-of* (≤) *A*)) ∧ (*S* ⊆ *A*) ∧ (*antichain S*)

definition *largest-antichain-on*:: - *set* ⇒ - *set* ⇒ *bool* **where**
largest-antichain-on P lac ⟷
(*antichain-on P lac* ∧ (∀ *ac*. *antichain-on P ac* ⟶ *card ac* ≤ *card lac*))

definition *chain-cover-on*:: - *set* ⇒ - *set set* ⇒ *bool* **where**
chain-cover-on S cv ⟷ (⋃ *cv* = *S*) ∧ (∀ *x* ∈ *cv* . *chain-on x S*)

definition *antichain-cover-on*:: - *set* ⇒ - *set set* ⇒ *bool* **where**
antichain-cover-on S cv ⟷ (⋃ *cv* = *S*) ∧ (∀ *x* ∈ *cv* . *antichain-on S x*)

definition *smallest-chain-cover-on*:: - *set* ⇒ - *set set* ⇒ *bool* **where**
smallest-chain-cover-on S cv ≡
(*chain-cover-on S cv* ∧
(∀ *cv2*. (*chain-cover-on S cv2* ∧ *card cv2* ≤ *card cv*) ⟶ *card cv* = *card cv2*))

definition *chain-decomposition* **where**
chain-decomposition S cd ≡ ((*chain-cover-on S cd*) ∧
(∀ *x* ∈ *cd*. ∀ *y* ∈ *cd*. *x* ≠ *y* ⟶ (*x* ∩ *y* = {})))

definition *smallest-chain-decomposition*:: *- set* ⇒ *- set set* ⇒ *bool* **where**
smallest-chain-decomposition S cd
≡ (*chain-decomposition S cd*
∧ (∀ *cd2*. (*chain-decomposition S cd2* ∧ *card cd2* ≤ *card cd*)
⟶ *card cd* = *card cd2*))

2 Preliminary Lemmas

The following lemma shows that given a chain and an antichain, if the cardinality of their intersection is equal to 0, then their intersection is empty..

lemma *inter-nInf*:
assumes *a1*: *Complete-Partial-Order.chain* (⊆) *X*
and *a2*: *antichain Y*
and *asmInf*: *card* (*X* ∩ *Y*) = *0*
shows *X* ∩ *Y* = {}
⟨*proof*⟩

The following lemma shows that given a chain X and an antichain Y that both are subsets of S, their intersection is either empty or has cardinality one..

lemma *chain-antichain-inter*:
assumes *a1*: *Complete-Partial-Order.chain* (⊆) *X*
and *a2*: *antichain Y*
and *a3*: *X* ⊆ *S* ∧ *Y* ⊆ *S*
shows (*card* (*X* ∩ *Y*) = *1*) ∨ ((*X* ∩ *Y*) = {})
⟨*proof*⟩

Following lemmas show that given a finite set S, there exists a chain decomposition of S.

lemma *po-restr*: **assumes** *partial-order-on B r*
and *A* ⊆ *B*
shows *partial-order-on A* (*r* ∩ (*A* × *A*))
⟨*proof*⟩

lemma *eq-restr*: (*Restr* (*relation-of* (≤) (*insert a A*)) *A*) = (*relation-of* (≤) *A*)
(**is** *?P* = *?Q*)
⟨*proof*⟩

lemma *part-ord*:*partial-order-on S* (*relation-of* (≤) *S*)
⟨*proof*⟩

The following lemma shows that a chain decomposition exists for any finite set S.

lemma *exists-cd*: **assumes** *finite S*
shows ∃ *cd*. *chain-decomposition S cd*
⟨*proof*⟩

The following lemma shows that the chain decomposition of a set is a chain cover.

lemma *cd-cv*:
  assumes *chain-decomposition P cd*
  shows *chain-cover-on P cd*
  ⟨*proof*⟩

The following lemma shows that for any finite partially ordered set, there exists a chain cover on that set.

lemma *exists-chain-cover*: **assumes** *finite P*
  shows $\exists$ *cv*. *chain-cover-on P cv*
⟨*proof*⟩

lemma *finite-cv-set*: **assumes** *finite P*
  and $S = \{x.$ *chain-cover-on P x*$\}$
  shows *finite S*
⟨*proof*⟩

The following lemma shows that for every element of an antichain in a set, there exists a chain in the chain cover of that set, such that the element of the antichain belongs to the chain.

lemma *elem-ac-in-c*: **assumes** *a1*: *antichain-on P ac*
  and *chain-cover-on P cv*
  shows $\forall\ a \in ac.\ \exists\ c \in cv.\ a \in c$
⟨*proof*⟩

For a function f that maps every element of an antichain to some chain it belongs to in a chain cover, we show that, the co-domain of f is a subset of the chain cover.

lemma *f-image*: **fixes** *f* :: - ⇒ - *set*
  assumes *a1*: (*antichain-on P ac*)
  and *a2*: (*chain-cover-on P cv*)
  and *a3*: $\forall\, a \in ac.\ \exists\ c \in cv.\ a \in c \wedge f\ a = c$
  shows $(f\ `\ ac) \subseteq cv$
⟨*proof*⟩

3 Size of an antichain is less than or equal to the size of a chain cover

The following lemma shows that given an antichain ac and chain cover cv on a finite set, the cardinality of ac will be less than or equal to the cardinality of cv.

lemma *antichain-card-leq*:
  assumes (*antichain-on P ac*)
  and (*chain-cover-on P cv*)

and *finite P*
shows *card ac* $\leq$ *card cv*
⟨*proof*⟩

4 Existence of a chain cover whose cardinality is the cardinality of the largest antichain

4.1 Preliminary lemmas

The following lemma shows that the maximal set is an antichain.

lemma *maxset-ac*: *antichain* ($\{x$. *is-maximal-in-set P x*$\}$)
⟨*proof*⟩

The following lemma shows that the minimal set is an antichain.

lemma *minset-ac*: *antichain* ($\{x$. *is-minimal-in-set P x*$\}$)
⟨*proof*⟩

The following lemma shows that the null set is both an antichain and a chain cover.

lemma *antichain-null*: *antichain* $\{\}$
⟨*proof*⟩

lemma *chain-cover-null*: **assumes** $P = \{\}$ **shows** *chain-cover-on P* $\{\}$
⟨*proof*⟩

The following lemma shows that for any arbitrary x that does not belong to the largest antichain of a set, there exists an element y in the antichain such that x is related to y or y is related to x.

lemma *x-not-in-ac-rel*: **assumes** *largest-antichain-on P ac*
and $x \in P$
and $x \notin ac$
and *finite P*
shows $\exists\ y \in ac.\ (x \leq y) \vee (y \leq x)$
⟨*proof*⟩

The following lemma shows that for any subset Q of the partially ordered P, if the minimal set of P is a subset of Q, then it is a subset of the minimal set of Q as well.

lemma *minset-subset-minset*:
assumes *finite P*
and $Q \subseteq P$
and $\forall\ x.$ (*is-minimal-in-set P x* $\longrightarrow x \in Q$)
shows $\{x$. *is-minimal-in-set P x*$\} \subseteq \{x.$ *is-minimal-in-set Q x*$\}$
⟨*proof*⟩

The following lemma show that if P is not empty, the minimal set of P is not empty.

lemma *non-empty-minset*: **assumes** *finite P*
and $P \neq \{\}$
shows $\{x\ .\ \textit{is-minimal-in-set}\ P\ x\} \neq \{\}$
⟨*proof*⟩

The following lemma shows that for all elements m of the minimal set, there exists a chain c in the chain cover such that m belongs to c.

lemma *elem-minset-in-chain*: **assumes** *finite P*
and *chain-cover-on P cv*
shows *is-minimal-in-set P a* $\longrightarrow (\exists\ c \in cv.\ a \in c)$
⟨*proof*⟩

The following lemma shows that for all elements m of the maximal set, there exists a chain c in the chain cover such that m belongs to c.

lemma *elem-maxset-in-chain*: **assumes** *finite P*
and *chain-cover-on P cv*
shows *is-maximal-in-set P a* $\longrightarrow (\exists\ c \in cv.\ a \in c)$
⟨*proof*⟩

The following lemma shows that for a given chain cover and antichain on P, if the cardinality of the chain cover is equal to the cardinality of the antichain then for all chains c of the chain cover, there exists an element a of the antichain such that a belongs to c.

lemma *card-ac-cv-eq*: **assumes** *finite P*
and *chain-cover-on P cv*
and *antichain-on P ac*
and *card cv = card ac*
shows $\forall\ c \in cv.\ \exists\ a \in ac.\ a \in c$
⟨*proof*⟩

The following lemma shows that if an element m from the minimal set is in a chain, it is less than or equal to all elements in the chain.

lemma *e-minset-lesseq-e-chain*: **assumes** *chain-on c P*
and *is-minimal-in-set P m*
and $m \in c$
shows $\forall\ a \in c.\ m \leq a$
⟨*proof*⟩

The following lemma shows that if an element m from the maximal set is in a chain, it is greater than or equal to all elements in the chain.

lemma *e-chain-lesseq-e-maxset*: **assumes** *chain-on c P*
and *is-maximal-in-set P m*
and $m \in c$
shows $\forall\ a \in c.\ a \leq m$
⟨*proof*⟩

The following lemma shows that for any two elements of an antichain, if they both belong to the same chain in the chain cover, they must be the same element.

lemma *ac-to-c* : **assumes** *finite P*
and *chain-cover-on P cv*
and *antichain-on P ac*
shows $\forall\ a \in ac.\ \forall\ b \in ac.\ \exists\ c \in cv.\ a \in c \wedge b \in c \longrightarrow a = b$
⟨*proof*⟩

The following lemma shows that for two finite sets, if their cardinalities are equal, then their cardinalities would remain equal after removing a single element from both sets.

lemma *card-Diff1-eq*: **assumes** *finite A*
and *finite B*
and *card A* $=$ *card B*
shows $\forall\ a \in A.\ \forall\ b \in B.\ card\ (A - \{a\}) = card\ (B - \{b\})$
⟨*proof*⟩

The following lemma shows that for two finite sets A and B of equal cardinality, removing two unique elements from A and one element from B will ensure the cardinality of A is less than B.

lemma *card-Diff2-1-less*: **assumes** *finite A*
and *finite B*
and *card A* $=$ *card B*
and $a \in A$
and $b \in A$
and $a \neq b$
shows $\forall\ x \in B.\ card\ ((A - \{a\}) - \{b\}) < card\ (B - \{x\})$
⟨*proof*⟩

The following lemma shows that for all elements of a partially ordered set, there exists an element in the minimal set that will be less than or equal to it.

lemma *min-elem-for-P*: **assumes** *finite P*
shows $\forall\ p \in P.\ \exists\ m.$ *is-minimal-in-set* $P\ m \wedge m \leq p$
⟨*proof*⟩

The following lemma shows that for all elements of a partially ordered set, there exists an element in the maximal set that will be greater than or equal to it.

lemma *max-elem-for-P*: **assumes** *finite P*
shows $\forall\ p \in P.\ \exists\ m.$ *is-maximal-in-set* $P\ m \wedge p \leq m$
⟨*proof*⟩

The following lemma shows that if the minimal set is not considered as the largest antichain on a set, then there exists an element a in the minimal set such that a does not belong to the largest antichain.

lemma *min-e-nIn-lac*: **assumes** *largest-antichain-on P ac*
and $\{x.$ *is-minimal-in-set P x*$\} \neq ac$
and *finite P*
shows $\exists\, m.$ (*is-minimal-in-set P m*) $\wedge$ $(m \notin ac)$
(**is** $\exists\, m.$ (*?ms m*) $\wedge$ $(m \notin ac)$)
⟨*proof*⟩

The following lemma shows that if the maximal set is not considered as the largest antichain on a set, then there exists an element a in the maximal set such that a does not belong to the largest antichain.

lemma *max-e-nIn-lac*: **assumes** *largest-antichain-on P ac*
and $\{x$. *is-maximal-in-set P x*$\} \neq ac$
and *finite P*
shows $\exists$ *m* . *is-maximal-in-set P m* $\wedge$ $m \notin ac$
(**is** $\exists$ *m*. *?ms m* $\wedge$ $m \notin ac$)
⟨*proof*⟩

4.2 Statement and Proof

Proves theorem for the empty set.

lemma *largest-antichain-card-eq-empty*:
assumes *largest-antichain-on P lac*
and $P = \{\}$
shows $\exists$ *cv*. (*chain-cover-on P cv*) $\wedge$ (*card cv* = *card lac*)
⟨*proof*⟩

Proves theorem for the non-empty set.

lemma *largest-antichard-card-eq*:
assumes *asm1*: *largest-antichain-on P lac*
and *asm2*: *finite P*
and *asm3*: $P \neq \{\}$
shows $\exists$ *cv*. (*chain-cover-on P cv*) $\wedge$ (*card cv* = *card lac*)
⟨*proof*⟩

5 Dilworth's Theorem for Chain Covers: Statement and Proof

We show that in any partially ordered set, the cardinality of a largest antichain is equal to the cardinality of a smallest chain cover.

theorem *Dilworth*:
assumes *largest-antichain-on P lac*
and *finite P*
shows $\exists$ *cv*. (*smallest-chain-cover-on P cv*) $\wedge$ (*card cv* = *card lac*)
⟨*proof*⟩

6 Dilworth's Decomposition Theorem

6.1 Preliminaries

Now we will strengthen the result above to prove that the cardinality of a smallest chain decomposition is equal to the cardinality of a largest antichain. In order to prove that, we construct a preliminary result which states that cardinality of smallest chain decomposition is equal to the cardinality of smallest chain cover.

We begin by constructing the function make_disjoint which takes a list of sets and returns a list of sets which are mutually disjoint, and leaves the union of the sets in the list invariant. This function when acting on a chain cover returns a chain decomposition.

fun *make-disjoint*::- *set list* ⇒ -
 where
 make-disjoint [] = ([])
|*make-disjoint* (*s*#*ls*) = (*s* − (⋃ (*set ls*)))#(*make-disjoint ls*)

lemma *finite-dist-card-list*:
 assumes *finite S*
 shows ∃ *ls*. *set ls* = *S* ∧ *length ls* = *card S* ∧ *distinct ls*
 ⟨*proof*⟩

lemma *len-make-disjoint*:*length xs* = *length* (*make-disjoint xs*)
 ⟨*proof*⟩

We use the predicate *list-all2* (⊆), which checks if two lists (of sets) have equal length, and if each element in the first list is a subset of the corresponding element in the second list.

lemma *subset-make-disjoint*: *list-all2* (⊆) (*make-disjoint xs*) *xs*
 ⟨*proof*⟩

lemma *subslist-union*:
 assumes *list-all2* (⊆) *xs ys*
 shows ⋃ (*set xs*) ⊆ ⋃ (*set ys*)
 ⟨*proof*⟩

lemma *make-disjoint-union*:⋃ (*set xs*) = ⋃ (*set* (*make-disjoint xs*))
⟨*proof*⟩

lemma *make-disjoint-empty-int*:
 assumes *X* ∈ *set* (*make-disjoint xs*) *Y* ∈ *set* (*make-disjoint xs*)
 and *X* ≠ *Y*
shows *X* ∩ *Y* = {}
 ⟨*proof*⟩

lemma *chain-subslist*:
assumes $\forall\, i < length\ xs.\ Complete\text{-}Partial\text{-}Order.chain\ (\leq)\ (xs!i)$
and *list-all2* $(\subseteq)$ *ys xs*
shows $\forall\, i < length\ ys.\ Complete\text{-}Partial\text{-}Order.chain\ (\leq)\ (ys!i)$
⟨*proof*⟩

lemma *chain-cover-disjoint*:
assumes *chain-cover-on P* (*set C*)
shows *chain-cover-on P* (*set* (*make-disjoint C*))
⟨*proof*⟩

lemma *make-disjoint-subset-i*:
assumes $i < length\ as$
shows $(make\text{-}disjoint\ (as))!i \subseteq (as!i)$
⟨*proof*⟩

Following theorem asserts that the corresponding to the smallest chain cover on a finite set, there exists a corresponding chain decomposition of the same cardinality.

lemma *chain-cover-decompsn-eq*:
assumes *finite P*
and *smallest-chain-cover-on P A*
shows $\exists\ B.\ chain\text{-}decomposition\ P\ B \wedge card\ B = card\ A$
⟨*proof*⟩

lemma *smallest-cv-cd*:
assumes *smallest-chain-decomposition P cd*
and *smallest-chain-cover-on P cv*
shows $card\ cv \leq card\ cd$
⟨*proof*⟩

lemma *smallest-cv-eq-smallest-cd*:
assumes *finite P*
and *smallest-chain-decomposition P cd*
and *smallest-chain-cover-on P cv*
shows $card\ cv = card\ cd$
⟨*proof*⟩

6.2 Statement and Proof

We extend the Dilworth's theorem to chain decomposition. The following theorem asserts that size of a largest antichain is equal to the size of a smallest chain decomposition.

theorem *Dilworth-Decomposition*:
assumes *largest-antichain-on P lac*
and *finite P*
shows $\exists\ cd.\ (smallest\text{-}chain\text{-}decomposition\ P\ cd) \wedge (card\ cd = card\ lac)$

⟨*proof*⟩

end

end

Acknowledgement

We would like thank Divakaran D. for valuable suggestions.

References

[1] M. Desharnais. Minimal, maximal, least, and greatest elements w.r.t. restricted ordering. *Archive of Formal Proofs*, October 2024. https://isa-afp.org/entries/Min_Max_Least_Greatest.html, Formal proof development.

[2] R. P. Dilworth. A decomposition theorem for partially ordered sets. *Annals of Mathematics*, 51(1):161–166, 1950.

[3] M. A. Perles. A proof of dilworths decomposition theorem for partially ordered sets. *Israel Journal of Mathematics*, 1:105–107, 1963.

[4] A. K. Singh. Fully mechanized proofs of dilworths theorem and mirskys theorem. *arXiv preprint arXiv:1703.06133*, 2017.