CS 880: Complexity of Counting Problems 02/16/2012

Lecture 8: Universal Algebra

Instructor: Jin-Yi Cai Scribe: Chetan Rao

1 Introduction

In today's lecture, we will look more closely into *Universal Algebra* and the properties of invariants (Inv) and polymorphisms (Pol). We shall also look at a few key theorems that will help prove dichotomy in the following lectures.

A universal algebra is an algebraic system consists of a structure $\mathcal{A} = (A, \Gamma)$ where A is the domain set (finite) and Γ is a set of relations on A with finite arity (Γ can be infinite). Let $\mathcal{F}$ be a set of functions.

To better understand the relation between Pol and Inv, we need the concept of Galois-correspondence between sets $\mathcal{F}$ and Γ.

Definition 1 (Galois correspondence)**.** *A Galois-correspondence between sets A and B is a pair (σ, τ) of mappings between the power sets $\mathcal{P}(A)$ and $\mathcal{P}(B)$:*

$$\sigma : \mathcal{P}(A) \to \mathcal{P}(B), \text{ and } \tau : \mathcal{P}(B) \to \mathcal{P}(A)$$

σ and τ must satisfy the following conditions. For all $X, X' \subseteq A$ and all $Y, Y' \subseteq B$,

1. *$X \subseteq X' \to \sigma(X) \supseteq \sigma(X')$, and $Y \subseteq Y' \to \tau(Y) \supseteq \tau(Y')$*
2. *$X \subseteq \tau\sigma(X)$, and $Y \subseteq \sigma\tau(Y)$*

Applying the Pol operator on Γ, we get a set of functions that commute with Γ i.e. $\mathsf{Pol}(\Gamma)$. On the other hand, if we apply the Inv operator on $\mathcal{F}$, we get a set of relations that commute with $\mathcal{F}$ i.e. $\mathsf{Inv}(\mathcal{F})$. It is easy to see that Pol and Inv satisfy property 1 of Galois-correspondence by their definitions as any subset of relations cannot decrease the number of functions that commute (and vice-versa). In other words, the double application of correspondence mapping is no smaller in size in set containment relation.

If we set $\mathcal{F} = \mathsf{Pol}(\Gamma)$, then we can see that Γ commutes with every function in $\mathsf{Pol}(\Gamma)$ which, in turn, commutes with every relation in $\mathsf{Inv}(\mathsf{Pol}(\Gamma))$. Hence, $\Gamma \subseteq \mathsf{Inv}(\mathsf{Pol}(\Gamma))$ as pictured in figure 1. We can similarly prove that $\mathcal{F} \subseteq \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$. Thus, we show that $(\mathsf{Pol}, \mathsf{Inv})$ form a Galois-correspondence between $\mathcal{F}$ and Γ.

Lemma 1. *Let the pair (σ, τ) be a Galois-correspondence between the sets A and B. Then $\sigma\tau\sigma = \sigma$ and $\tau\sigma\tau = \tau$.*

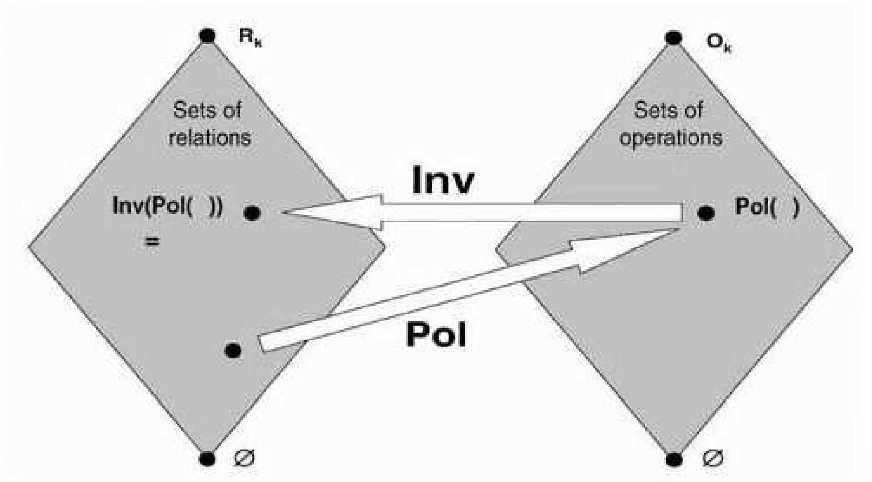

Figure 1: [1] The operators Pol and Inv on the set of functions (operations) $\mathbf{O_k}$ and set of relations $\mathbf{R_k}$.

Proof. Let $X \subseteq A$. By property 2 of Galois-correspondence, $X \subseteq \tau\sigma(X)$. By property 1, if we apply σ, it gives us $\sigma(X) \supseteq \sigma\tau\sigma(X)$. By applying property 2, we also have $\sigma(X) \subseteq \sigma(\tau\sigma(X))$. Therefore, $\sigma\tau\sigma(X) = \sigma(X)$. The second part of the claim can be proved similarly. $\square$

Hence, we can see that $\mathsf{Pol}(\Gamma) = \mathsf{Pol}(\mathsf{Inv}(\mathsf{Pol}(\Gamma)))$ and $\mathsf{Inv}(\mathcal{F}) = \mathsf{Inv}(\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})))$. In other words, going forward twice makes the set no smaller and going forward thrice is equivalent to once. This is depicted in figure 2.

$$\begin{tikzcd}
\Gamma \arrow[r, "\mathsf{Pol}"] \arrow[d, phantom, "\subseteq"] & \mathsf{Pol}(\Gamma) \arrow[dl, "\mathsf{Inv}"'] \arrow[d, phantom, "="] \\
\mathsf{Inv}(\mathsf{Pol}(\Gamma)) \arrow[r, "\mathsf{Pol}"] & \mathsf{Pol}(\mathsf{Inv}(\mathsf{Pol}(\Gamma)))
\end{tikzcd}$$

Figure 2: Sequence of $\mathsf{Pol}, \mathsf{Inv}, \mathsf{Pol}$ operators applied on Γ.

2 Properties of Pol and Inv

In this section, we look at certain important properties of Pol and Inv.

2.1 $\mathsf{Inv}(\mathcal{F})$

Given a set of functions $\mathcal{F}$, its invariant $\mathsf{Inv}(\mathcal{F})$ has the following properties:

1. Closed under $\wedge$: Let $P, Q \in \mathsf{Inv}(\mathcal{F})$ on A^r and $N = [\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}]$ where $\mathbf{a_i}$ is a column vector of length r and $\mathbf{a_i} \in P \wedge Q$, then for all functions $f \in \mathcal{F}$, the following holds: $b = f_{\rightarrow}(N) \in P \wedge Q$.

$$
\begin{array}{cccccccc}
N = & [\mathbf{a_1} & \mathbf{a_2} & \ldots & \mathbf{a_n}] & \xrightarrow{f} & \mathbf{b} \\
 & a_{1,1} & a_{2,1} & \ldots & a_{n,1} & \xrightarrow{f} & b_1 \\
 & a_{1,2} & a_{2,2} & \ldots & a_{n,2} & \xrightarrow{f} & b_2 \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & a_{1,r} & a_{2,r} & \ldots & a_{n,r} & \xrightarrow{f} & b_r \\
 & \in & \in & \in & & & \in \\
 & P \wedge Q & P \wedge Q & P \wedge Q & & & P \wedge Q
\end{array}
$$

2. Closed under $\exists$: Let $P \in \mathsf{Inv}(\mathcal{F})$ on $A^r (r \geq 2)$ and $Q \subseteq A^{r-1}$ s.t. $Q = \exists x P$ i.e. $Q(x_1, x_2, \ldots, x_{r-1}) = \exists x_r P(x_1, x_2, \ldots, x_r)$.

$$
\widehat{N} = \begin{array}{ccccc}
\mathbf{x_1} = [x_{1,1} & \ldots & x_{n,1}] & \xrightarrow{f} & b_1 \\
\mathbf{x_2} = [x_{1,2} & \ldots & x_{n,2}] & \xrightarrow{f} & b_2 \\
\vdots \quad \vdots & \vdots & \vdots & \vdots & \vdots \\
\mathbf{x_{r-1}} = [x_{1,r-1} & \ldots & x_{n,r-1}] & \xrightarrow{f} & b_{r-1} \\
\in & \in & & & \in \\
Q & Q & & & Q
\end{array}
\xRightarrow{\exists \mathbf{x_r}}
\begin{array}{ccccc}
\mathbf{x_1} = [x_{1,1} & \ldots & x_{n,1}] & \xrightarrow{f} & b_1 \\
\mathbf{x_2} = [x_{1,2} & \ldots & x_{n,2}] & \xrightarrow{f} & b_2 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\mathbf{x_{r-1}} = [x_{1,r-1} & \ldots & x_{n,r-1}] & \xrightarrow{f} & b_{r-1} \\
\mathbf{x_r} = [x_{1,r} & \ldots & x_{n,r}] & \xrightarrow{f} & b_r \\
\in & \in & & & \in \\
P & P & & & P
\end{array}
$$

3. Closed under Π (permutation): Let $P \in \mathsf{Inv}(\mathcal{F})$ on A^r and Π be a permutation s.t. $Q(x_1, x_2, \ldots, x_r) = P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(r)})$, then $Q = \Pi P \in \mathsf{Inv}(\mathcal{F})$.

4. Closed under direct product: Let $P \in \mathsf{Inv}(\mathcal{F})$ on A^r and $A \times P$ be a cartesian product. Then for all $P \in \mathsf{Inv}(\mathcal{F})$, $A \times P \in \mathsf{Inv}(\mathcal{F})$. This property combined with arity-2 Equality gates ($=_2$) gives rise to the next property:

5. Closed under R (repetition): Let $P \in \mathsf{Inv}(\mathcal{F})$ on A^r and R be a repetition s.t. $R.P = \{(x_1, x_1, x_2, \ldots, x_r) | (x_1, x_2, \ldots, x_r) \in P\}$, then $R.P \in \mathsf{Inv}(\mathcal{F})$.

The set of relations satisfying these properties is called a 'clone'.

2.2 $\mathsf{Pol}(\Gamma)$

Given a set of relations Γ, it's polymorphism $\mathsf{Pol}(\Gamma)$ has the following properties:

1. Closed under composition ($\circ$): Let f and g be two polymorphisms (of arity-n over Γ) and N_i be matrices for $i \in \{1, 2, \ldots, n\}$ which have column vectors $\in \mathsf{Pol}(\Gamma)$. Then, $\forall i, f_{\rightarrow}(N_i) \in \mathsf{Pol}(\Gamma)$ and hence, $(g \circ f)_{\rightarrow}(\mathbf{N}) = g_{\rightarrow}(f_{\rightarrow}(N_1), f_{\rightarrow}(N_2), \ldots, f_{\rightarrow}(N_n)) \in \mathsf{Pol}(\Gamma)$.

2. Closed under projection: Let f be a polymorphism over $R \in \Gamma$. Then, any such $f_i(x_1, \ldots, x_n) = x_i$ is a polymorphism as f_i is just selecting one of the columns that are already known to be in $R \in \Gamma$.

To handle cases where the arity of composed functions are not the same, we can compose such functions to obtain full arity functions. For instance if we want to compute $f(g_1(x_1, x_2), g_2(x_2, x_4), g_3(x_1, x_2, x_3))$, we can project x_1, x_2 from (x_1, x_2, x_3, x_4) for g_1 to obtain an equivalent function with full arity. Similar techniques can be applied to g_2 and g_3 to obtain a composition of arity-3 function with arity-4 functions.

Definition 2 (closed system)**.** *A closed system of functions on a finite set is a set of functions that satisfies the above two properties.*

3 Geiger's Theorems

The theorems that follow in this section are from the work by Geiger [2]. We recall the definition of partial polymorphism before we state the theorems.

Definition 3 (partial polymorphism)**.** *A partial function $f : A^r \rightarrow A$ is a partial polymorphism if f is defined for all matrices N such that every column belongs to the relation $R \in \Gamma$, then $f_{\rightarrow}(N) \in R$.*

Theorem 1. *If Γ is a clone, then any partial polymorphism f of Γ can be extended to a full polymorphism.*

Proof. Let f be a partial polymorphism of Γ of arity-r. We may assume f is not empty as we can extend any empty f to the idempotent function i.e. $(i, i, \ldots, i) \mapsto i$. WLOG, f is non-empty and not full. If we manage to extend the polymorphism by one more tuple, by induction we can extend it to the whole set and we are done.

Let $\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_k}$ and $\mathbf{r} \neq \mathbf{r_i}$, $\forall i \in \{1, 2, \ldots, k\}$ be the tuples on which f is defined. Also, let

$$N = \begin{pmatrix} \mathbf{r_1} \\ \mathbf{r_2} \\ \vdots \\ \mathbf{r_k} \end{pmatrix}$$

Now, we extend the partial function f by $f_j(\mathbf{r}) = j$ as follows: define $f_j = f \cup (f_j(\mathbf{r}) = j)$ $\forall j \in \{1, 2, \ldots, |A|\}$. Now, if we can show that at least one of the f_j is a polymorphism, we are done.

Claim 1. *At least one of the f_j's is a partial polymorphism of Γ.*

Proof. We prove this claim by contradiction. Let's assume that none of the f_j's are partial polymorphisms of $\Gamma, \forall j \in \{1, 2, \dots, |A|\}$. This means that for every j, we have a relation $R_j \in \Gamma$ and a matrix N_j such that -

$$N_j = \begin{array}{c} \begin{bmatrix} n^j_{1,1} & \dots & n^j_{1,r} \\ n^j_{2,1} & \dots & n^j_{2,r} \\ \vdots & \vdots & \vdots \\ n^j_{n,1} & \dots & n^j_{n,r} \end{bmatrix} \\ \begin{array}{ccc} \in & \cdots & \in \\ R_j & & R_j \end{array} \end{array} \xrightarrow{f_j \to (N_j)} \mathbf{b_j} \notin R_j \quad \forall j \in \{1, 2, \dots, |A|\}$$

Also, it cannot be the case where f_j is not defined on the rows as this will not result in an invalidation. Hence, the rows of N_j are among $\mathbf{r_1}, \mathbf{r_2}, \dots, \mathbf{r_k}, \mathbf{r}$. Now, let us suppose that there are two equal rows s and t. In this case, we can define a relation $R_j^{'}$ such that $R_j^{'}(x_1, \dots, x_s, \dots, x_t, \dots, x_n) = \exists x_t(R_j(x_1, \dots, x_s, \dots, x_t, \dots, x_n) \wedge (x_s = x_t))$. Since Γ is a clone, we can always find such a minimal arity relation $R_j^{'}$.

Hence $\forall j$, $\exists R_j \in \Gamma$ of minimal arity such that -

1. N_j has no repeated rows.
2. N_j must have row $\mathbf{r}$.
3. For some j, N_j has at least 2 rows.

Property 2 follows from the definition of the partial polymorphism f because otherwise the table would prove that f is not a partial polymorphism. Property 3 also holds because if it does not, then all the matrices N_j have only row $\mathbf{r}$. Let the first component of $\mathbf{r}$ be i. Then consider the table N_i for R_i. This $i \in R_i$. But then $f_i(\mathbf{r}) = i \in R_i$, a contradiction. Hence some N_j has at least two rows.

From these matrices, we can construct a new matrix N^* by stacking each matrix N_j on top of each other and pulling out the common row $\mathbf{r}$ from every N_j:

$$\overline{N} = \left[\begin{array}{cc} & \overline{\phantom{N_{|A|}N_{|A|}}} \quad = \mathbf{r} \\ N^* & \left.\left[\begin{array}{c} \boxed{N_1} \\ \boxed{N_2} \\ \vdots \\ \boxed{N_{|A|}} \end{array}\right]\right\} \neq \phi \end{array}\right]$$

Since the clone Γ is closed under conjunction and extension, a new relation R can be defined which says that the corresponding subsets of coordinates are in the relation R_j, for $j \in \{1, 2, \dots, |A|\}$.

Then a new relation R^*, using existential quantifier on the first row, can be defined, such that N^* is a table for it ($R^* \in \langle\Gamma\rangle$).

Then f is defined on the rows of N^*, and would produce a tuple $\in R^*$. By definition of R^*, this means there is some $i \in A$ such that f_i commutes with the table $\overline{N}$. But then looking at only the corresponding subset of coordinates for R_i, this is a contradiction to the statement that f_i does not commute with N_i. Therefore, $f_{\rightarrow}(N^*) \in R$ and hence for some j, f_j is a partial polymorphism. $\square$

Thus, we show that every partial polymorphism can be extended by one more and this concludes the theorem. $\square$

Theorem 2. *If $\mathcal{F}$ is a closed system (under composition and projection), then $\mathsf{Inv}(\mathcal{F})$ is a clone and $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})) = \mathcal{F}$.*

Proof. From the Galois-correspondence, we know that $\mathcal{F} \subseteq \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$. We need to show that the other way holds true if $\mathcal{F}$ is closed. Thus, it is enough to prove that given any function $g \notin \mathcal{F}$, there is a relation $R \in \mathsf{Inv}(\mathcal{F})$ such that g does not commute with R.

Let g be a function with arity-r. Now, we list all the $|A|^n$ tuples for which g is defined. Let this be represented by matrix N. Let $g_{\rightarrow}(N)$ be the set of corresponding relations.

We now extend the matrix N by appending non-repetitive columns generated by applying $f(\forall f \in \mathcal{F})$ to each sequence (possible repetition of coordinates) of rows. This eventually terminates as the number of columns in the extended matrix ($N^{'}$) are bounded (by size $|A|^n$). Let all such columns define the relation R. If we show that g does not commute with this relation, we are done.

Claim 2. *$g \notin \mathcal{F}$ does not commute with $R \in \mathsf{Inv}(\mathcal{F})$ (constructed above).*

Proof. If g commutes with relation R, then g should produce an element of $R \in \mathsf{Inv}(\mathcal{F})$ on it's application on any column in the extended matrix $N^{'}$. However, note that every column in $N^{'}$ is a composition of functions in $\mathcal{F}$. Since $\mathcal{F}$ is a closed system, any composition of functions in it will produce a function $f \in \mathcal{F}$. Thus, this forces $g \in \mathcal{F}$ if g commutes with R and hence contradicts the assumption that $g \notin \mathcal{F}$. $\square$

Thus, we prove that $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})) \subseteq \mathcal{F}$ and hence $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})) = \mathcal{F}$ for a closed system $\mathcal{F}$. Also note that $\mathsf{Inv}(\mathcal{F})$ is a clone. $\square$

Theorem 3. *If Γ is a clone, $\mathsf{Inv}(\mathsf{Pol}(\Gamma)) = \Gamma$. In general, for all Γ, $\mathsf{Inv}(\mathsf{Pol}(\Gamma)) = \langle\Gamma\rangle$*

The proof of this theorem will be done in the next lecture.

References

[1] A. Krokhin, A. Bulatov, and P. Jeavons, *Structural Theory of Automata, Semigroups, and Universal Algebra*, Proceedings of the NATO Advanced Study Institute on Structural Theory of Automata, Semigroups and Universal Algebra, Montreal, Canada, 2003.

[2] David Geiger, *Closed systems of functions and predicates.*, Pacific J. Math. Volume 27, Number 1 (1968), 95-100.