Duality in Logic

Lecture 2

Mai Gehrke

Université Paris 7 and CNRS
Further examples - revisited

1. Completeness of **modal logic** with respect to Kripke semantics was obtained via duality in the form of canonical extensions by Jónsson and Tarski in 1951. Ten years before Kripke!

2. Henkin’s proof of **completeness for FOL** relies on building a model from an ultrafilter then adding witnesses for existential formulas. It was shown by Rasiowa and Sikorski in 1950 that this second step can be eliminated by applying **Baire category theorem** to the dual space of the Lindenbaum algebra.

3. In the late 1960’s, Dana Scott built the first **model of the lambda-calculus** using an inverse limit of finite spaces (which then is a Stone space). In his 1994 paper on domains in logical form Abramsky later gave a general way of solving domain equations based on Stone duality.
Duality for operators

Restrict to $DL_{fin}$

An operator is an operation that preserves finite joins ($0$ and $\lor$) in each coordinate

$$\begin{align*}
\text{operator} \quad \diamond : D^n &\rightarrow D \\
\iff & \quad R \subseteq X \times X^n \quad \text{relation} \\
\diamond & \quad \iff \quad R_\diamond = \{(x, \bar{x}) \mid x \leq \diamond(\bar{x})\} \\
(\diamond_R : \overline{S} \rightarrow R^{-1}[S_1 \times \ldots \times S_n]) & \quad \iff \quad R
\end{align*}$$
Duality for operators

operator $\diamond : D^n \to D \leftrightarrow R \subseteq X \times X^n$ relation

$\diamond \mapsto \ R_{\diamond} = \{ (x, x) \mid x \leq \diamond(\overline{x}) \}$

$(\diamond_R : \overline{S} \mapsto R^{-1}[S_1 \times \ldots S_n]) \leftrightarrow R$

Some observations:

- The dual relations are those satisfying $\leq \circ R \circ (\leq)^n = R$
- $R$ is a relational ‘lower adjoint’ of the corresponding operator
- $xR$ has a minimum for each $x$ iff $\diamond$ is meet preserving iff $\diamond$ is a homomorphism
Duality for operators

- Function
  - homomorphism

- Partial function
  - not 1-preserving

- General relation
  - not ∧-preserving
Duality for dual operators

What do we do for a □ that preserves finite meets (1 and ∧) in each coordinate?

dual operator □ : $D^n \rightarrow D \quad \longleftrightarrow \quad S \subseteq M \times M^n \quad \text{relation}

□ \quad \mapsto \quad S_\Box = \{(m, \overline{m}) \mid m \geq □(\overline{m})\}

\left(□_S : \overline{u} \mapsto \bigwedge S^{-1}[\uparrow \overline{u} \cap M^n]\right) \quad \leftarrow \quad S

where $M = M(D)$ and we use the duality with respect to meet-irreducibles instead of duality with respect to join-irreducibles.
A neutral dual space

The posets $J(D)$ and $M(D)$ of join- and meet-irreducibles of a finite DL are order isomorphic

$$J(D) \rightarrow M(D)$$

$$j \mapsto \bigvee \{a \in D \mid j \not\leq a\}$$

Choose for the dual space a set $X$ with maps

$j : X \rightarrow J(D), x \mapsto j_x$ a bijection

$m : X \rightarrow M(D), x \mapsto m_x$ a bijection

and $\forall x \in X \forall a \in D \ (j_x \leq a \iff a \not\leq m_x)$
Duality for residuated families

Consider a binary residuated family on a finite $D$

$$\forall a, b, c \in D \quad (a \cdot b \leq c \iff b \leq a \setminus c \iff a \leq c/b)$$

then we have, for $x, y, z \in X$

$$R.(x, y, z) \iff j_x \leq j_y \cdot j_z$$
$$\iff j_y \cdot j_z \not\leq m_x$$
$$\iff j_z \not\leq j_y \setminus m_x$$
$$\iff j_y \setminus m_x \leq m_z$$
$$\iff S' \setminus (z, y, x)$$

All three operations are given by one ternary relation
Duality for operations on DLs

This goes through in some form to the general setting:

- The correspondence between prime filters and ideals allows us to encode both meet and join pres/rev-ersing operations on the dual space.

- If the operation is \( n \)-ary then the relation is \((n + 1)\)-ary and order compatible with certain topological properties.

- If \( f \) is join preserving in each coordinate, then the relation is morally its lower adjoint; If \( f \) is meet preserving, then the relation is morally its upper adjoint.

- Families of operations related by residuation are all encoded by one and the same relation on the dual.
A finite automaton

The states are \( \{1, 2, 3\} \).
The initial state is 1, the final states are 1 and 2.
The alphabet is \( A = \{a, b\} \) The transitions are

\[
1 \cdot a = 2 \quad 2 \cdot a = 3 \quad 3 \cdot a = 3 \\
1 \cdot b = 3 \quad 2 \cdot b = 1 \quad 3 \cdot b = 3
\]
Recognition by automata

Transitions extend to words: $1 \cdot aba = 2$, $1 \cdot abb = 3$.
The language recognized by the automaton is the set of words $u$ such that $1 \cdot u$ is a final state. Here:

$$L(A) = (ab)^* \cup (ab)^* a$$

where $*$ means arbitrary iteration of the product.
Rational and recognizable languages

A language is **recognizable** provided it is recognized by some finite automaton.

A language is **rational** provided it belongs to the smallest class of languages containing the **finite languages** which is closed under **union**, **product** and **star**.

**Theorem:** [Kleene ’54] A language is **rational** iff it is **recognizable**.

**Example:** \( L(A) = (ab)^* \cup (ab)^*a. \)

**Corollary:** The rational languages are closed under all the Boolean operations.
Logic on words

To each non-empty word $u$ is associated a structure

$$\mathcal{M}_u = (\{1, 2, \ldots, |u|\}, <, (a)_{a \in A})$$

where $a$ is interpreted as the set of integers $i$ such that the $i$-th letter of $u$ is an $a$, and $<$ as the usual order on integers.

Example:

Let $u = abbaab$ then

$$\mathcal{M}_u = (\{1, 2, 3, 4, 5, 6\}, <, (a, b))$$

where $a = \{1, 4, 5\}$ and $b = \{2, 3, 6\}$. 
Some examples

The formula $\phi = \exists x \ a x$ interprets as:

*There exists a position $x$ in $u$ such that the letter in position $x$ is an $a$.*

This defines the language $L(\phi) = A^*aA^*$.

The formula $\exists x \ \exists y \ (x < y) \land ax \land by$ defines the language $A^*aA^*bA^*$.

The formula $\exists x \ \forall y \ [(x < y) \lor (x = y)] \land ax$ defines the language $aA^*$.
Defining the set of words of even length

Macros:

\[(x < y) \lor (x = y) \text{ means } x \leq y\]

\[\forall y \; x \leq y \text{ means } x = 1\]

\[\forall y \; y \leq x \text{ means } x = |u|\]

\[x < y \land \forall z \; (x < z \rightarrow y \leq z) \text{ means } y = x + 1\]

Let \(\phi = \exists X \; (1 \notin X \land |u| \in X \land \forall x \; (x \in X \leftrightarrow x + 1 \notin X))\)

Then \(1 \notin X, \; 2 \in X, \; 3 \notin X, \; 4 \in X, \ldots, \; |u| \in X\). Thus

\[L(\phi) = \{u \mid |u| \text{ is even}\} = (A^2)^*\]
Monadic second order

Only second order quantifiers over unary predicates are allowed.

Theorem: (Büchi ’60, Elgot ’61)

Monadic second order captures exactly the recognizable languages.

Theorem: (McNaughton-Papert ’71)

First order captures star-free languages

(star-free = the ones that can be obtained from the alphabet using the Boolean operations on languages and lifted concatenation product only).

How does one decide the complexity of a given language???
Algebraic theory of automata

**Theorem:** [Myhill '53, Rabin-Scott '59] There is an effective way of associating with each finite automaton, \( A \), a finite monoid, \( (M_A, \cdot, 1) \).

**Theorem:** [Schützenberger '65] Starfree languages correspond to monoids \( M \) such that there exists \( n > 0 \) with \( x^n = x^{n+1} \) for each \( x \in M \).

Submonoid generated by \( x \):

This makes starfreeness decidable!
Pseudo-varieties

The class of finite aperiodic monoids is closed under homomorphic images, subalgebras, and finite products. Such classes are called pseudo-varieties.

Eilenberg’s Theorem identifies which (indexed) classes of regular languages correspond to pseudo-varieties of monoids.

Reiterman’s Theorem tells us these are given by equations in pseudoterms.

The pseudo-equational specification of aperiodicity is \( x^\omega \approx x^{\omega+1} \) where \( x^\omega \) is a pseudoterm that evaluates to the unique idempotent in the submonoid generated by \( x \).
Encompassing more general classes

Several generalizations of Eilenberg’s and Reiterman’s theorems have been obtained:

- Pippenger (1997)
- Poláš (2001)

No one of these results provides a common and most general framework for these kinds of results.

NOT a modular collection of results
Duality in Logic

- Duality and recognizable languages
- The syntactic monoid as a dual space

Duality and recognizable languages

Duality applied in the setting of recognizable languages
Quotient operations

\[ L(A) = (ab)^* \cup (ab)^* a \]

\[ a^{-1}L = \{ u \in A^* \mid au \in L \} = (ba)^* b \cup (ba)^* \]

\[ La^{-1} = \{ u \in A^* \mid ua \in L \} = (ab)^* \]

\[ b^{-1}L = \{ u \in A^* \mid bu \in L \} = \emptyset \]

NB! These are recognized by the same underlying machine.
Capturing the underlying machine

Given a recognizable language $L$ the underlying machine is captured by the Boolean algebra $\mathcal{B}(L)$ of languages generated by

$$\left\{ x^{-1}L y^{-1} \mid x, y \in A^* \right\}$$

NB! This generating set is finite since all the languages are recognized by the same machine with varying sets of initial and final states.

NB! $\mathcal{B}(L)$ is closed under quotients since the quotient operations commute with all the Boolean operations.
The residuation ideal generated by a language

Since $\mathcal{B}(L)$ is finite it is also closed under residuation with respect to arbitrary denominators.

For any $K \in \mathcal{B}(L)$ and any $S \in A^*$

$$S \setminus K = \bigcap_{u \in S} u^{-1}K \in \mathcal{B}(L)$$

$$K/S = \bigcap_{u \in S} Ku^{-1} \in \mathcal{B}(L)$$

**Theorem:** [GGP2008] For a recognizable language $L$, the dual space of the algebra $(\mathcal{B}(L), \cap, \cup, (\cdot)^c, 0, 1, \setminus, /)$ is the syntactic monoid of $L$.

- including the product operation!
Recognition by monoids

A language \( L \subseteq A^* \) is recognized by a finite monoid \( M \) provided there is a monoid morphism \( \varphi : A^* \to M \) with \( \varphi^{-1}(\varphi(L)) = L \).

\[ \begin{align*}
L \text{ recognizable by a finite automaton} & \implies \mathcal{B}(L) \hookrightarrow \mathcal{P}(A^*) \text{ finite residuation ideal} \\
& \implies A^* \twoheadrightarrow M(L) \text{ finite monoid quotient} \\
& \implies L \text{ is recognizable by a finite monoid} \\
& \implies L \text{ recognizable by a finite automaton}
\end{align*} \]
The recognizable subsets of an abstract algebra

\[ \text{Rec}(A) = \{ \varphi^{-1}(S) \mid \varphi : A \to F \text{ hom, } F \text{ finite, } S \subseteq F \} \]
The dual of \((\text{Rec}(A), /, \backslash)\)

**Theorem:** [GGP2008] The dual space of

\[ \text{Rec}(A) + \text{residuals of liftings of operations} \]

is the profinite completion \(\hat{A}\) with its operations.

In particular, the duals of the residual operations are **FUNCTIONAL** and **CONTINUOUS**.

In binary case:

\[ R_{(\backslash, /)} = \cdot : \hat{A} \times \hat{A} \rightarrow \hat{A} \]
Reiterman’s pseudoterms

Duality yields a 1-1 correspondence between continuous monoid morphisms

\[ \hat{\varphi} : \hat{A}^* \to F, \quad F \text{ a finite monoid} \]

and maps

\[ \varphi : A \to F, \quad F \text{ a finite monoid.} \]

**Theorem:** [GGP2008]
The dual space \((\hat{A}^*, \tau, \cdot)\) of the residuated Boolean algebra \((\text{Rec}(A^*), \cdot, /, \backslash)\) is Reiterman’s space of pseudoterms over \(A\).
Categorical dualities

\[
\text{subalgebras} \quad \longleftrightarrow \quad \text{quotient structures}
\]

\[
\text{quotient algebras} \quad \longleftrightarrow \quad (\text{generated}) \text{ substructures}
\]

\[
\text{products} \quad \longleftrightarrow \quad \text{sums}
\]

\[
\text{sums} \quad \longleftrightarrow \quad \text{products}
\]
Classes of languages

\( \mathcal{C} \) a class of recognizable languages closed under \( \cap \) and \( \cup \)

\[
\begin{align*}
\mathcal{C} &\rightarrow Rec(A^*) &\rightarrow \mathcal{P}(A^*) \\
DUALLY
X_\mathcal{C} &\leftarrow \widehat{A^*} &\leftarrow \beta(A^*)
\end{align*}
\]

That is, \( \mathcal{C} \) is described dually by \textbf{EQUATING} elements of \( \widehat{A^*} \).

This is Reiterman’s theorem in a very general form.
The mechanism behind Reiterman’s theorem

Let \( A \) be an abstract algebra.

\( B \) a Boolean subalgebra (sublattice) of \( \text{Rec}(A) \)

corresponds to

\( E \subseteq \hat{A} \times \hat{A} \) (in)equations of elements of the profinite completion of \( A \)

This correspondence is given by the following Galois connection:

\[ \mathcal{P}(\text{Rec}(A)) \leftrightarrow \mathcal{P}(\hat{A} \times \hat{A}) \]

\[ S \mapsto \approx_S = \{(x, y) \in X \mid \forall b \in S \quad (b \in y \iff b \in x)\} \]

and

\[ E \mapsto B_E = \{b \in B \mid \forall (x, y) \in E \quad (b \in y \iff b \in x)\} \]
A fully modular Eilenberg-Reiterman theorem

Using the fact that sublattices of $\text{Rec}(A^*)$ correspond to Stone quotients of $\widehat{A}^*$ we get a vast generalization of the Eilenberg-Reiterman theory for recognizable languages.

### Closed under

<table>
<thead>
<tr>
<th>Closed under</th>
<th>Equations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\cup, \cap$</td>
<td>$u \rightarrow v$</td>
<td>$\hat{\varphi}(v) \in \varphi(L) \Rightarrow \hat{\varphi}(u) \in \varphi(L)$</td>
</tr>
<tr>
<td>quotienting</td>
<td>$u \leq v$</td>
<td>for all $x, y$, $xuy \rightarrow xvy$</td>
</tr>
<tr>
<td>complement</td>
<td>$u \leftrightarrow v$</td>
<td>$u \rightarrow v$ and $v \rightarrow u$</td>
</tr>
<tr>
<td>quotienting and complement</td>
<td>$u = v$</td>
<td>for all $x, y$, $xuy \leftrightarrow xvy$</td>
</tr>
</tbody>
</table>

### Interpretation of variables

<table>
<thead>
<tr>
<th>Closed under inverses of morphisms</th>
<th>Interpretation of variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>all morphisms</td>
<td>words</td>
</tr>
<tr>
<td>non-erasing morphisms</td>
<td>nonempty words</td>
</tr>
<tr>
<td>length multiplying morphisms</td>
<td>words of equal length</td>
</tr>
<tr>
<td>length preserving morphisms</td>
<td>letters</td>
</tr>
</tbody>
</table>
An example

\[ \mathcal{C} = \text{class of languages generated by finite } \cap, \cup \text{ from the factor languages } \langle u \rangle = A^* u A^*, \ u \in A^* \]

These are called positively strongly locally testable (PSLT) languages reflecting the property of their recognizing automata.

Algebraic identities for PSLT: (making the class decidable!)

\[
\begin{align*}
x^\omega y x^\omega &= x^\omega y x^\omega y x^\omega \\
x^\omega y x^\omega z x^\omega &= x^\omega z x^\omega y x^\omega \\
x^\omega y x^\omega &\leq x^\omega \\
x^\omega u y^\omega v x^\omega &\iff y^\omega v x^\omega u y^\omega \\
y(x y)^\omega &\iff (x y)^\omega \iff (x y)^\omega x
\end{align*}
\]
Eilenberg, Reiterman, and Stone

Classes of monoids

(1) Eilenberg theorems
(2) Reiterman theorems
(3) extended Stone/Priestley duality

(3) allows generalization beyond pseudo-varieties and regular languages
Equational theory of lattices of languages


The (two outer) theorems are proved using the duality between subalgebras (possibly with additional operations) and dual quotient spaces.
A few References


