1 Introduction

In today’s lecture, we will look more closely into \textit{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 $A = (A, \Gamma)$ where $A$ is the domain set (finite) and $\Gamma$ is a set of relations on $A$ with finite arity ($\Gamma$ can be infinite). Let $\mathcal{F}$ be a set of functions.

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

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

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

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

1. $X \subseteq X' \rightarrow \sigma(X) \supseteq \sigma(X')$, and $Y \subseteq Y' \rightarrow \tau(Y) \supseteq \tau(Y')$

2. $X \subseteq \tau \sigma(X)$, and $Y \subseteq \sigma \tau(Y)$

Applying the $\text{Pol}$ operator on $\Gamma$, we get a set of functions that commute with $\Gamma$ i.e. $\text{Pol}(\Gamma)$. On the other hand, if we apply the $\text{Inv}$ operator on $\mathcal{F}$, we get a set of relations that commute with $\mathcal{F}$ i.e. $\text{Inv}(\mathcal{F})$. It is easy to see that $\text{Pol}$ and $\text{Inv}$ 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 $\mathcal{F} = \text{Pol}(\Gamma)$, then we can see that $\Gamma$ commutes with every function in $\text{Pol}(\Gamma)$ which, in turn, commutes with every relation in $\text{Inv}(\text{Pol}(\Gamma))$. Hence, $\Gamma \subseteq \text{Inv}(\text{Pol}(\Gamma))$ as pictured in figure 1. We can similarly prove that $\mathcal{F} \subseteq \text{Pol}(\text{Inv}(\mathcal{F}))$. Thus, we show that $(\text{Pol}, \text{Inv})$ form a Galois-correspondence between $\mathcal{F}$ and $\Gamma$.

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

1
Proof. Let $X \subseteq A$. By property 2 of Galois-correspondence, $X \subseteq \tau \sigma(X)$. By property 1, if we apply $\sigma$, 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.

Hence, we can see that $\text{Pol}(\Gamma) = \text{Pol}(\text{Inv}(\text{Pol}(\Gamma)))$ and $\text{Inv}(\mathcal{F}) = \text{Inv}(\text{Pol}(\text{Inv}(\mathcal{F})))$. 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.

![Diagram](image)

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

**Figure 2:** Sequence of $\text{Pol}$, $\text{Inv}$, $\text{Pol}$ operators applied on $\Gamma$.

## 2 Properties of $\text{Pol}$ and $\text{Inv}$

In this section, we look at certain important properties of $\text{Pol}$ and $\text{Inv}$.

### 2.1 $\text{Inv}(\mathcal{F})$

Given a set of functions $\mathcal{F}$, its invariant $\text{Inv}(\mathcal{F})$ has the following properties:
1. Closed under $\land$: Let $P, Q \in \text{Inv}(\mathcal{F})$ on $A^r$ and $N = [a_1, a_2, \ldots, a_n]$ where $a_i$ is a column vector of length $r$ and $a_i \in P \land Q$, then for all functions $f \in \mathcal{F}$, the following holds: $b = f(N) \in P \land Q$.

$$N = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix}$$

$$\begin{array}{cccc}
    a_{1,1} & a_{2,1} & \ldots & a_{n,1} \\
    a_{1,2} & a_{2,2} & \ldots & a_{n,2} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1,r} & a_{2,r} & \ldots & a_{n,r}
\end{array} \xrightarrow{f} \begin{array}{c} b_1 \\
    b_2 \\
    \vdots \\
    b_r
\end{array}$$

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

$$\begin{array}{l}
    \hat{N} = \begin{bmatrix} x_{1,1} & \ldots & x_{1,n_1} \end{bmatrix} \xrightarrow{f} b_1 \\
    \begin{bmatrix} x_{1,2} & \ldots & x_{1,n_2} \end{bmatrix} \xrightarrow{f} b_2 \\
    \vdots \\
    \begin{bmatrix} x_{1,r-1} & \ldots & x_{1,n_{r-1}} \end{bmatrix} \xrightarrow{f} b_{r-1} \\
    \begin{bmatrix} x_{1,r} & \ldots & x_{1,n_r} \end{bmatrix} \xrightarrow{f} b_r \\
\end{array}$$

3. Closed under $\Pi$ (permutation): Let $P \in \text{Inv}(\mathcal{F})$ on $A^r$ and $\Pi$ 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 $Q = \Pi P \in \text{Inv}(\mathcal{F})$.

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

5. Closed under $R$ (repetition): Let $P \in \text{Inv}(\mathcal{F})$ 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 $R.P \in \text{Inv}(\mathcal{F})$.

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

### 2.2 Pol($\Gamma$)

Given a set of relations $\Gamma$, it’s polymorphism Pol($\Gamma$) has the following properties:
1. Closed under composition \((\circ)\): Let \(f\) and \(g\) be two polymorphisms (of arity-\(n\) over \(\Gamma\)) and \(N_i\) be matrices for \(i \in \{1, 2, \ldots, n\}\) which have column vectors \(\in \text{Pol}(\Gamma)\). Then, \(\forall i, f_\rightarrow(N_i) \in \text{Pol}(\Gamma)\) and hence, \((g \circ f)_\rightarrow(N) = g_\rightarrow(f_\rightarrow(N_1), f_\rightarrow(N_2), \ldots, f_\rightarrow(N_n)) \in \text{Pol}(\Gamma)\).

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 \(f : A' \to A\) 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 \(\Gamma\) is a clone, then any partial polymorphism \(f\) of \(\Gamma\) can be extended to a full polymorphism.

**Proof.** Let \(f\) be a partial polymorphism of \(\Gamma\) 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 \(r_1, r_2, \ldots, r_k\) and \(r \neq r_i, \forall i \in \{1, 2, \ldots, k\}\) be the tuples on which \(f\) is defined. Also, let

\[
N = \begin{pmatrix}
    r_1 \\
    r_2 \\
    \vdots \\
    r_k
\end{pmatrix}
\]

Now, we extend the partial function \(f\) by \(f_j(r) = j\) as follows: define \(f_j = f \cup (f_j(r) = j) \forall j \in \{1, 2, \ldots, |A|\}\). 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 $\Gamma$.

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

$$N_j = \begin{bmatrix} n_{1,1}^j & \cdots & n_{1,r}^j \\ n_{2,1}^j & \cdots & n_{2,r}^j \\ \vdots & \vdots & \vdots \\ n_{n,1}^j & \cdots & n_{n,r}^j \\ \in & \cdots & \in \\ R_j & \cdots & R_j \end{bmatrix} \xrightarrow{f_j \circ (N_j)} b_j \notin R_j \ \forall j \in \{1, 2, \ldots, |A|\}$$

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 $r_1, r_2, \ldots, r_k, r$. 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 $R_j'(x_1, \ldots, x_s, \ldots, x_t, \ldots, x_n) = \exists x_t(R_j(x_1, \ldots, x_s, \ldots, x_t, \ldots, x_n) \wedge (x_s = x_t))$. Since $\Gamma$ 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 $r$.
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 $r$. Let the first component of $r$ be $i$. Then consider the table $N_i$ for $R_i$. This $i \in R_i$. But then $f_i(r) = i \in R_i$, 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 $r$ from every $N_j$:

$$\overline{N} = \begin{bmatrix} N^* \\ \begin{array}{c} N_1 \\ N_2 \\ \vdots \\ \overline{N}_{|A|} \end{array} \end{bmatrix} = r$$

Since the clone $\Gamma$ 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 $j \in \{1, 2, \ldots, |A|\}$. 


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 $\mathbf{N}$. 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, $f_\neg(N^*) \in R$ and hence for some $j$, $f_j$ is a partial polymorphism.

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

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

Proof. From the Galois-correspondence, we know that $\mathcal{F} \subseteq \text{Pol(Inv}(\mathcal{F}))$. 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 $R \in \text{Inv}(\mathcal{F})$ 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 $g_\neg(N)$ 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 $R \in \text{Inv}(\mathcal{F})$ (constructed above).

Proof. If $g$ commutes with relation $R$, then $g$ should produce an element of $R \in \text{Inv}(\mathcal{F})$ 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 $g \notin \mathcal{F}$.

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

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

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

References