Kalpa Publications in Computing

Volume XXX, 2017, Pages 1–15

LPAR 21. Selected Workshop and Short Presentations

Formalization of some central theorems in combinatorics of finite sets

Abhishek Kr Singh

School of Technology and Computer Science,
Tata Institute of Fundamental Research, Mumbai
abhishek.singh@tifr.res.in

Abstract

We present fully formalized proofs of some central theorems from combinatorics. These are Dilworth's decomposition theorem, Mirsky's theorem, Hall's marriage theorem and the Erdős-Szekeres theorem. Dilworth's decomposition theorem is the key result among these. It states that in any finite partially ordered set (poset), the size of a smallest chain cover and a largest antichain are the same. Mirsky's theorem is a dual of Dilworth's decomposition theorem, which states that in any finite poset, the size of a smallest antichain cover and a largest chain are the same. We use Dilworth's theorem in the proofs of Hall's Marriage theorem and the Erdős-Szekeres theorem. The combinatorial objects involved in these theorems are sets and sequences. All the proofs are formalized in the Coq proof assistant. We develop a library of definitions and facts that can be used as a framework for formalizing other theorems on finite posets.

1 Introduction

Formalization of any mathematical theory is a difficult task because the length of a formal proof blows up significantly. In combinatorics the task becomes even more difficult due to the lack of structure in the theory. Some statements often admit more than one proof using completely different ideas. Thus, exploring dependencies among important results may help in identifying an effective order amongst them. Dilworth's decomposition theorem, first proved by R. P. Dilworth[6] in 1951, is a well-known result in combinatorics. It states that in any finite partially ordered set (poset) the size of a smallest chain cover and a largest antichain are the same. Since then, the theorem attracted significant attention and several new proofs [15, 19, 8] were discovered. In addition to being an important structural result on posets, Dilworth's Theorem can be used to give intuitive and concise proofs of some other important results in combinatorics such as Hall's Theorem [10, 11, 4], the Erdős-Szekeres Theorem [7], and Konig's Theorem [3].

In this paper we present a fully formalized proof of Dilworth's decomposition theorem. Among the several proofs available we follow the proof by Perles [15] due to its clean and concise reasoning steps. We then mechanize proofs of Hall's Marriage theorem [11, 4] and the Erdős-Szekeres theorem [7]. Proofs that we mechanize for these theorems essentially use Dilworth's decomposition theorem. In these proofs a finite poset is constructed from the objects involved and then Dilworth's decomposition theorem is applied to obtain the result. These proofs are explained in detail in Section 3-4. We also formalize a dual of Dilworth's Theorem (Mirsky's Theorem [14]) which relates the size of an antichain cover and a chain in a poset.

Formalization of known mathematical results can be traced back to the systems Automath and Mizar [9]. Mizar hosts the largest repository of formalized mathematics. Mizar system also supports some built in automation to save time during proof development. However, this results in a large kernel (core) and reduces our faith in the system. The Coq proof assistant[13, 5] deals with this problem in a novel way. It separates the process of proof development from proof checking. Some small scale proof automation is also possible in Coq. However, every proof process finally yields a proof-term which is verified using a small kernel. Thus the part (kernel) of the code we need to trust remains small. All the results discussed in this paper are fully formalized in the Coq proof assistant. In addition to a small kernel, the Coq proof assistant also has some other useful features such as *dependent records* and *coercions*. Dependent records are used to pack mathematical objects and their properties in one definition. For example, in the Coq standard library different components of a partial order and their properties are expressed using a single definition of dependent record (PO). Similarly, coercions can be used to define a hierarchy among mathematical structures. This avoids redefining similar things at different places. The Coq system also hosts a standard library [2] that contains a large collection of useful definitions and results. We use this facility and avoid new definitions unless absolutely essential.

In this paper, we present the details of our mechanized proofs of Dilworth's, Mirsky's, Hall's, and the Erdős-Szekeres theorems. All the terms that appear in the formal statement of these theorems are explained in Section 2 and Sections 4-6. The exact definitions of these terms in Coq are listed in Section A (Appendix). Description of some useful results on sets and posets appears in Section 3. Finally, we review related work in Section 7 and conclude in Section 8.

2 Definitions

Once a statement is proved in Coq, the proof is certified without having to go through the proof-script. It is however necessary to verify whether the statement being proved correctly represents the original theorem. Therefore the number of new definitions needed to understand the theorem statement should be small. We have attempted to achieve this by reusing the definitions from the Coq standard Library whenever possible. In this section we explain the definitions of all the terms which appear in the formal statements of Dilworth's and Mirsky's Theorem.

2.1 Definitions from the Standard Library

The Coq Standard Library[2] is well documented. We have used the *Sets* module from the Standard Library, where a declaration S: Ensemble U is used to represent a set S.

- Sets are treated as predicates, i.e, $x \in S$ iff S x is provable.
- Set membership is written as In S x instead of just writing S x.
- The Empty set is defined as a predicate Empty_set which is not provable anywhere. Singleton x and Couple x y represent the sets $\{x\}$ and $\{x, y\}$ respectively.

A Partial Order is defined as a record type in the Coq standard library. It has four fields,

```
Record PO (U : Type) : Type := Definition_of_PO {
    Carrier_of : Ensemble U;
    Rel_of : Relation U;
    PO_cond1 : Inhabited U Carrier_of;
    PO_cond2 : Order U Rel_of }.
```

For example, consider the following declaration,

```
Variable U:Type.
```

```
Variable P: PO U.
```

It creates a record P of type PO U. Here P can be treated as a poset with four fields. The first field of P is accessed using the term Carrier_of _ P. It represents the carrier set of P. The second field represents binary relation ≤ of the partially ordered set P. It is accessed using the term Rel_of _ P. The term PO_cond1 _ P is a proof that the carrier set of P is a non-empty set. Similarly, the term PO_cond2 _ P is a proof that ≤ is an order (i.e, reflexive, transitive and antisymmetric).

2.2 New Definitions

Coercions and Finite partial orders

We extend the definition of poset to define *finite partial orders* (FPO) as a dependent record,

```
Record FPO (U : Type) : Type := Definition_of_FPO {
    PO_of :> PO U ;
    FPO_cond : Finite _ (Carrier_of _ PO_of ) }.
```

It has two components; a partial order and a proof that the carrier set of the partial order is finite. Here, FPO is defined as a dependent record which inherits all the fields of type PO. Note the use of coercion symbol :> in defining the first field of the record FPO. Here, PO_of acts as a function and is applied automatically to any term of type FPO that appears in a context where a term of type PO is expected. Hence, from now onward we can use an object of type FPO in any context where an object of type PO is expected.

Chains and antichains as predicates

In the Coq Standard Library a chain is defined as a poset whose carrier set is totally ordered.

```
Record Chain : Type := Definition_of_chain {
    PO_of_chain : PO U;
    Chain_cond : Totally_ordered U PO_of_chain (@Carrier_of _ PO_of_chain)}.
```

However, using this definition it becomes difficult to say that a given set is a chain in two different posets. In the proof of Dilworth's theorem we frequently refer to a set in the context of two different posets and wish to claim that the set is totally ordered in both the posets. Thus we use a different definition for chain. A chain is defined using a predicate Is_a_chain_in. For a finite partial order P: FPO U on some type U let, C := Carrier_of U P and R:= Rel_of U P. Then,

```
Definition Is_a_chain_in (e: Ensemble U): Prop:= (Included U e C /\ Inhabited U e) /\ (∀
    x y:U, (Included U (Couple U x y) e) → R x y \/ R y x).
```

Here, a *chain* is a subset of P any two of whose elements are comparable. A subset of P in which no two distinct elements are comparable is called an *antichain.* An antichain is defined using the predicate Is_an_antichain_in. Note that, a chain and an antichain can have at most one element in common. In a similar way we also define the following notions,

- A *chain cover* is a collection of chains whose union is the entire poset.
- An *antichain cover* is a collection of antichains such that their union is the entire poset.
- The *width* of a poset P, $width(P)$, is the size of a largest antichain in P.
- The *height* of a poset, $height(P)$, is the size of a largest chain in P.
- An element $b \in P$ is called a *maximal element* if there is no $a \in P$ such that $b \leq a$.
- An element $a \in P$ is called a *minimal element* if there is no $b \in P$ such that $b \leq a$.

The exact definitions that we use for these terms are listed in Section A(Appendix).

3 Some useful results on sets and posets

In this section we explain some general results on finite partial orders. These results are used at more than one place in the formal proofs of these theorems. They are proved as Lemmas and compiled in separate files. Most of the Lemma's statements can be inferred from their names. These Lemmas appear with the same name in the actual Coq files. Here we only provide an English description of some of them.

Existence proofs

A large number of lemmas are concerned with the existence of a defined object. For example, in our proof when we say "Let A be an antichain of the poset P..." we assume that there exists an antichain for the poset P. However, in a formal system like Coq, we need a proof of existence of such an object before we can instantiate it. Following is a partial list of such results:

Lemma-1 *Chain_exists*: There exists a chain in every finite partial order (FPO).
Proof. Trivial.

Lemma-2 *Chain_cover_exists:* There exists a chain cover for every FPO.
Proof. Trivial.

Lemma-3 *Minimal_element_exists:* The set minimal(P) is non-empty for every P: FPO.
Proof. Using induction on the size of P.

Lemma-4 *Maximal_element_exists:* The set maximal(P) is non-empty for every P: FPO.
Proof. Using induction on the size of P.

Lemma-5 *Largest_element_exists:* If a finite partial order is also totally ordered then there exists a largest element in it.
Proof. The maximal element becomes the largest element and we know that there exists a maximal element.

Lemma-6 *Minimal_for_every_y:* For every element y of a finite partial order P there exists an element x in P such that $x \leq y$ and $x \in$ minimal(P).
Proof. Let $X = \{x : P | \, x \leq y\}$. Then the poset $(X, \leq)$ will have a minimal element, say x_0. It is also a minimal element of P.

Lemma-7 *Maximal_for_every_x:* For every element x of a finite partial order P there exists an element y in P such that $x \leq y$ and $y \in$ maximal(P).
Proof. Let $Y = \{y : P | \, x \leq y\}$. Then the poset $(Y, \leq)$ will have a maximal element, say y_m. It is also a maximal element of P.

Lemma-8 *Largest_set_exists:* There exists a largest set (by cardinality) in a finite and non-empty collection of finite sets.
Proof. Consider the collection of sets together with the strict set-inclusion relation. This forms a finite partial order. Any maximal element of this finite partial order will be a largest set. Moreover, such a maximal element exists due to Lemma-4.

Lemma-9 *exists_largest_antichain:* In every finite partial order there exists a largest antichain.
Proof. Note that this statement is not true for partial orders. The proof is similar to Lemma-8.

Lemma-10 *exists_largest_chain:* In every finite partial order there exists a largest antichain.
Proof. Again, it is true only for finite partial orders. Proof is similar to Lemma-8.

Some other proofs

When dealing with sets the set-inclusion relation occurs more naturally than the comparison based on the set sizes. Therefore, we defined a binary relations *Inside* (or $\prec$) on the collection of all the finite partial orders.

- We say $P_1 \prec P_2$ iff carrier set of P_1 is strictly included in the carrier set of P_2 and both the posets are defined on the same binary relation.

In order to use well-founded induction we proved that the relation $\prec$ is well founded.

Lemma-11 *Inside_is_WF:* The binary relation Inside (i.e, $\prec$) is well founded on the set of all finite partial orders.
Proof. Using strong induction on the size of finite partial orders.

Lemma-12 *Largest_antichain_remains:* If $\mathcal{A}$ is a largest antichain of P_2 and $P_1 \prec P_2$ then $\mathcal{A}$ is also a largest antichain in P_1 provided $\mathcal{A} \subset P_1$.
Proof. Assume otherwise, then there will be a larger antichain say $\mathcal{A}'$ in P_1. This will also be larger in P_2, which contradicts.

Lemma-13 *NoTwoCommon:* A chain and an antichain can have at most one element in common.
Proof. Trivial.

Lemma-14 *Minimal_is_antichain:* Minimal(P) is an antichain in P.
Proof. Trivial.

Lemma-15 *Maximal_is_antichain:* Maximal(P) is an antichain in P.
Proof. Trivial.

Lemma-17 *exists_ disjoint_ cover:* If $\mathcal{C}_{\mathcal{V}}$ is a smallest chain cover of size m for P, then there also exists a disjoint chain cover $\mathcal{C}_{\mathcal{V}}'$ of size m for P.
Proof. Using induction on m.

Lemma-18 *Largest_ chain_ has_ maximal:* In any finite poset P, maximal(P) shares an element with every largest chain of P.
Proof. First we observe that every chain in a finite poset has a largest element. We prove that this element is also in maximal(P).

Lemma-19 *Largest_ chain_ has_ minimal:* In any finite poset P, minimal(P) shares an element with every largest chain of P.
Proof. Similar to the proof of Lemma-18.

Lemma-20 *Pre_ ES:* If P is a poset with $r.s+1$ elements, then it has a chain of size $r+1$ or an antichain of size $s+1$.
Proof. There can be two cases; either there is an antichain $\mathcal{A}$ of size $s+1$ or the size of a largest antichain is s. In the first case statement is trivially true. In the second case, using Dilworth's theorem we know that there exists a chain cover $\mathcal{C}_{\mathcal{V}}$ of size s. Since $\mathcal{C}_{\mathcal{V}}$ covers the whole poset P and its size is $r.s+1$, there must be an chain of size at least $r+1$ in $\mathcal{C}_{\mathcal{V}}$.

4 Mirsky's theorem and Dilworth's decomposition theorem

4.1 Mirsky's theorem

Mirsky's theorem relates the size of an antichain cover and a chain in a poset. The definitions we have seen so far are sufficient to express the formal statement of Mirsky's theorem in Coq.

Theorem Dual_Dilworth: ∀ (P: FPO U), Dual_Dilworth_statement P.

where, Dual_Dilworth_statement is defined as,

Definition Dual_Dilworth_statement:= fun (P: FPO U) ⇒ ∀ (m n: nat), (Is_height P m) → (∃ cover: Ensemble (Ensemble U), (Is_a_smallest_antichain_cover P cover) /\ (cardinal _ cover n)) → m=n.

It states that in any poset the maximum size of a chain is equal to the minimum number of antichains in any antichain cover. In other words, if $c(P)$ represents the size of a smallest antichain cover of P, then $height(P) = c(P)$.
Proof : The equality will follow if one can prove:

1. Size of a chain ≤ Size of an antichain cover, and

2. There is an antichain cover of size equal to $height(P)$.

It is easy to see why (1) is true. Any chain shares at most one element with each antichain from an antichain cover. Moreover, every element of the chain must be covered by some antichain from the antichain cover. Hence, the size of any chain is smaller than or equal to the size of any antichain cover.

We will prove (2) using strong induction on the size of the largest chain of P. Let m be the size of the largest chain in P, i.e, $m = height(P)$.

- Induction hypothesis: For all posets P' of height at most $m-1$, there exists an antichain cover of size equal to $height(P')$.

Induction Step: Let M denote the set of all maximal elements of P, i.e, M = maximal(P). Observe that M is a non-empty antichain and shares an element with every largest chain of P. Consider now the partially ordered set $(P-M, \leq)$. The length of the largest chain in $P-M$ is at most $m-1$. On the other hand, if the length of the largest chain in $P-M$ is less than $m-1$, M must contain two or more elements that are members of the same chain, which is a contradiction. Hence, we conclude that the length of largest chain in $P-M$ is $m-1$. Using induction hypothesis there we get an antichain cover $\mathcal{A}_\mathcal{C}$ of size $m-1$ for $P-M$. Thus, we get an antichain cover $\mathcal{A}_\mathcal{C} \cup \{M\}$ of size m for P. □

Note that in the induction step of the above proof we assume that maximal(P) shares an element with every largest chain of P. However, in the formal setting we need a proof of this fact. It is proved as Lemma-18 in Section 3.

4.2 Dilworth's decomposition theorem

Dilworth's decomposition theorem is the central result in our formalization. It relates the size of a chain cover and an antichain in a poset. We prove the following formal statement,

Theorem Dilworth: ∀ (P: FPO U), Dilworth_statement P.

where Dilworth_statement is defined as,

Definition Dilworth_statement:= fun (P: FPO U)⇒ ∀ (m n: nat), (Is_width P m) → (∃ cover: Ensemble (Ensemble U), (Is_a_smallest_chain_cover P cover) /\ (cardinal _ cover n)) → m=n.

It states that in any poset, the maximum size of an antichain is equal to the minimum number of chains in any chain cover. In other words, if $c(P)$ represents the size of a smallest chain cover of P, then $width(P) = c(P)$.

The statement of Dilworth's theorem appears dual to the statement of Mirsky's theorem. However, the proof of Dilworth's theorem is more involved. The key idea in proving Mirsky's theorem was to identify an antichain which intersects every largest chain (Lemma-18). It is however not easy to identify a chain in a poset which intersects every largest antichain. This is the main difficulty in translating the proof of Mirsky's theorem to a proof of Dilworth's theorem. Therefore, we mechanize a different proof of Dilworth's theorem due to Perles[15].

Proof (Perles): The equality $width(P) = c(P)$ will follow if one can prove:

1. Size of an antichain $\leq$ Size of a chain cover, and
2. There is a chain cover of size equal to $width(P)$.

Again, it is easy to see why (1) is true. Assume otherwise, i.e., there is an antichain $\mathcal{A}$ of size bigger than the size of a smallest chain cover $\mathcal{C}_\mathcal{V}$. Then $\mathcal{A}$ will have more elements than the number of chains in $\mathcal{C}_\mathcal{V}$. Hence, there must exist a chain $\mathcal{C}$ in $\mathcal{C}_\mathcal{V}$ which covers two elements of $\mathcal{A}$. However, this cannot be true since a chain and an antichain (in this case $\mathcal{C}$ and $\mathcal{A}$) can have at most one element in common.

Proof of (2) is more involved. We will prove (2) using strong induction on the size of P. Let m be the size of the largest antichain in P, i.e., $m = width(P)$.

- Induction hypothesis: For all posets P' of size at most n, there exists a chain cover of size equal to $width(P')$.

Induction step: Fix a poset P of size at most $n+1$. Let maximal(P) and minimal(P) represent respectively the set of all maximal and the set of all minimal elements of P. Now, one of the following two cases might occur,

1. There exists an antichain $\mathcal{A}$ of size m which is neither maximal(P) nor minimal(P).

2. No antichain other than maximal(P) or minimal(P) has size m.

Case-1: For the first case we define the sets P^+ and P^- as follows:

$$P^+ = \{x \in P : x \geq y \text{ for some } y \in \mathcal{A}\}$$
$$P^- = \{x \in P : x \leq y \text{ for some } y \in \mathcal{A}\}$$

Here P^+ captures the notion of being above $\mathcal{A}$ and P^- captures the notion of being below $\mathcal{A}$. Note that the elements of $\mathcal{A}$ are both above and below $\mathcal{A}$, i.e, $\mathcal{A} \subseteq P^+ \cap P^-$. For any arbitrary element $x \in P$

- If $x \in A$ then $x \in P^+ \cap P^-$ and hence $x \in P^+ \cup P^-$.

- If $x \notin \mathcal{A}$ then x must be comparable to some element in $\mathcal{A}$; otherwise $\{x\} \cup \mathcal{A}$ will be an antichain of size $m+1$. Hence, if $x \notin \mathcal{A}$ then $x \in P^+ \cup P^-$.

Therefore, $P^+ \cup P^- = P$. Since there is at least one minimal element not in $\mathcal{A}$, $P^+ \neq P$. Similarly $P^- \neq P$. Thus $|P^+| < |P|$ and $|P^-| < |P|$, hence we will be able to apply induction hypothesis to them. Observe that $\mathcal{A}$ is also a largest antichain in the poset restricted to P^+; because if there was a larger one, it would have been larger in P also. Therefore by induction there exists a chain cover of size m for P^+, say $P^+ = \cup_{i=1}^m C_i$. Similarly, there is a chain cover of size m for P^-, say $P^- = \cup_{i=1}^m D_i$.

Elements of $\mathcal{A}$ are the minimal elements of the chains C_i and the maximal elements of the chains D_i. Therefore we can join the chains C_i and D_i together in pairs to form m chains which form a chain cover for the original poset P.

Case-2: In this case we can't have an antichain of size m which is different from both maximal(P) and minimal(P). Consider a minimal element x. Choose a maximal element y such that $x \leq y$. Such a y always exists. Remove the chain $\{x, y\}$ from P to get the poset P'. Then P' contains an antichain of size $m-1$. Also note that P' can't have an antichain of size m. Because if there was an antichain of size m in P', then that would also be an antichain in P which is different from both maximal(P) and minimal(P), and we would have been in the first case (i.e., Case-1). Hence by induction hypothesis we get a chain decomposition of P' of size $m-1$. These chains, together with $\{x, y\}$, give a decomposition of P into m chains. □

We mechanize the above proof in Coq with a slight modification. Instead of using induction on the cardinality of posets we use well-founded induction on the strict set-inclusion relation. When working with the Ensemble module of the Coq standard library it is easy to deal with the set-inclusion relation compared to the comparison based on set cardinalities. Thus, we defined a binary relations *Inside* (or $\prec$) on the collection of all the finite partial orders.

- We say $P_1 \prec P_2$ iff carrier set of P_1 is strictly included in the carrier set of P_2 and both the posets are defined on the same binary relation.

Then to use well-founded induction we proved that the relation $\prec$ is well founded. This is explained as Lemma-11 in Section 3.

In the formalization of above proofs we use the principle of excluded middle at many places. At certain points, we also need to extract functions from relations. Therefore, we import the *Classical* and *ClassicalChoice* modules of the standard library, which assumes the following three axioms:

Axiom classic : ∀ P:Prop, P \/ ~ P.

Axiom dependent_unique_choice : ∀ (A:Type) (B:A → Type) (R:∀ x:A, B x → Prop), (∀ x : A, ∃! y : B x, R x y) →(∃ f : (∀ x:A, B x), ∀ x:A, R x (f x)).

Axiom relational_choice : ∀ (A B : Type) (R : A→B→Prop), (∀ x : A, ∃ y : B, R x y) → ∃ R' : A→B→Prop, subrelation R' R /\ ∀ x : A, ∃! y : B, R' x y.

5 Hall's Marriage Theorem

5.1 Bipartite graphs

A bipartite graph is a triple (L, R, E) where $L \cap R = \phi$, and E consists of pairs from $L \times R$. Elements of $L \cup R$ are called vertices and elements of E are called edges. Here, we consider only finite bipartite graphs. In Coq, we define it as a dependent record.

```
Record Bipar_Graph: Type := Def_of_BG {
    Graph_of_BG:> Finite_Graph ;
    L_of: Ensemble U;
    R_of: Ensemble U;
    LR_Inhabited: Inhabited _ L_of /\ Inhabited _ R_of;
    LR_Disj: Disjoint _ L_of R_of;
    LR_Union: Vertices_of (Graph_of_BG ) = (Union _ L_of R_of);
    LR_Rel: ∀ x y: U, (Edge_Rel_of (Graph_of_BG )) x y → (In _ L_of x /\ In _ R_of
    y) }.
```

Edges are defined as a binary relation on the vertices.

- The neighborhood of a set $S \subset L$, denoted $N(S)$, is the set of all those vertices that are in some edge containing a vertex from S, i.e.,
$N(S) = \{v \in R : \exists u \in L, (u, v) \in E\}$.

- A matching is a collection of disjoint edges, i.e., no two edges in a matching have a common vertex.

- A matching is said to be L-perfect if each vertex in L is part of some edge of the matching.

In Coq we define these terms as N (S), Is_a_matching and Is_L_Perfect. The exact definitions appear in Section A(Appendix).

5.2 Hall's Marriage Theorem

Let $G = (L, R, Edge)$ be a bipartite graph and $V = L \cup R$. Then we have,

Theorem Halls_Thm: (∀(S: Ensemble U), Included _ S L → (∀ m n :nat,(cardinal _ S m /\ cardinal _ (N S) n) → m <=n)) ↔ (∃ Rel:Relation U, Included_in_Edge Rel /\ Is_L_Perfect Rel).

where, Included_in_Edge is defined as,

Definition Included_in_Edge (Rel: Relation U): Prop := ∀ x y:U, Rel x y → Edge x y.

It states that, for any bipartite graph $G = (L, R, E)$, $\forall S \subset L$, $|N(S)| \geq |S|$ if and only if ∃ an L-perfect matching.
Proof : We prove the "only if" (forward direction) part of the theorem, the "if" part being trivial. Once we have Dilworth's theorem, a proof of Hall's theorem follows rather easily. Turn the bipartite graph (L, R, E) into a poset $\mathcal{P}$ whose elements are vertices of $L \cup R$ and the relation is the reflexive closure of the edge relation. One can imagine the bipartite graph as the Hasse diagram of poset $\mathcal{P}$.

First, we prove that R is a largest antichain. Fix any antichain $\mathcal{A} = \mathcal{A_L} \cup \mathcal{A_R}$ where $\mathcal{A_L}, \mathcal{A_R}$ are in L, R respectively. Now, $N(\mathcal{A_L})$ is disjoint from $\mathcal{A_R}$ as $\mathcal{A}$ is an antichain. Hence, $|\mathcal{A}| = |\mathcal{A_L}| + |\mathcal{A_R}| \leq |N(\mathcal{A_L})| + |\mathcal{A_R}| \leq |R|$. Here the first inequality follows from the hypothesis $\forall S \subset L$, $|S| \leq |N(S)|$.

Now, from Dilworth's theorem, there is a chain cover $\mathcal{C}$ of size $|R|$. Without loss of generality, the chains in $\mathcal{C}$ are disjoint. Each chain has to have an element of R. If we restrict attention to the two element chains in $\mathcal{C}$, they form an L-perfect matching. □

Note that in the above proof Dilworth's theorem only assures the existence of a chain cover $\mathcal{C}$ of size $|R|$. However, we claim that without loss of generality the chains in $\mathcal{C}$ are disjoint. This is a hidden assumption and needs a justification in the formal proof. Just by looking at the informal proof of Hall's theorem one might consider proving the following statement which justifies the claim,

- In any finite poset P, if $\mathcal{C}$ is a chain cover of size $|R|$ then there exists a disjoint chain cover $\mathcal{C}'$ of size $|R|$.

It however turns out that the above statement is too strong. For example, let $P = (C, R)$ be a poset where $C = \{a, b, c\}$ and R is the reflexive and transitive closure of the binary relation $R' = \{(a, b)\}$. Now consider $\mathcal{C} = \{\{a\}, \{b\}, \{c\}, \{a, b\}\}$, it is clearly a chain cover of size 4. However, there can't be a disjoint chain cover of size 4 for the poset P. Therefore, we consider the following weaker statement,

- In any finite poset P, if $\mathcal{C}$ is a smallest chain cover of size $|R|$ then there exists a disjoint chain cover $\mathcal{C}'$ of size $|R|$.

This statement is proved as Lemma-17 in Section 3. Since Dilworth's theorem assures the existence of a smallest chain cover $\mathcal{C}$ of size $|R|$ we use Lemma-17 in the formal proof of Hall's Marriage theorem to justify the existence of a disjoint chain cover.

Sequence of distinct representative (SDR)

The Hall's theorem on bipartite graph can be used to prove the original form of Hall's theorem which talks about the representation of each set in a collection of finite sets. Let $S = \{S_1, \ldots, S_n\}$ be a family of sets and $X = \underset{i \leq n}{\cup} S_i$.

- A sequence of distinct representatives (SDR) for S is a sequence $\{x_1, \ldots, x_n\}$ of pairwise distinct elements of X such that $x_i \in S_i, 1 \leq i \leq n$.

Hall's Marriage theorem then states that,

- S has an SDR iff the union of any k members of S contains at least k elements.

The above result easily follows from Hall's theorem on graphs. Consider the bipartite graph (S, X, E) where E consists of all the pairs (S_i, a_i) where a_i is a member of set S_i. An L-perfect matching in this graph corresponds to an SDR for S and the neighborhood $N(S)$ becomes $\bigcup_{S_i \in S} S_i$. Hence the above statement gets transformed to the statement of Hall's theorem on graphs.

We closely follow this line of reasoning to prove the SDR version of Hall's theorem in Coq. However, instead of considering a sequence of distinct representatives we consider a relation that assures the SDR criterions. It reduces the overheads of dealing with sequences. In this setting we have,

Theorem The_Halls_Thm: exists_a_one_one_map ↔ union_is_at_least_m.

where,

exists_a_one_one_map is an abbreviation for, (∃ Rel': Ensemble U → U→ Prop, (∀ (x:Ensemble U) (y:U), Rel' x y → In _ x y) /\ (∀ (x y:Ensemble U) (z: U), (Rel' x z /\ Rel' y z)→ x=y) /\ (∀ x: Ensemble U, In _ S x → (∃ y: U, Rel' x y))) and,

union_is_at_least_m is an abbreviation for, (∀ S': Ensemble (Ensemble U), Included _ S' S → (∀ m n:nat, (cardinal _ S' m /\ cardinal _ (Union_over S') n) → m<= n))

Note that the existence of such a relation Rel' assures the existence of a one-one map from S to X. Moreover, Rel' is contained in the set membership relation; because Rel' x y → In _ x y. Hence, the existence of such relation implies the existence of an SDR and vice-versa.

6 Sequences and the Erdős-Szekeres Theorem

6.1 Finite Sequence of Integers

A sequence $(C, \prec)$ consists of a non-empty set C together with a binary relation $\prec$ satisfying asymmetry and transitivity properties. Moreover, any two distinct elements of C must be related with this ordering relation. Note the difference with partial orders, the relation $\prec$ is asymmetric instead of being antisymmetric. This means for any two elements $a, b \in C$, $a \prec b \rightarrow \sim b \prec a$. We define a sequence of integers in Coq as a dependent record,

```
Record Int_seq:Type:= Def_of_seq {
    C_of: Ensemble nat;
    R_of: Relation nat;
    Seq_cond1: Inhabited _ (C_of);
    Seq_cond2: Finite _ (C_of);
    Seq_cond3: Transitive _ R_of;
    Seq_cond4: Asymmetric _ R_of;
    Seq_cond5: Total_Order R_of C_of ; }.
```

Since we are working only with finite sequences we declare it as Seq_cond2 in the definition of Int_seq.

6.2 The Erdős-Szekeres Theorem

For a finite sequence s: Int_seq we prove,

Theorem Erdos_Szeker: ∀ m n, cardinal (C_of s) (m*n+1) → ((∃ s1: Int_seq, sub_seq s1 s /\ Is_increasing s1 /\ cardinal (C_of s1) (m+1)) \/ (∃ s2: Int_seq, sub_seq s2 s /\ Is_decreasing s2 /\ cardinal (C_of s2) (n+1))).

Here Is_increasing and Is_decreasing capture the notions of increasing and decreasing sequences respectively. That s1 is a subsequence of s2 is represented by predicate sub_seq s1 s2. The exact definitions of these terms are given in Section A(Appendix).

The Erdős-Szekeres theorem then states that for any two natural numbers m and n, every sequence of $m.n + 1$ distinct integers contains an increasing subsequence of length $m + 1$ or a decreasing subsequence of length $n + 1$.

Proof: Let $(C, \prec)$ be the sequence where $|C| = m.n + 1$. To prove this theorem, we construct a poset $(C, \leq)$ where for any two $x, y \in C$, $x \leq y$ iff $x \prec y$ and x is less than y as numbers. Note that,

- A chain in this partial order $(C, \leq)$ is a monotonically increasing subsequence in $(C, \prec)$, and
- An antichain in $(C, \leq)$ is a monotonically decreasing subsequence in $(C, \prec)$.

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

- 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 $n + 1$.

This statement is proved as Lemma-20 in Section 3. It follows easily from the Dilworth's theorem. There can be two cases; either there is an antichain $\mathcal{A}$ of size $n + 1$ or the size of a largest antichain is n. In the first case statement is trivially true. In the second case, using Dilworth's theorem we know that there exists a chain cover $\mathcal{C_V}$ of size n. Since $\mathcal{C_V}$ covers the whole poset P and its size is $m.n + 1$, there must be a chain of size at least $m + 1$ in $\mathcal{C_V}$. This completes the proof. □

Wrapping Up

This work is done in the Coq Proof General (Version 4.4pre). We have used the Company-Coq extension [16] for the Proof General. The Coq code for this work is available at [1]. The code is split into different files. *BasicFacts.v* and *BasicFacts2.v* contains some useful properties on numbers and sets. *PigeonHole.v* contains some variants of the Pigeonhole Principle. Most of the definitions and results on finite partial orders are proved in *FPO_Facts.v*, *FPO_Facts2.v* and *FPO_Facts3.v*. Proofs of Dilworth's theorem and Mirsky's theorems appear in the files *FiniteDilworth.v* and *Dual_Dilworth.v* respectively. *Halls_Thm.v* contains the proof of Hall's theorem on bipartite graphs. The second form of Hall's theorem on sequence of distinct representatives (SDR) is proved in *Marriage_Thm.v*. Proof of the Erdős-Szekeres theorem appears in *Erdos_Szeker.v*.

7 Related Work

Rudnicki [18] presents a formalization of Dilworth's decomposition theorem in Mizar. In the same paper they also provide a proof of the Erdős-Szekeres theorem using Dilworth's theorem. A separate proof of the Hall's marriage theorem in Mizar appeared in [17]. Jiang and Nipkow [12] also presented two different proofs of Hall's theorem in Isabelle/HOL. We have used a different theorem prover and formalized all of these results in a single framework. Our work is closest to the work of [18]. However, we added extra results (Hall's theorem) in the same framework. The proof we mechanize for Hall's theorem uses Dilworth's theorem and we formalize Hall's theorem in both of its popular forms. The first form deals with the matching in a bipartite graph and the second form is about sequence of distinct representatives (SDR) for a collection of finite sets. We also provide a clear compilation of some useful results on finite sets and posets that can be used for mechanizing other important results from the combinatorics of finite structures.

8 Conclusions

Formalization of any mathematical theory involves significant time and effort because the size of formal proofs blows up significantly. In such circumstances exploring dependencies among important results might save some time and effort. Dilworth's decomposition theorem is an important result on partially ordered sets (poset). It has been used successfully to give concise proofs of some other important results from combinatorics. Here we use Dilworth's theorem on posets to mechanize proofs of two other well known results on sets and sequences. The main contributions of this paper are:

1. Fully formalized proofs of Dilworth's decomposition theorem and Mirsky's theorem in Coq, together with an explanation of all the definitions and the theorem statement.

2. Fully mechanized proofs of Hall's Marriage theorem and the Erdős-Szekeres theorem using Dilworth's decomposition theorem.

3. A clear compilation of some general results and definitions which could be used as a framework in the formalization of other similar results.

The Coq code for this work is available at [1]. One can further explore the dependencies of these mechanized results with other well known results in combinatorics. It can save a lot of time and effort in mechanizing their proofs.

Acknowledgements

We are thankful to Mohit Garg for explaining these proofs and motivating us to formalize them.

References

[1] Dilworth, Halls and Erdos-Szekeres theorem in Coq. `http://www.tcs.tifr.res.in/~abhishek/`.

[2] The Coq Standard Library. `https://coq.inria.fr/library/`.

[3] Wikipedia: Kőnig's theorem (graph theory).

[4] Martin Aigner and Gűnter M. Ziegler. *Proofs from THE BOOK (4th ed.)*. Springer Publishing Company.

[5] Y. Bertot and P. Castéran. *Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

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

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

[8] F. Galvin. A proof of Dilworth's chain decomposition theorem. In *American Mathematical Monthly*, volume 101, pages 352–353, 1994.

[9] H. Geuvers. Proof assistants: History, ideas and future. In *Sadhana*, volume 34, pages 3–25, 2009.

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

[11] Paul R. Halmos and Herber E Vaughan. The marriage problem. In *American Journal of Mathematics*, volume 72, pages 214–215, 1950.

[12] D. Jiang and Tobias Nipkow. Proof pearl: The marriage theorem. In *Certified Programs and Proofs: First International Conference, CPP 2011, Kenting, Taiwan, December 7-9, 2011. Proceedings*, pages 394–399. Springer Berlin Heidelberg, 2011.

[13] The Coq development team. *The Coq proof assistant reference manual*, 2016. Version 8.5.

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

[15] M. A. Perles. A proof of Dilworth's decomposition theorem for partially ordered sets. In *Israel J. Math*, pages 105–107, 1963.

[16] Clément Pit-Claudel and Pierre Courtieu. Company-coq: Taking proof general one step closer to a real ide. In *CoqPL'16: The Second International Workshop on Coq for PL*, 2016.

[17] E. Romanowicz and Adam Grabowski. The Hall's marriage theorem. In *Formalized Mathematics*, volume 12, pages 315–320, 2004.

[18] P. Rudnicki. Dilworth's decomposition theorem for posets. In *Formalized Mathematics*, volume 17, pages 223–232, 2009.

[19] H. Tverberg. On Dilworth's decomposition theorem for partially ordered sets. In *J. Combin. theory*, pages 305–306, 1967.

A Appendix

Partial Orders, chains and antichains

For a finite partial order P: FPO U on some type `U` let,
C := Carrier_of U P and,
R:= Rel_of U P.
Then, we have the following definitions:

1. Definition *Is_a_chain_in* (e: Ensemble U): Prop:= (Included U e C /\ Inhabited U e) /\ (∀ x y:U, (Included U (Couple U x y) e) → R x y \/ R y x).

2. Definition *Is_an_antichain_in* (e: Ensemble U): Prop := (Included U e C /\ Inhabited U e) /\ (∀ x y:U, (Included U (Couple U x y) e) → (R x y \/ R y x) → x=y).

3. Inductive *Is_largest_chain_in* (e: Ensemble U): Prop:= largest_chain_cond: Is_a_chain_in e → (∀ (e1: Ensemble U) (n n1:nat), Is_a_chain_in e1 → cardinal _ e n → cardinal _ e1 n1 → n1 ≤ n) → Is_largest_chain_in e.

4. Inductive *Is_largest_antichain_in* (e: Ensemble U): Prop:= largest_antichain_cond: Is_an_antichain_in e → (∀ (e1: Ensemble U) (n n1: nat), Is_an_antichain_in e1 → cardinal _ e n → cardinal _ e1 n1 → n1 ≤ n) → Is_largest_antichain_in e.

5. Inductive *Is_ a_ chain_ cover*(cover:Ensemble(Ensemble U)): Prop:= cover_cond: (∀ (e: Ensemble U), In _ cover e → Is_a_chain_in e) → (∀ x:U, In _ C x → (∃ e: Ensemble U, In _ cover e /\ In _ e x)) → Is_a_chain_cover cover.

6. Inductive *Is_ an_ antichain_ cover* (cover: Ensemble (Ensemble U)): Prop:= AC_cover_cond: (∀ (e: Ensemble U), In _ cover e → Is_an_antichain_in e) → (∀ x:U, In _ C x → (∃ e: Ensemble U, In _ cover e /\ In _ e x)) → Is_an_antichain_cover cover.

7. Inductive *Is_ a_ smallest_ chain_ cover* (scover: Ensemble (Ensemble U)): Prop:= smallest_cover_cond: (Is_a_chain_cover P scover) → (∀(cover: Ensemble (Ensemble U)) (sn n: nat), (Is_a_chain_cover P cover /\ cardinal _ scover sn /\ cardinal _ cover n) → (sn ≤ n)) → Is_a_smallest_chain_cover P scover.

8. Inductive *Is_ a_ smallest_ antichain_ cover* (scover: Ensemble (Ensemble U)): Prop:= smallest_cover_cond_AC: (Is_an_antichain_cover P scover) → (∀(cover: Ensemble (Ensemble U)) (sn n: nat), (Is_an_antichain_cover P cover /\cardinal _ scover sn /\ cardinal _ cover n) → (sn ≤ n)) → Is_a_smallest_antichain_cover P scover.

9. Inductive *Is_ height* (n: nat) : Prop:= H_cond: (∃ lc: Ensemble U, Is_largest_chain_in P lc /\ cardinal _ lc n) → (Is_height P n).

10. Inductive *Is_ width* (n: nat) :Prop := W_cond: (∃ la: Ensemble U, Is_largest_antichain_in P la /\ cardinal _ la n) → (Is_width P n).

Bipartite graphs and matching

1. Definition *N* (S: Ensemble U): Ensemble U:= fun (y: U) ⇒ ∃ x:U, In _ S x /\ Edge x y.

2. Definition *Is_ a_ matching* (R: Relation U): Prop:= (∀ x y z: U, ((R x z /\ R y z)\/ (R z x /\ R z y)) → x=y).

3. Definition *Is_ L_ Perfect* (Rel: Relation U): Prop:= (Is_a_matching Rel /\ (∀ x: U, In _ L x → (∃ y: U, Rel x y))).

Increasing and decreasing subsequences

1. Definition *Asymmetric* := fun (U : Type) (R : Relation U) ⇒ ∀ x y : U, R x y → ~ R y x.

2. Definition *Total_ Order* (U:Type)(R: Relation U)(S: Ensemble U): Prop:= ∀ s1 s2, (In _ S s1 /\ In _ S s2) → (R s1 s2 \/ R s2 s1).

3. Definition *sub_ seq* (s1 s2: Int_seq): Prop:= Included _ (C_of s1) (C_of s2)/\ (∀ m n, (In _ (C_of s1) m /\ In _ (C_of s1) n) → R_of s1 m n → R_of s2 m n).

4. Definition *Is_ increasing* (s: Int_seq): Prop:= ∀ m n, (In _ (C_of s) m /\ In _ (C_of s) n) → R_of s m n → m < n.

5. Definition *Is_ decreasing* (s: Int_seq): Prop:= ∀ m n, (In _ (C_of s) m /\ In _ (C_of s) n) → R_of s m n → m > n.