CS 735: Formal Methods for Concurrent and Asynchronus Systems **Spring 2018**

Guest Lecture: March 6 2018

Instructor: Prof. Akshay S. *Scribes: Jatin Arora, Shaan Vaidya*
Guest Lecturer: Prof. Alain Finkel

Disclaimer:[1] *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

1.1 Introduction

A large class of safety properties can be reduced to the coverability problem, which is decidable for WSTS under some effectivity assumptions. One of the ways to check coverability is the backward coverability algorithm which computes a finite basis of the set $\uparrow Pre^*(\uparrow s)$. Another approach would be to try to come up with a forward reachability algorithm via which we can check the membership of the state, whose coverability is to be decided, in the set $\downarrow Post^*(\downarrow s)$. This set is also more useful because it characterizes a good approximation of the reachability set. This method is more difficult in theory because unlike upward closed sets, downward closed sets cannot always be defined by a finite basis. In this report, we show that a downward closed set can be decomposed into a finite union of *ideals* which are introduced below and can be used for forward coverability. We start with some definitions.

1.2 Ideals

Definition 1.2.1. *(**Ideal**) A non-empty set $I \subseteq X$ is an ideal if*

- *I is downward closed i.e. $I = \downarrow I$*
- *I is directed i.e. $a, b \in X \Rightarrow \exists c \in X$ st $a \leq c$ and $b \leq c$*

The set of all ideals of X are denoted by Ideals(X).

Example 1.2.1. *An ideal $I \in Ideals(\mathbb{N})$ is either the set $\mathbb{N}$ itself or of the form $\downarrow a$ for some $a \in \mathbb{N}$*

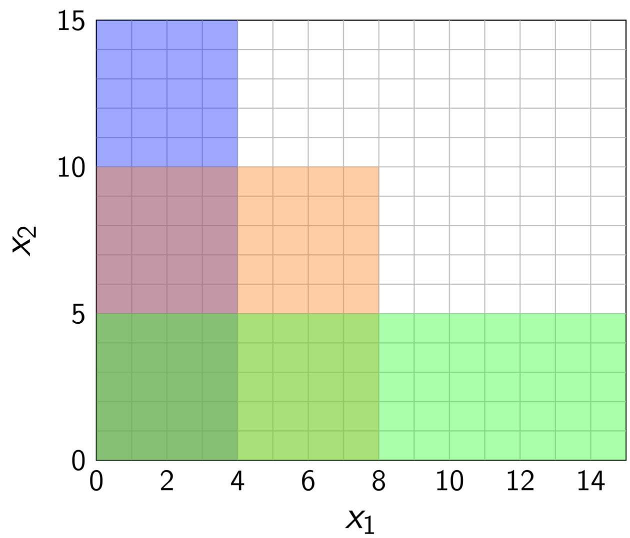
Example 1.2.2. *Note that*

$$Ideals(\mathbb{N}^d) = \underbrace{Ideals(\mathbb{N}) \times Ideals(\mathbb{N}) \times \cdots \times Ideals(\mathbb{N})}_{d\ times}$$

Consider the downward closed set (Verify!) $X = \{(x, y) \in \mathbb{N}^2 : (x \leq 4) \vee (x \leq 8 \wedge u \leq 10) \vee (y \leq 5)\}$. Observe that (see figure)

$$X = \downarrow 4 \times \mathbb{N} \cup \downarrow 8 \times \downarrow 10 \cup \mathbb{N} \times \downarrow 5$$

[1]**Note**: *LaTeX template courtesy of UC Berkeley EECS dept.*



Definition 1.2.2. *(X, ≤) is FAC if all antichains in X are finite.*

1.3 The Erdös & Tarski Theorem

Lemma 1.1. *Let $D =\downarrow D \subseteq X$ and $(X, \leq)$ be a wqo. Then $D = I_1 \cup I_2 \dots I_m$ where $I_1, \dots, I_m \in$ Ideals(X)*

Proof. We prove the above lemma by using contradiction and extremality. Suppose there exists a downward closed subset of D which cannot be decomposed into a finite set of ideals. We say that such sets are "bad". We claim that this also means that there will exist a minimal such D. Starting with $D_0 = D$, we consider $D_i \subset D_{i-1}$ such that D_i is bad. Also consider the sequence $\{x_i\}$ st $x_i \in D_{i-1}$ but $x_i \notin D_i$, this is possible since $D_i \subset D_{i-1}$. Now note that $x_i \not\leq x_j$ $\forall i < j$, because $x_j \in D_{j-1}$ and $x_i \notin D_{j-1}$ $(x_i \notin D_i)$. Therefore, if the sequence $\{D_k\}$ is infinite, we have an infinite sequence $\{x_k\}$ which satisfies $\forall i, j$ $i < j \Rightarrow x_i \not\leq x_j$. This is a contradiction since X is a wqo.
Since D is not an ideal itself $\exists x_1, x_2 \in D$ such that for any element $c \in D$, $x_1 \leq c$ and $x_2 \leq c$ does not hold. Now, consider two downward closed sets $D_p = D \backslash \uparrow x_1$ and $D_q = D \backslash \uparrow x_2$. Since D was a minimal bad set, D_p and D_q can be expressed as a finite union of ideals and so can $D_p \cup D_q$(say D'). We have $D' \neq D$ since D is bad and D' is not. In other terms, $D' = D \setminus \uparrow x_1 \cap \uparrow x_2$ and hence $\uparrow x_1 \cap \uparrow x_2 \neq \emptyset$. Any element $d \in D \cap \uparrow x_1 \cap \uparrow x_2$ satisfies $x_1 \leq d$ and $x_2 \leq d$ which is a contradiction since $d \in D$.

□

Theorem 1.2. *(The Erdös & Tarski Theorem) $(X, \leq)$ is FAC $\Leftrightarrow \forall D =\downarrow D \subseteq X$, $D = I_1 \cup I_2 \dots I_m$ where $I_1, \dots, I_m \in Ideals(X)$*

Proof. We will concern ourselves with the particular case where X is countable.
$\Longrightarrow$
We prove this direction by using the previous lemma. The main idea is to construct a well-founded downward-closed equivalent subset $D^{'} \subseteq D$ and then use the lemma.
Let $d_0, d_1, \dots, d_n, \dots$ be an infinite enumeration of D (countability of X). Let $D_0 \overset{def}{=} D$. Now, for $i \geq 0$, we take the *first element* $e_i \in D_i$ in the enumeration of D, and then define $D_{i+1} \overset{def}{=} D_i \backslash \downarrow e_i$. Observe that

(1) $\forall i,\ e_i \not\leq e_0, e_1, \ldots, e_{i-1}$. Finally, define $D^{'} \stackrel{def}{=} \{e_i : i \in \mathbb{N}\}$. Consider $(D^i, \leq^{'})$ where $\leq^{'}$ is the subset of $\leq$ restricted to $D^{'}$. $(D^i, \leq^{'})$ is of course FAC $(D^i \subseteq X)$. Suppose that $D^{'}$ contains an infinitely decreasing sequence $e_{i_0} > e_{i_1} > \cdots > e_{i_k} > \ldots$. Since this is an infinite sequence, $\exists k, i_0 < i_k$ and due to (1), we have $e_{i_0} \not\geq e_{i_k}$. Thus, we have a contradiction and so $(D^i, \leq^{'})$ is well-founded and therefore, a wqo. Using the previous lemma, $\exists I_1, ..., I_k \in Ideals(D^{'}, \leq^{'})$ $st \downarrow^{'} D^{'} = \bigcup_{i=1}^{k} I_i$ where $\downarrow^{'}$ denotes the $\leq^{'}$-downward closure.
Now, $\downarrow D^{'} \subseteq D$ ($D^{'} \subseteq D$ and $D = \downarrow D$). Let $x \in D$, by construction of $D^{'}$, $y \leq e_i \in D^{'}$ for some $i \in \mathbb{N}$ i.e. either y is one of the $e_i^{'}s$ or it is in some $\downarrow e_i$ and hence, $y \in \downarrow e_i \subseteq \downarrow D^{'}$. Thus, $D \subseteq \downarrow D^{'}$ and therefore, $D = \downarrow D^{'}$. Now,

$$D = \downarrow D^{'} = \downarrow (\bigcup_{i=1}^{k} I_i) = \bigcup_{i=1}^{k} (\downarrow I_i)$$

If we can prove that $\downarrow I_i$ is a directed set wrt $\leq$, we are done. Let $a, b \in \downarrow I_i$, $\exists a^{'}, b^{'} \in I_i$ such that $a \leq a^{'}$ and $b \leq b^{'}$. Since $I_i \in Ideals(D^{'}, \leq^{'})$ and therefore is directed, $\exists c \in I_i$ st $a^{'} \leq^{'} c$ and $b^{'} \leq^{'} c$. Hence, $\exists c \in \downarrow I_i$ st $a \leq a^{'} \leq c$ and $b \leq b^{'} \leq c$. Thus, $\downarrow I_i$ is directed and $\downarrow I_i \in Ideals(X, \leq)$. Thus, D can be written as a finite union of ideals.

$\Longleftarrow$
Given $\forall D = \downarrow D \subseteq X$, $\exists I_1, \ldots, I_m \in Ideals(X, \leq)$ st $D = \bigcup_{i=1}^{m} I_i$. Suppose X is not FAC. Let $A \subseteq X$ be an infinite antichain. Let $D \stackrel{def}{=} \downarrow A$. Since $D = \downarrow D \subseteq X$, we have, $D = \downarrow A$ can be written as a finite union of ideals i.e. $\exists I_1, \ldots, I_m \in Ideals(X, \leq)$ st $D = \bigcup_{i=1}^{m} I_i$. Now, $\exists i \leq m$ st I_i contains infinitely many elements of A (By PHP). Let $a \neq b \in I_i \cap A$. Since I_i is directed, $\exists c \in I_i$ st $a \leq c$ and $b \leq c$. Also, since $c \in I_i \subseteq \downarrow A$, $\exists c^{'} \in A$ st $c \leq c^{'}$. Therefore, $a \leq c^{'}$ and $b \leq c^{'}$. Since $a \neq b$, $a^{'}$ can be equal to a or b but never both (of course, it can be not equal to both). Therefore, in each case we have b and $a^{'}$, a and $a^{'}$, a and $a^{'}$ respectively pairs of elements in A that are *comparable*. Hence, A is not an antichain. We have a contradiction and therefore X is FAC. $\square$

1.4 A useful corollary

We will now prove a useful corollary to the Erdös & Tarski theorem. But first, let's prove the following lemma.

Lemma 1.3. *If $I \subseteq \bigcup_{i=1}^{n} J_i$ where $I, J_1, \ldots, J_n \in Ideals(X, \subseteq)$ then $\exists k$ such that $I \subseteq J_k$*

Proof. We prove the above lemma by using induction on the number of ideals whose union is considered. The base case ($n = 1$) is trivially true. Suppose the above property holds for $n = k$.
Now consider $n = k + 1$. Consider the following three cases.

1. Case: $I \subseteq J_{k+1}$
2. Case: $I \cap J_{k+1} = \emptyset$
   In this case $I \subseteq \bigcup_{i=1}^{k} J_i$ and by the inductive hypothesis $\exists l\ I \subseteq J_l$
3. Case: $I \cap J_{k+1} \neq \emptyset$ and $I \not\subseteq J_{k+1}$
   Consider two elements $x, y \in I$ such that $x \in J_{k+1}$ and $y \notin J_{k+1}$. The case assumptions are sufficient

for existence of such an x and y. Since x and y belong to an ideal I, $\exists c \in I$ such that $x \leq c$ and $y \leq c$. Now c cannot belong to J_{k+1} because then all elements less than it must also belong to J_{k+1}. Hence $\exists l \leq k$ st $c \in J_l$ which in turn implies $x \in J_l$. Therefore for any $x \in J_{k+1}$ and $x \in I$ $\exists l \leq k$ such that $x \in J_l$. This means that we do not need J_{k+1} for the union to be a superset of I because any element of I that is there in J_{k+1} is also present in some other ideal J_l. Hence, $I \subseteq \bigcup_{i=1}^{k} J_i$ and the inductive hypothesis is applicable.

The above three cases are exhaustive and exclusive and the hypothesis has been proven in all three of them, so the proof is complete.

Note that, due to this lemma, testing the inclusion of an ideal I in a union $\bigcup_{i=1}^{k} J_i$ of ideals reduces to testing whether $I \subseteq J_j$ for some j such that $1 \leq j \leq k$ □

Theorem 1.4. *Any downward closed subset in a wqo $(X, \subseteq)$ admits a unique decomposition as a finite union of pairwise incomparable (under inclusion) ideals. Therefore, a downward closed subset decomposes canonically as the union of its maximal ideals.*

Proof. Suppose there are two different sets of pairwise incomparable ideals I and J and let them be $I = \{I_1, \ldots, I_n\}$ and $J = \{J_1, \ldots, J_m\}$, where $I_1, \ldots, I_n, J_1, \ldots, J_m \in Ideals(X, \subseteq)$
Claim: $n = m$
Suppose, if possible, $n \neq m$. WLOG assume $n > m$. Now, since I and J are sets of ideals for the same downward closed set, $\bigcup_{i=1}^{n} I_i = \bigcup_{j=1}^{m} J_j$ and so using the previous lemma, $\forall i$ st $1 \leq i \leq n, \exists j$ st $1 \leq j \leq m$ and $I_i \subseteq J_j$ and vice versa. By pigeonhole principle, $\exists i, j, k, i \neq j$ st $I_i \subseteq J_k$ and $I_j \subseteq J_k$. Also, $\exists l$ st $J_j \subseteq I_l$ and therefore, $I_i \subseteq I_l$ and $I_j \subseteq I_l$. Since $i \neq j$, we have a pair of distinct ideals in I that are comparable $\rightarrow$ contradiction! Thus, $n = m$.
Claim: $I = J$
We know that $\forall i$ st $1 \leq i \leq n, \exists j$ st $1 \leq j \leq m$ and $I_i \subseteq J_j$ and vice versa. List both I and J as a sequence : $I_1, I_2, \ldots, I_n$ and $J_1, J_2, \ldots, J_m$. Pick the first element in the sequence for I : I_1. $\exists j$ st $I_1 \subseteq J_j$ and $\exists k$ st $J_j \subseteq I_k$ and therefore, $I_1 \subseteq I_k$ but I is a set of incomparable ideals. Thus, $I_k = I_1$ and therefore, $I_1 = J_j$. Remove both I_1 and J_j from the sequences, and repeat this procedure. At every point, since $n = m$, the length of the sequences are same, and at every point one removes a pair $< I_i, J_j >$ st $I_i = J_j$. Also, at every point, the invariant that the two sequences represent the same downward closed set is maintained (since one removes the same ideal from both sequences) which allows one to apply the previous lemma at each step. The procedure ends and we can easily see that thus, $I = J$.
Here, a set of ideals representing a downward closed set is said to be a set of *maximal* ideals if for every ideal I in the set, there exists no J in the ideal decomposition of the downward closed set by Theorem 1.2 st $I \subseteq J$. Suppose the set of pairwise incomparable ideals described in the theorem is not a set of maximal ideals, then there is an ideal I in the set st $\exists J \in Ideals(X, \subseteq)$ and $J \subseteq D$ where D is the downward closed set. Replacing I with J and removing any smaller ideals from the set would give us another (possibly smaller) set of pairwise incomparable ideals representing D but as proved above, that is not possible.

□

1.5 Another way of characterising wqos

Theorem 1.5. *(X, $\leq$) is a wqo if and only if every upward closed set $U = \uparrow U \subseteq X$ has a finite basis*

Proof. $\Longrightarrow$

- Existence of Basis: If the set U does not have minimal elements then from any element we can form an infinite decreasing sequence which cannot happen since $U \subseteq X$. Let the set of minimal elements be B. We claim that $U = \uparrow B$. For any element $x \in \uparrow B$, $x \in U$ because $B \subseteq U$ and all elements greater than any element of B belong to U. This proves $\uparrow B \subseteq U$. Now consider $x \in U$ and the set $Y = \downarrow x \cap U$. If this set does not have a minimal element then this contradicts X being a wqo as above. Also note that all minimal elements of Y are also the minimal elements of U because any element smaller than any of them will appear in both U and $\downarrow x$ and hence that element will not be minimal.

- Finiteness of Basis: Note that the set B defined above is an antichain since it is the set of minimal elements. If B has an infinite number of elements then X has an infinite anti-chain which is again a contradiction.

$\Longleftarrow$

1. No infinite antichain
   Let B be the set of elements that form an infinite antichain. Consider $U = \uparrow B$. Let the set of basis elements of U be B'. Since $\uparrow B' = U$, there is an element in B' whose upward closure has infinitely many elements of B. Let that element be x. Also $\exists b \in B$ st $x \in \uparrow b$ since every element in U has been obtained from upward closure of elements in B. Since $\exists b_1, b_2 \in B$ and $b_1, b_2 \in \uparrow x$ (Pick any two from the infinite set of elements of B in $\uparrow x$), $b \leq x \leq b_1$ and $b \leq x \leq b_2$. Now, since b_1 and b_2 are distinct, only one of them can be equal to b. Therefore, B isn't a set of elements of an antichain.

2. No infinite decreasing sequence
   Suppose there exists such a sequence and let X be the set that contains all the elements of that sequence. Now $\uparrow X$ will have at least one minimal element (say k). If $k \in X$ then that is a contradiction since X contains an element less than k. If $k \notin X$ then k must have been introduced by upward closure of some element in X and hence is not minimal. Therefore, such a set X cannot exist and such a decreasing sequence cannot exist either.

$\square$