Stone duality and the recognisable languages over an algebra

Mai Gehrke[1]

Radboud University Nijmegen, The Netherlands

Abstract. This is a theoretical paper giving the extended Stone duality perspective on the recently discovered connection between duality theory as studied in non-classical logic and theoretical computer science and the algebraic theory of finite state automata. As a bi-product we obtain a general result about profinite completion, namely, that it is the dual under extended Stone duality of the recognisable languages over the original algebra equipped with certain residuation operations.

1 Introduction

In the algebraic theory of finite state automata, finite semigroups are associated with the regular or recognisable languages which are exactly the ones recognised by finite state automata. The highlights of this theory include tools such as syntactic monoids as defined by Rabin and Scott [12], which are powerful algebraic invariants of finite state automata, and the Reiterman theorems that give equational properties for various classes of automata, thus rendering membership in these classes decidable. In [3] new results were reported identifying many of these tools and theorems as special cases of extended Stone duality and thereby vastly generalising them. There the focus was on the impact of these results for automata theory and the form of the underlying duality results was somewhat hidden. Nevertheless, the entire development may be seen from a duality theory perspective. Showing this is the purpose of this paper.

The paper is organised as follows: we start with the necessary preliminaries on duality, then we look at algebras as relational frames and identify the ultrafilter extension and the residuation operations both of which will turn out to play a central role. We then look at the algebra of recognisable subsets of an algebra and show that, with the residuation operations, it is the dual of the profinite completion for any algebra. Finally we *briefly* sketch how these results tie up with the tools of automata theory such as syntactic monoids, profinite terms and Reiterman theorems. For more details and examples on this see [3] and [10].

We work with algebras M with one binary operation which we denote as multiplication. Eventually we will apply the theory in the case of monoids, and finitely generated free monoids in particular, but most of what we will talk about here works for algebras in any signature of operations of finite arity.

2 Preliminaries on duality

In this section we collect a few basic and well-known facts about extended duality that we will need. Stone duality lies at the core of many dualities between algebras and coalgebras as it connects Boolean algebras with (topologised) sets. Extended Stone or Priestley duality takes additional structure into account and treats dualities between algebras and coalgebras based on this duality.

One fundamental perspective on duality is that it is about representing abstract algebras in concrete ones, that is, embedding an abstract distributive lattice in a concrete one consisting of subsets with the operations of $\wedge$ and $\vee$ provided by the set-theoretic intersection and union. The embedding perspective is emphasised in the approach introduced by Jónsson and Tarski in their 1951 paper [9] on so-called canonical extensions. This approach has since been generalised to distributive lattices [4] and is particularly useful when additional structure (i.e., algebras and coalgebras) must be treated.

A canonical extension [4] of a distributive lattice D is an embedding $e : D \hookrightarrow D^\sigma$ with the properties:

(1) D^σ is a *complete* lattice;
(2) e is *dense* in the sense that each element of D^σ is a join of meets and a meet of joins of elements from D;
(3) e is *compact* in the sense that for $S, T \subseteq D$ we have $\bigwedge e(S) \leqslant \bigvee e(T)$ implies the existence of finite subsets $S' \subseteq S$ and $T' \subseteq T$ with $\bigwedge S' \leqslant \bigvee T'$.

Each distributive lattice, D, has a canonical extension and it is unique up to isomorphism. In the presence of the Axiom of Choice, it is an equivalent encoding of the dual space of D. Given a distributive lattice D and its canonical extension $D \hookrightarrow D^\sigma$, one may obtain the points of the dual space of D as the set $J^\infty(D^\sigma)$ of completely join irreducible elements of D^σ ordered as a subposet of D^σ and equipped with the topology generated by the basis of subsets of the form $\hat{d} = \{x \in J^\infty(D^\sigma) \mid x \leqslant d\}$ for $d \in D$. Conversely, given the Priestley dual $(X, \leqslant, \tau)$ with the corresponding embedding of D into the clopen downsets of the dual, we obtain the canonical extension by considering the codomain of this embedding to be the collection $\mathcal{D}(X)$ of downsets of $(X, \leqslant)$.

Given a distributive lattice D and its canonical extension $D \hookrightarrow D^\sigma$, we will think of D as a subset of D^σ. We define $K(D^\sigma)$ to be the $\bigwedge$-closure of D and refer to the elements of $K(D^\sigma)$ as closed elements. Dually, $O(D^\sigma)$ is the $\bigvee$-closure of D in D^σ and the elements of $O(D^\sigma)$ are referred to as open elements. The compactness of the embedding $D \hookrightarrow D^\sigma$ is the lattice theoretic encoding of the fact that the dual space $Spec(D)$ of D is topologically compact. It is a consequence of compactness that $K(D^\sigma) \cap O(D^\sigma) = D$ so that the 'clopen' elements of D^σ are exactly the elements of D.

The points of the dual space of D may be recognised in D^σ either as the set $J^\infty(D^\sigma)$ of completely join-prime elements or as the dually defined set $M^\infty(D^\sigma)$ of completely meet-prime elements. These two subposets of D^σ are isomorphic via the isomorphism

$$\begin{aligned}\kappa : J^\infty(D^\sigma) &\to M^\infty(D^\sigma)\\ x &\mapsto \kappa(x) = \bigvee\{u \in D^\sigma \mid x \nleq u\}.\end{aligned}$$

In fact, just as in finite distributive lattices, the completely join-prime and completely meet-prime elements come in pairs $(x, \kappa(x))$ that split the lattice in two disjoint pieces: $D^\sigma = {\uparrow}x \cup {\downarrow}\kappa(x)$. Or, in an alternative formulation which we shall make use of here, we have for $x \in J^\infty(D^\sigma)$

$$\forall u \in D^\sigma \ (x \leqslant u \iff u \nleq \kappa(x)).$$

The elements of $J^\infty(D^\sigma)$ correspond to the prime filters of D (*with the reverse order of inclusion*) via $x \mapsto (\uparrow x) \cap D$ for $x \in J^\infty(D^\sigma)$ and $p \mapsto \bigwedge p$ where the meet is taken in D^σ for p a prime filter of D. The elements of $M^\infty(D^\sigma)$ correspond to the prime ideals of D, and the isomorphism κ witnesses the correspondence given by set-complementation between prime filters and prime ideals of a distributive lattice. A homomorphism, $h : D \to E$, between bounded distributive lattices extends uniquely to a complete homomorphism $h^\sigma : D^\sigma \to E^\sigma$, and the lower adjoint of such a map sends $X_E = J^\infty(E^\sigma)$ into $X_D = J^\infty(D^\sigma)$. This is the dual map which is order preserving and continuous.

In extended Priestley or Stone duality [7], additional operations on a distributive lattice are captured by additional relational structure on the dual space, see also [5, 6]. Here we give a brief description of the relational dual of the additional operations we will be most concerned with. It is easiest to start with an operation $\cdot : D \times D \to D$ preserving $\vee$ in each coordinate. Because the embedding of D in D^σ is dense, D^σ is $\bigvee$-generated by $K(D^\sigma)$. Thus we may extend $\cdot : D \times D \to D$ to an operation on D^σ in two tempi: For $x_1, x_2 \in K(D^\sigma)$ we let

$$x_1 \cdot^\sigma x_2 = \bigwedge\{d_1 \cdot d_2 \mid x_i \leqslant d_i \in D, i = 1, 2\}$$

and for $u_1, u_2 \in D^\sigma$ in general we let

$$u_1 \cdot^\sigma u_2 = \bigvee\{x_1 \cdot^\sigma x_2 \mid u_i \geqslant x_i \in K(D^\sigma), i = 1, 2\}.$$

This is an extension of the original multiplication on D preserving $\bigvee$ in each coordinate, see [4, Theorem 2.21, p. 25]. Thus its action on D^σ is completely captured by its restriction to $X = J^\infty(D^\sigma)$ which is given by:

$$R_{\,\cdot} = \{(x, y, z) \in X^3 \mid x \cdot^\sigma y \geqslant z\}.$$

This yields a relation R that is order compatible in the sense that

$$[\geqslant \times \geqslant] \circ R \circ \geqslant = R$$

if we think of R as a relation from $X \times X$ to X. Topologically, as derived in [7], such a relation R comes from an operation $\cdot : D \times D \to D$ if and only if

(1) For each $x \in X$ the set $R[\_, \_, x]$ is closed;
(2) For all U, V clopen downsets of X the set $R[U, V, \_]$ is clopen;
(Notice that our last coordinate is the first coordinate in [7]).

For operations with other preservation properties, one has to apply some order duality. For this to work it is important that all domain coordinates transform to joins in the codomain or all transform to meets. For example, for an operation $\backslash : D \times D \to D$ that sends joins in the first coordinate to meets and meets in the second coordinate to meets (when the other coordinate remains fixed), we must first extend $\backslash$ to $K(D^\sigma) \times O(D^\sigma)$ by setting

$$x \backslash^\pi y = \bigvee \{d \backslash d' \mid x \leqslant d \in D \text{ and } y \geqslant d' \in D\}$$

for $x \in K(D^\sigma)$ and $y \in O(D^\sigma)$ and then let

$$u \backslash^\pi v = \bigwedge \{x \backslash^\pi y \mid u \geqslant x \in K(D^\sigma) \text{ and } v \leqslant y \in O(D^\sigma)\}$$

for $u, v \in D^\sigma$. This results in an operation on D^σ which sends arbitrary joins in the first coordinate to meets, and arbitrary meets in the second coordinate to meets. Consequently the operation is fully captured by its action on $J^\infty(D^\sigma) \times M^\infty(D^\sigma)$ which is encoded on $X = J^\infty(D^\sigma)$ by

$$S_{\backslash} = \{(x, y, z) \in X^3 \mid x(\backslash)^\pi \kappa(z) \leqslant \kappa(y)\}.$$

In the sequel we will be applying these results in a situation where we have operations $(\cdot, \backslash, /)$ that form a residuated family on D. That is, for all $a, b, c \in D$ we have

$$a \cdot b \leqslant c \iff b \leqslant a \backslash c \iff a \leqslant c/b.$$

In this case one can prove that the extended operations $(\cdot^\sigma, \backslash^\pi, /^\pi)$ also form a residuated family and consequently that $R_{\cdot}, S_\backslash$ and $S_/$ are identical relations given simultaneously by

$$R(x, y, z) \iff x \cdot^\sigma y \geqslant z \iff x \backslash^\pi \kappa(z) \leqslant \kappa(y) \iff \kappa(z) /^\pi y \leqslant \kappa(x). \quad (1)$$

Given an order-compatible relation R, it always will give rise to a residuated family of maps on the lattice $\mathcal{D}(X)$ of downsets of X given by

$$\begin{aligned} S \cdot T &= R[S, T, \_] = \big\{n \mid \text{there exist } \ell, m \ \big[\ell \in S \text{ and } m \in T \text{ and } R(\ell, m, n)\big]\big\} \\ S \backslash T &= (R[S, \_, T^c])^c = \big\{m \mid \text{for all } \ell, n \ \big[(\ell \in S \text{ and } R(\ell, m, n)) \implies n \in T\big]\big\} \\ T/S &= (R[\_, S, T^c])^c = \big\{\ell \mid \text{for all } m, n \ \big[(m \in S \text{ and } R(\ell, m, n)) \implies n \in T\big]\big\}. \end{aligned}$$

However, one of these can be a topological dual without the other two being such. This is determined by the topological properties of the relation. As stated above, this multiplication $\cdot$ on $\mathcal{D}(X) \cong D^\sigma$ coming from R is the extension of an operation on D that has R as its dual relation if and only if

(1) For each $x \in X$ the set $R[\_, \_, x]$ is closed;
(2) For all U, V clopen downsets of X the set $R[U, V, \_]$ is clopen.

The properties for \ and / to be topological duals are, respectively:

(1) For each $x \in X$ the set $R[\_, x, \_]$ is closed;
(2) For all U clopen downset of X and V clopen upset of X, the set $R[U, \_, V]$ is clopen,

and

(1) For each $x \in X_B$ the set $R[x, \_, \_]$ is closed;
(2) For all U clopen downset of X and V clopen upset of X, the set $R[\_, U, V]$ is clopen.

3 Algebras as relational frames

Now we get to the subject proper of this work. One can think of an algebra M as a *relational structure*, playing a role dual to a Boolean algebra with operators. Indeed M is a relational structure as any n-ary operation is an $n+1$-ary relation (which just happens to be functional). We may lift this relation to an algebraic structure over the Boolean algebra, $\mathcal{P}(M)$, of all subsets of M. We work with the case of a single binary operation as it is typical. We will refer to the operation as a multiplication though we do not assume it to be associative. The multiplication lifts to a binary operation on $\mathcal{P}(M)$

$$XY = \{xy \mid x \in X \text{ and } y \in X\}.$$

The complex algebra (after Frobenius' *algebra of complexes* in group theory) of the structure $(M, \cdot)$ is the multimodal algebra $(\mathcal{P}(M), \cap, \cup, (\ )^c, \emptyset, M, \cdot)$ (in the sequel we will suppress the Boolean operations $\cap$, $\cup$, $(\ )^c$, $\emptyset$, M and only specify the additional operations, thus in this case $(\mathcal{P}(M), \cdot)$). Since the multiplication is obtained by relation lifting, it preserves arbitrary unions in each coordinate and is thus residuated. That is, there are operations

$$\backslash\ , / : \mathcal{P}(M) \times \mathcal{P}(M) \to \mathcal{P}(M)$$

such that, for all $H, K, L \in \mathcal{P}(M)$,

$$HK \subseteq L \iff K \subseteq H\backslash L \iff H \subseteq L/K.$$

More explicitly, the *left* and *right residuals* of L by K are defined by:

$$K\backslash L = \{m \in M \mid Km \subseteq L\} = \{m \in M \mid \text{ for all } u \in K,\ um \in L\}$$
$$L/K = \{m \in M \mid mK \subseteq L\} = \{m \in M \mid \text{ for all } u \in K,\ mu \in L\}.$$

We will see in the sequel that in order to understand M as a dual structure the residual operations are a lot more important than the lifted multiplication. This should come as no surprise since, in duality theory, duals of morphisms are given by residuation of the lifted maps. It is thus to be expected that if we think of M as a frame (with the forward direction of multiplication as the direction of the relation $\cdot$), then what we might call the quotient-operation-algebra $(\mathcal{P}(M), /, \backslash)$

(with the Boolean operations) should be its dual complex algebra. However, the algebra $\mathcal{P}(M)$ is closed under all three operations and is thus a residuated Boolean algebra $(\mathcal{P}(M), \cdot, \backslash, /)$.

We will be interested in subalgebras of $\mathcal{P}(M)$ that are not necessarily complete and atomic and thus we need the dual of $\mathcal{P}(M)$ under topological duality rather than under the discrete duality between complex algebras and their atom structures. The extended Stone dual of the residuated Boolean algebra, $(\mathcal{P}(M), \cdot, \backslash, /)$, is the topo-relational space $(\beta(M), \tau, R)$ where $(\beta(M), \tau)$ is the Stone-Čech compactification of the discrete space M (or equivalently the Stone dual of the Boolean algebra $\mathcal{P}(M)$). We have the embedding

$$\begin{aligned} M &\hookrightarrow \beta(M) \\ m &\mapsto \mu_m = \bigwedge\{L \in \mathcal{P}(M) \mid m \in L\} \end{aligned}$$

where the meet is taken in $\mathcal{P}(M)^\sigma$ and the resulting element, μ_m, is the atom corresponding to the principal ultrafilter generated by $m \in M$. The relation R is given by the definition in (1). In the modal logic literature this (or at least the non-topologised version) is known as the ultrafilter extension of the original frame $(M, \cdot)$. It is not hard to see that this is an extension of M. The following result is true about ultrafilter extensions also for non-functional frames.

Theorem 1. *Let $(M, \{f_\alpha\}_\alpha)$ be any algebra for a type of finitary operations. The ultrafilter extension of $(M, \{f_\alpha\}_\alpha)$ as a relational frame is the topo-relational structure $(\beta(M), \tau, \{R_\alpha\}_\alpha)$ where $M \hookrightarrow (\beta(M), \tau)$ is the Stone-Čech compactification of M as a discrete space, and R_α is the closure of the graph of f_α for each α. Furthermore, if f_α is n-ary, then the restriction of R_α to domain elements from A^n is functional and equal to f_α.*

If a function on a dense subset of a topological space has a continuous extension to the whole space then the graph of the extension is the closure of the graph on the dense subset, so the relation R above is the graph of this extension if it exists. Since the power set $\mathcal{P}(M)$ is closed under the complexified operations of M as well as each of the residuals, the dual relation satisfies all topological conditions for R being dual to each of these. In the binary case these are the six properties listed at the end of Section 2. Clearly this implies that R is continuous *if* it is functional. However, this is typically not the case. In particular, even for the monoid, $\mathbb{N}$, of non-negative integers under addition, the Stone-Čech compactification, $\beta(\mathbb{N})$, is well known not to admit any simultaneously right and left continuous extension of the addition on $\mathbb{N}$, see [8].

4 The algebra of recognisable subsets of an algebra

A fundamental notion in automata theory is that of recognition. In an algebraic form: A subset L of M is *recognised* by a surjective homomorphism $\varphi : M \to N$ if there is a $P \subseteq N$ such that $L = \varphi^{-1}(P)$ and L is *recognised by* N if there is a $\varphi : M \to N$ which recognises L. Here we are interested in finite recognition.

Definition 1. *Let M be an algebra. The recognisable subsets of M are those that are recognised by some finite algebra of the same type as M. That is,*

$$\mathrm{Rec}(M) = \{\varphi^{-1}(P) \mid \varphi : M \to F \text{ is an onto morphism, } F \text{ is finite, } F \supseteq P\}.$$

Proposition 1. *Let M be an algebra. Then $\mathrm{Rec}(M)$ is closed under the Boolean operations as well as under the residuals w.r.t. arbitrary subsets of M.*

Proof. If L is recognisable then L^c is recognised by the same morphism and the complementary subset. The intersection of two recognisable subsets is recognised by the image of the product map using the intersection of the product of the two subsets with that image. Finally, for any subsets S of M. If L is recognised by a monoid morphism $\varphi : M \to F$, then $S\backslash L$ and L/S are also recognised by φ as $\varphi^{-1}(\varphi(S)\backslash P) = S\backslash\varphi^{-1}(P)$ and $\varphi^{-1}(P/\varphi(S)) = \varphi^{-1}(P)/S$. □

In general $\mathrm{Rec}(M)$ is not closed under product, but as we have seen above it is always closed under the residuals. In fact, more is true since it is closed under taking the left or right residual with respect to *any* subset of M. That is, $\mathrm{Rec}(M)$ is a kind of *residuation ideal*. As we will see, this property has essential consequences. For classes of recognisable sets closed under finite intersections, closure under the residuals with arbitrary denominators amounts to the same as closure under the unary residuals which we call quotient operators.

Proposition 2. *Let M be an algebra and C a subset of $\mathrm{Rec}(M)$ closed under finite intersections. Then C is closed under a residual of one of the operations of M for any denominator in $\mathcal{P}(M)$ if and only if C is closed under the residual w.r.t. singleton denominators.*

Proof. Consider a binary operation $\cdot$ and its residual $\backslash$. The result follows easily from the fact that for an arbitrary subset S and a recognisable language L recognised by a homomorphism into a finite algebra, $\varphi : M \to F$, we have $S\backslash L = \varphi^{-1}(\varphi(S)\backslash P)$ where $P = \varphi(L)$, and $\varphi(S)\backslash P = \bigcap_{v\in S}\varphi(\{v\})\backslash P = \bigcap_{v\in S'}\varphi(v)\backslash P$ for some finite subset S' of S since $\varphi(S) \subseteq F$ is finite. That is, $S\backslash L = \varphi^{-1}(\bigcap_{v\in S'}\varphi(v)\backslash P) = \bigcap_{v\in S'}\varphi^{-1}(\varphi(v)\backslash P) = \bigcap_{v\in S'} v\backslash L$. □

From this result we see that the unary residuals, that is, the quotient operators and thus also the modal algebra $(\mathcal{P}(M), (v^{-1}(\ ), (\ )v^{-1})_{v\in M})$ play an important role for recognisable languages.

5 Profinite completions as dual spaces

We will show that the profinite completion of an algebra M is equal to the extended Stone dual of $\mathrm{Rec}(M)$ as a residuation ideal. We start by looking at the underlying Boolean algebra. Since $\mathrm{Rec}(M) \hookrightarrow \mathcal{P}(M)$ is a Boolean embedding, dually, we have a topological quotient map $\beta(M) \twoheadrightarrow \widehat{M}$ where $\widehat{M}$ is the dual space of $\mathrm{Rec}(M)$. In general the composition $M \hookrightarrow \beta(M) \twoheadrightarrow \widehat{M}$ is not injective.

Proposition 3. *Let M be an algebra. The map*

$$\begin{aligned} M &\to \widehat{M} \\ m &\mapsto \bigwedge\{L \in \mathrm{Rec}(M) \mid m \in L\} \end{aligned}$$

is an injection if and only if M is residually finite. In particular, for $M = A^*$, the free monoid over a finite set A, this map is injective.

Proof. The kernel, θ_M, of the above map is easily seen to be $\theta_M = \bigcap\{\theta \in Con(M) \mid M/\theta \text{ is finite}\}$. Notice that this kernel is always a congruence and that it is trivial if and only if the finite quotients of M separate the points of M. That is, exactly if M is residually finite. The fact that A^* is residually finite is not hard to prove. □

In fact more can be said than this proposition. The quotient M/θ_M is the residually finite reflection of M and $\widehat{M}$ is homeomorphic to the dual space of the Boolean algebra of recognisable subsets over M/θ_M. We will henceforth assume that M is residually finite.

Example 1. Let A be a finite set, A^* the free monoid generated by A. Since A^* is infinite, there are many points in the remainder of $\widehat{A^*}$, some of which have been used to great advantage in the algebraic theory of automata. For example, one may show that for any $u \in A^*$

$$u^\omega = \bigwedge\{L \in \mathrm{Rec}(A^*) : \exists n \ \forall k \ (n \leqslant k \ \Rightarrow \ u^{k!} \in L\}$$

is an element of $\widehat{A^*}$. To see this, let $L \in \mathrm{Rec}(A^*)$. Pick a monoid homomorphism $\varphi : A^* \to F$ into a finite monoid that recognises L with the set P. Let n be the order of the monoid F. Then it is an algebraic observation that $e = \varphi(u^{n!})$ must be an idempotent element of F, it follows that $e = \varphi(u^{k!})$ for all $k \geqslant n$ and since this element is in P or in P^c either L or L^c is above u^ω.

Theorem 2. *Let M be any algebra. The topological space underlying the profinite completion of M is the dual space, $\widehat{M}$, of the Boolean algebra* $\mathrm{Rec}(M)$.

Proof. The profinite completion of M is, by definition, the topological algebra obtained as the inverse limit of the finite quotients of M. For each such quotient $\varphi : M \to F$, viewed simply as a set map, the dual via the discrete duality corresponds to the Boolean algebra embedding $\varphi^{-1} : \mathcal{P}(F) \to \mathcal{P}(M)$. In fact, by definition of $\mathrm{Rec}(M)$, this map is into $\mathrm{Rec}(M)$ and $\mathrm{Rec}(M)$ is the direct union of the corresponding sub-Boolean algebras. Since direct limits are carried to inverse limits by the duality, the result follows. □

Profinite methods have been studied intensely in connection with automata theory [1]. The connection of the theorem was used directly in this context by Pippenger [11]. As we will now see the connection to duality also encompasses the additional operations and this is what really makes it powerful and interesting.

Lemma 1. *Let M be an algebra, $\widehat{M}$ the dual space of* $\mathrm{Rec}(M)$. *For each operation on M, the relation dual to the residual operations on* $\mathrm{Rec}(M)$ *is functional.*

Proof. We show it for a binary operation. By definition $R(x,y,z)$ if and only if $x(\backslash)^{\pi}\kappa(z) \leqslant \kappa(y)$ if and only if $y \nleqslant x(\backslash)^{\pi}\kappa(z)$. Since $x(\backslash)^{\pi}\kappa(z) = \bigwedge\{H\backslash L \mid x \leqslant H \in \mathrm{Rec}(M), z \nleqslant L \in \mathrm{Rec}(M)\}$, we obtain

$$\begin{aligned} R(x,y,z) \quad &\iff \quad \forall H, L \in \mathrm{Rec}(M) \quad [(x \leqslant H, z \nleqslant L) \ \Rightarrow \ y \nleqslant H\backslash L] \\ &\iff \quad \forall H, L \in \mathrm{Rec}(M) \quad [(x \leqslant H, y \leqslant H\backslash L) \ \Rightarrow \ z \leqslant L] \\ &\iff \quad \forall L \in \mathrm{Rec}(M) \quad [\exists H(x \leqslant H, y \leqslant H\backslash L) \ \Rightarrow \ z \leqslant L]. \end{aligned}$$

That is, given $x, y \in \widehat{M}$ we have $R(x,y,z)$ if and only if $z \leqslant \bigwedge \mu$ where $\mu = \{L \in \mathrm{Rec}(M) \mid \exists H(x \leqslant H, y \leqslant H\backslash L)\}$. We show that μ is an ultrafilter of $\mathrm{Rec}(M)$ and thus there is exactly one z with $R(x,y,z)$, namely $z = \bigwedge \mu$. Suppose $L_1, L_2 \in \mathrm{Rec}(M)$ and that there are $H_1, H_2 \in \mathrm{Rec}(M)$ with $x \leqslant H_i$ and $y \leqslant H_i\backslash L_i$ for $i = 1, 2$. Then $x \leqslant H_1 \cap H_2$ and

$$\begin{aligned} (H_1 \cap H_2)\backslash(L_1 \cap L_2) &= [(H_1 \cap H_2)\backslash L_1] \cap [(H_1 \cap H_2)\backslash L_2] \\ &\supseteq (H_1\backslash L_1) \cap (H_2\backslash L_2) \geqslant y \end{aligned}$$

and μ is closed under intersection. Now let $L \in \mathrm{Rec}(M)$ and let $\varphi : M \to F$ be a homomorphism into a finite algebra and $P \subseteq F$ such that $\varphi^{-1}(P) = L$. First observe that $x \leqslant M = \bigcup_{a \in F} \varphi^{-1}(a)$ implies $x \leqslant \varphi^{-1}(a)$ for some $a \in F$ since each $\varphi^{-1}(a) \in \mathrm{Rec}(M) \subseteq \mathrm{Rec}(M)^{\sigma}$ and x is completely join prime in $\mathrm{Rec}(M)^{\sigma}$. Furthermore, a residual operation always satisfies $K\backslash 1 = 1$ and since $1_{\mathrm{Rec}(M)} = M$, we have $y \leqslant M = \varphi^{-1}(a)\backslash M$. Since $\varphi^{-1}(F) = M$ then, as we saw in the proof of Proposition 1, $\varphi^{-1}(a)\backslash M = \varphi^{-1}(\varphi(\varphi^{-1}(a))\backslash F) = \varphi^{-1}(a\backslash F)$. Using the fact that residuals w.r.t. singletons preserve union, we now obtain $y \leqslant M = \varphi^{-1}(a\backslash F) = \varphi^{-1}(a\backslash P) \cup \varphi^{-1}(a\backslash P^c)$ and thus $y \leqslant \varphi^{-1}(a\backslash P)$ or $y \leqslant \varphi^{-1}(a\backslash P^c)$. Finally, using again the rewriting from Proposition 1, we get $\varphi^{-1}(a\backslash P) = \varphi^{-1}(a)\backslash\varphi^{-1}(P) = \varphi^{-1}(a)\backslash L$ and similarly $\varphi^{-1}(a\backslash P^c) = \varphi^{-1}(a)\backslash L^c$ so that $L \in \mu$ or $L^c \in \mu$. □

We now show that the continuity of a functional relation on a dual space is equivalent to the topological conditions guaranteeing that the relation is the topological dual of the residual operations corresponding to the relation.

Proposition 4. *Let X be a Boolean space and let $R \subseteq X^n \times X$ be the graph of a n-ary operation f, that is, $R(x_1, \ldots, x_n, z)$ if and only if $f(x_1, \ldots, x_n) = z$. Then , for each i with $1 \leqslant i \leqslant n$, the following conditions are equivalent:*

(1) *the operation f is continuous;*
(2) *for all $x \in X$, $R[\_\_, x, \_\_]$ (where x is in the ith spot) is closed in X^n and for all clopen sets $U_j, V \subseteq X$ the relational image $R[U_1, \ldots, U_{i-1}, \_, U_{i+1}, \ldots, V^c]$ is clopen.*

If these conditions are satisfied, the operation f is an open map if and only if for all $z \in X$, $R[\_\_, z]$ is closed in X^n and for all clopen sets $U_1, \ldots, U_n \subseteq X$, $R[U, \ldots, U_n, \_]$ is clopen.

Proof. We just prove the result for $i = 1$ to minimise notation. First we assume (2) holds and prove that f is continuous. Let $(x_1, \ldots, x_n) \in X^n$ with $z = f(x_1, \ldots, x_n) \in V$, where V is clopen in X. Since $R[x_1, \_\_]$ is closed and V is clopen, it follows that both $R[x_1, \_\_] \cap (X^n \times V)$ and $R[x_1, \_\_] \cap (X^n \times V^c)$ are closed. Furthermore, since the projection $\pi : X^{n-1} \times X \to X^{n-1}$ is a projection along a compact space, it is a closed map and thus both

$$\pi(R[x_1, \_\_] \cap (X^{n-1} \times V)) = f_{x_1}^{-1}(V)$$

and

$$\pi(R[x_1, \_\_] \cap (X^{n-1} \times V^c)) = f_{x_1}^{-1}(V^c)$$

are closed where $f_{x_1} : X^{n-1} \to X$ is given by $\overline{x} \mapsto f(x_1, \overline{x})$. The sets $f_{x_1}^{-1}(V)$ and $f_{x_1}^{-1}(V^c)$ are complementary, and thus they are also open. Since $\overline{x} = (x_2, \ldots, x_n) \in f_{x_1}^{-1}(V)$, there are clopens $U_2, \ldots, U_n$ with $\overline{x} \in U_2 \times \ldots \times U_n \subseteq f_{x_1}^{-1}(V)$. We have $x_1 \notin R[\_, U_2, \ldots, U_n, V^c]$, and thus $x_1 \in (R[\_, U_2, \ldots, U_n, V^c])^c = U_1$ which is clopen by condition (2). That is, $(x_1, \ldots, x_n) \in U_1 \times U_2 \times \ldots \times U_n$ and each U_i is clopen. Furthermore, if $(y_1, \ldots, y_n) \in U_1 \times U_2 \times \ldots \times U_n$ then $y_1 \in U_1 = (R[\_, U_2, \ldots, U_n, V^c])^c$ and thus

$$\begin{aligned} y_1 \notin\ & R[\_, U_2, \ldots, U_n, V^c] \\ &= \{y' \mid \exists (y'_2, \ldots, y'_n) \in U_2 \times \ldots \times U_n \ f(y', y'_2, \ldots, y'_n) \notin V\}. \end{aligned}$$

That is, for all $(y'_2, \ldots, y'_n) \in U_2 \times \ldots \times U_n$ we have $f(y_1, y'_2, \ldots, y'_n) \in V$ and in particular $f(y_1, y_2, \ldots, y_n) \in V$. We have shown then that $(x_1, \ldots, x_n) \in U_1 \times U_2 \times \ldots \times U_n \subseteq f^{-1}(V)$ and thus that f is continuous.

On the other hand, if f is continuous, then, for each $x_1 \in X$ we have that the function $f_{x_1} : X^{n-1} \to X$ as defined above is continuous and thus its graph, $R[x_1, \_\_]$, is closed in X^n. Also, by the definition of continuity, for any clopen set $V \subseteq X$ we have $f^{-1}(V) = R[\_\_, V^c]$ is clopen. But for clopen sets $U_2, \ldots, U_n \subseteq X$ we have that

$$R[\_, U_2, \ldots, U_n, V^c] = R[\_\_, V^c] \cap (U_2 \times \ldots \times U_n \times X)$$

which is is clopen.

Finally, assuming f is continuous, we have that $R[\_\_, z] = f^{-1}(\{z\})$ is closed and thus the first property adds no condition. The second property says that f maps clopen sets to clopen sets. Since forward image preserves unions, it follows that this condition is equivalent to f being an open map. □

Note that since the operations on $\widehat{M}$ are continuous extensions of the ones on M and since M is dense in $\widehat{M}$, it follows that $\widehat{M}$ satisfies exactly the same equations as M. By combining the above proposition and lemma and Theorem 2, we obtain the following result:

Theorem 3. *Let M be an algebra then, $\widehat{M}$, the dual space under the extended Stone duality of* $\mathrm{Rec}(M)$ *with the residuals of the liftings of the operations of M, is the profinite completion of M as a topological algebra.*

This result identifies profinite completions of algebras as special cases of extended Stone duality. This predicts potential cross-fertilisation between areas (e.g. of logic and theoretical computer science) where extended Stone duality methods are employed and areas (e.g. of algebra, geometry, functional analysis) where profinite completions are used. In fact, Proposition 4 indicates that even for more general topological algebras there is a connection. This theorem also gives a constructive access to profinite completions (including their algebraic operations!): Obtaining the extended dual space $\widehat{M}$ requires the Axiom of Choice in general, but one can always get the Boolean algebra with residuation operations, $\mathrm{Rec}(M)$, and the two carry the same information as they are dual to each other. As we will see in Section 7, the fruitfulness goes beyond this level. Sophisticated tools such as Reiterman theorems are also cases of extended Stone duality.

6 Syntactic monoids and profinite terms

The connection between automata theory and semigroup theory originates in the fact that every finite state automaton has a so-called syntactic monoid. A second fact central to the advanced algebraic theory of automata is the fact that, in the case where the algebra M is a finitely generated free algebra, the elements of $\widehat{M}$ may be viewed as the 'term algebra' for finite algebras of the given type.

Both of these facts are easy to understand from a duality point of view and depend just on the dual understanding of surjective Boolean topological algebra morphisms. We work with monoids from now on as these are the pertinent algebras for automata theory. A result more general than the following is proved in Mirte Dekkers' thesis [2, p.90].

Theorem 4. *Let A be a finite set, A^* the free monoid over A. The Boolean residuation ideals of $\mathrm{Rec}(A^*)$ correspond dually to the Boolean topological semigroup homomorphic images of $\widehat{A^*}$. That is, a Boolean algebra embedding $\varphi : B \hookrightarrow \mathrm{Rec}(A^*)$ embeds $(B, \backslash, /)$ as a residuation ideal if and only if the extended Stone dual of $(B, \backslash, /)$ is a Boolean topological monoid X and the continuous surjection, $f : \widehat{A^*} \to X$, dual to φ is a monoid morphism.*

Note that Boolean topological monoids that are finite are simply finite monoids.

We now outline how semigroups end up being related to automata. Given an automata $\mathcal{A}$ over the alphabet A, the associated language $L_{\mathcal{A}}$ is the set of words recognised by $\mathcal{A}$ (in the automata sense). It is easy to see that, for all $u, v \in A^*$, the language $u \backslash L_{\mathcal{A}} / v$ is recognised by an automaton obtained from $\mathcal{A}$ by moving the initial state and the set of final states around. Since this only results in finitely many automata, it follows that the residuation ideal generated by $\mathcal{A}$, $<L_{\mathcal{A}}>$, is finite. By extended duality we obtain the following result.

Theorem 5. *Let $\mathcal{A}$ be an automaton, $L_{\mathcal{A}}$ the associated language, then the dual of $<L_{\mathcal{A}}>$ is a finite quotient of $(\beta(A^*), R)$ that is a monoid.*

Proof. This follows easily from the fact that $<L_{\mathcal{A}}>$ is finite because A^* is dense in $\beta(A^*)$ so that it has to map onto the finite quotient and R is a monoid operation on A^*. □

The dual, $S(L_{\mathcal{A}})$, of $<L_{\mathcal{A}}>$ is the syntactic monoid of $L_{\mathcal{A}}$. Note that by the way duality works, the languages in $<L_{\mathcal{A}}>$ are recognised by $S(L_{\mathcal{A}})$ (in the semigroup sense) and thus belong to $\mathrm{Rec}(A^*)$. Conversely, every 'stamp' $\varphi : A^* \to F \supseteq P$ may be seen as an automaton that recognises $\varphi^{-1}(P)$ so that the languages recognised by automata are exactly those in $\mathrm{Rec}(A^*)$.

We now turn to the profinite terms. Let $A = \{a_1, \ldots, a_n\}$ be a finite set, A^* the free monoid freely generated by A, and F be a finite monoid. If we see the elements of A as variables, then an evaluation of these variables in F is a set function $\varphi : a_i \mapsto m_i \in F$. By freeness of A^* over A this uniquely extends to a surjective monoid homomorphism $\varphi^* : A^* \to F'$ with F' a submonoid of F. This map in turn gives an embedding

$$(\varphi^*)^{-1} : \mathcal{P}(F') \hookrightarrow \mathcal{P}(A^*)$$

of $(\mathcal{P}(F'), \backslash, /)$ as a residuation ideal. Now, by the definition of recognisable languages, in fact, $(\varphi^*)^{-1}$ maps into $\mathrm{Rec}(A^*)$ and by the above theorem, such an embedding corresponds to a Boolean topological semigroup quotient

$$\widehat{\varphi} : \widehat{A^*} \to X'_F.$$

But for finite algebras, the topological and the discrete dual coincide, and thus X'_F is just F' and we have interpreted each element of $\widehat{A^*}$ in F. That is, for $x \in \widehat{A^*}$, we have a term function $x^F(a_1, \ldots, a_n) : F^n \to F$ where, for each tuple $(m_1, \ldots, m_n) \in F^n$ we set $x^F(m_1, \ldots, m_n) = \widehat{\varphi}(x)$ where $\widehat{\varphi}$ is obtained as above from the map $\varphi : A \to F$ which maps a_i to m_i.

Example 2. Recall that in Example 1, we introduced, for each word $u \in A^*$ the profinite word $u^\omega = \bigwedge\{L \in \mathrm{Rec}(A^*) : \exists n\ \forall k\ (n \leqslant k \Rightarrow\ u^{k!} \in L\}$. Let F be a finite monoid and $m \in F$. We now show that $(a^\omega)^F(m) = m^\omega$ is the unique idempotent in the cyclic semigroup generated by m in F. If $A = \{a\}$ then $A^* = \mathbb{N}$, and if $\varphi : a \mapsto m$ then $\varphi^* : n \mapsto m^n \in F$. As mentioned in Example 1, $e = m^{n!}$ where $n = |F|$ is the unique idempotent in the cyclic semigroup generated by m in F. We have $\widehat{\varphi}(a^\omega) \leqslant e$ if and only if $a^\omega \leqslant (\varphi^*)^{-1}(e)$ and $(\varphi^*)^{-1}(e) = \{\ell \mid m^\ell = e\} \supseteq \{k! \mid k \geqslant n\} \geqslant a^\omega$. So indeed, $\widehat{\varphi}(a^\omega) \leqslant e$, and since e is an atom, it follows that $\widehat{\varphi}(a^\omega) = e$.

7 Duality for subalgebras and Eilenberg-Reiterman theorems

In this final section we will sketch how Eilenberg-Reiterman theorems essentially are special cases of duality theory for subalgebras. This yields the main theorem of [3]. Let $A \hookrightarrow B$ be an embedding of bounded distributive lattices. Then A gives rise to a quasiorder on X_B given by

$$x \preceq y \iff \forall\, a \in A\ (y \leqslant a \ \Rightarrow\ x \leqslant a)$$

where $\leqslant$ is the order in B^σ. It is easy to verify that $\preceq$ is a quasiorder extending the order on X_B.

Definition 2. *Let B be a bounded distributive lattice, X_B the dual frame of B. A quasiorder $\preceq$ on X_B extending the order $\leqslant$ on X_B is said to be compatible provided it satisfies*

$$\forall x, y \in X_B \quad [x \not\preceq y \;\Rightarrow \exists a \in B \;(y \leqslant a \text{ and } x \nleqslant a \text{ and } \hat{a} \text{ is a } \preceq\text{-downset})].$$

The set of compatible quasiorders on X_B is a poset under set inclusion.

This yields a dual characterisation of bounded sublattices.

Theorem 6. *Let B be a bounded distributive lattice, X_B the dual frame of B. The assignments*

$$E \mapsto A_E = \{a \in B \mid \forall (x, y) \in E \;(y \leqslant a \;\Rightarrow x \leqslant a)\}$$

for $E \subseteq X \times X$ and

$$S \mapsto \preceq_S = \{(x, y) \in X \mid \forall a \in S \;(y \leqslant a \;\Rightarrow x \leqslant a)\}$$

for $S \subseteq B$ establish a Galois connection whose Galois closed sets are the compatible quasiorders and the bounded sublattices, respectively.

Eilenberg theorems relate classes of languages with classes of finite monoids, Reiterman theorems classes of finite monoids and equational theories in profinite terms. The above result, applied to $B = \mathrm{Rec}(A^*)$, relates classes of languages and equational theories, thus yielding an 'Eilenberg-Reiterman theorem'. For $u, v \in \widehat{A^*}$, we write an 'equation' of this most general form as $u \to v$. As above, such an equation holds for a language $L \in \mathrm{Rec}(M)$ if and only if $u \leqslant L$ implies $v \leqslant L$. Note that if $\varphi : A^* \to F$ is the syntactic monoid of L with $L = \varphi^{-1}(P)$, then this means that the 'stamp' $\varphi : A^* \to F \supseteq P$ satisfies $u \to v$, namely $\widehat{\varphi}(u) \in P$ implies $\widehat{\varphi}(v) \in P$. The above theorem specialises to the following result.

Theorem 7. *A set of recognisable languages of A^* is a lattice of languages if and only if it can be defined by a set of equations of the form $u \to v$, where $u, v \in \widehat{A^*}$. Furthermore, given $\mathcal{D} \subseteq \mathcal{P}(A^*)$, the set of all equations $u \to v$ that hold in $\mathcal{D}$ form a compatible quasiorder on the space $\widehat{A^*}$.*

Note that Boolean subalgebras are exactly those for which the corresponding compatible quasiorder is an equivalence relation. Writing $u \leftrightarrow v$ for ($u \to v$ and $v \to u$), we get an equational description of the Boolean algebras of languages.

Corollary 1. *A set of recognisable languages of A^* is a Boolean algebra of languages if and only if it can be defined by a set of equations of the form $u \leftrightarrow v$, where $u, v \in \widehat{A^*}$.*

We say that a lattice of recognisable languages $\mathcal{Q}$ is closed under quotienting provided, for every $L \in \mathcal{Q}$ and $v \in A^*$, $v^{-1}L$ and Lv^{-1} are also in $\mathcal{Q}$ and we call $\mathcal{Q}$ a quotienting subalgebra of $\mathrm{Rec}(A^*)$. As we've seen in Proposition 2, $\mathcal{Q}$

is a quotienting subalgebra if and only if it is a residuation ideal of $\mathrm{Rec}(A^*)$. By Theorem 4 these correspond to Priestley quotients of $\widehat{A^*}$ that are also monoid quotients. Consequently, if for u and v in $\widehat{A^*}$ we say that L *satisfies the equation* $u \leqslant v$ if, for all $x, y \in \widehat{A^*}$, it satisfies the equation $xvy \to xuy$ (that is, we generate a monoid quotient) then we obtain the following theorem.

Theorem 8. *A set of recognisable languages of A^* is a lattice of languages closed under quotients if and only if it can be defined by a set of equations of the form $u \leqslant v$, where $u, v \in \widehat{A^*}$.*

For a language L and the quotienting lattice $\mathcal{Q}_L$ generated by L we get the following formulation in terms of ordered syntactic monoids.

Proposition 5. *Let L be a recognisable language of A^*, let $(M, \leqslant_L)$ be its syntactic ordered monoid and let $\varphi : A^* \to M$ be its syntactic morphism. Then L satisfies the equation $u \leqslant v$ if and only if $\widehat{\varphi}(u) \leqslant_L \widehat{\varphi}(v)$.*

Theorem 8 can be readily extended to Boolean algebras. Let u and v be two profinite words. We say that a recognisable language L *satisfies the equation* $u = v$ if it satisfies the equations $u \leqslant v$ and $v \leqslant u$. Proposition 5 now gives immediately:

Corollary 2. *A set of recognisable languages of A^* is a Boolean algebra of languages closed under quotients if and only if it can be defined by a set of equations of the form $u = v$, where $u, v \in \widehat{A^*}$.*

Example 3. A language with zero is a language whose syntactic monoid has a zero. The class of regular languages with zero is closed under Boolean operations and quotients, but *not* under inverse of morphisms so that this example isn't covered by previous results. One can show that a regular language has a zero iff it satisfies the equations $u\rho_A = \rho_A = \rho_A u$ for all $u \in A^*$. Here ρ_A is the limit of the sequence $(v_n)_{n \geqslant 0}$ where $v_0 = u_0, v_{n+1} = (v_n u_{n+1} v_n)^{(n+1)!}$ obtained by fixing a total order on A and letting $u_0, u_1, \ldots$ be the ordered sequence of all words of A^* in the induced shortlex order. For more details and further examples, see [3].

So far our 'equations' are 'local', that is, they are not invariant under substitution. The last ingredient of the original Reiterman theorem is this invariance. Substitutions are given by maps $A \to B^*$ where B is another finite alphabet, or equivalently monoid homomorphisms $f : A^* \to B^*$. We define a *class of recognisable languages* to be a correspondence $\mathcal{V}$ which associates with each alphabet A a set $\mathcal{V}(A^*)$ of recognisable languages of A^*. Let $\mathcal{C}$ be a class of morphisms between finitely generated free monoids that is closed under composition and contains all length-preserving morphisms. Examples include the classes of all length-preserving morphisms (morphisms for which the image of each letter is a letter), of all length-multiplying morphisms (morphisms such that, for some integer k, the length of the image of a word is k times the length of the word), all non-erasing morphisms (morphisms for which the image of each letter is a non-empty word), all length-decreasing morphisms (morphisms for which the image of each letter is either a letter of the empty word) and all morphisms. We say a class $\mathcal{V}$ is closed under $\varphi\colon A^* \to B^*$ provided $L \in \mathcal{V}(B^*)$ implies $\varphi^{-1}(L) \in \mathcal{V}(A^*)$. Since substitutions extend to the profinite terms $\widehat{f} : \widehat{A^*} \to \widehat{B^*}$, a class $\mathcal{V}$ is closed under f if and only if the corresponding class of equations is closed under the substitution $\widehat{f}$. In summary we obtain a fully modular generalised Reiterman theorem that is summed up in the following table.

Closed under	**Equations**	**Definition**
$\cup, \cap$	$u \to v$	$\hat{\eta}(u) \in \eta(L) \Rightarrow \hat{\eta}(v) \in \eta(L)$
quotient	$u \leqslant v$	$xuy \to xvy$
complement	$u \leftrightarrow v$	$u \to v$ and $v \to u$
quotient and complement	$u = v$	$xuy \leftrightarrow xvy$
Closed under inverse of morphisms		**Interpretation of variables**
all morphisms		words
nonerasing morphisms		non-empty words
length multiplying morphisms		words of equal length
length preserving morphisms		letters

References

1. J. Almeida, *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1994.
2. M. Dekkers, Stone duality: An application in the theory of formal languages, Master's thesis, Radboud Universiteit Nijmegen, the Netherlands, December 2008.
3. M. Gehrke, S. Grigorieff and J.-E. Pin, Duality and Equational Theory of Regular Languages, *Lect. Notes Comp.Sci. (ICALP)* **5125** (2008), 246–257.
4. M. Gehrke and B. Jónsson, Bounded distributive lattices expansions, *Mathematica Scandinavica* **94**,2 (2004), 13–45.
5. M. Gehrke and H. A. Priestley, Canonical extensions of certain algebras with binary operations, *J. Pure Appl. Alg.* **209** (2007), 269–290.
6. M. Gehrke and H. A. Priestley, Duality for certain algebras with binary operations via their canonical extensions, *Stud. Log.* **86**,1 (2007), 31–68.
7. R. Goldblatt, Varieties of complex algebras, *APAL* **44** (1989), 173–242.
8. N. Hindman and D. Strauss, *Algebra in the Stone-Čech compactification*, *de Gruyter Expositions in Mathematics* vol. 27, de Gruyter & Co., 1998.
9. B. Jónsson and A. Tarski, Boolean algebras with operators I, *Amer. J. Math.* **73** (1951), 891–939.
10. J.-E. Pin, Profinite Methods in Automata Theory, in *STACS 2009*, Albers and Marion (ed.), pp. 31–50, *Leibniz International Proceedings in Informatics* vol. 3, Schloss Dagstuhl, 2009.
11. N. Pippenger, Regular Languages and Stone Duality, *Theory Comput. Syst.* **30**,2 (1997), 121–134.
12. M. O. Rabin and D. Scott, Finite automata and their decision problems, *Journal of IBM* **3** (1959), 114–125.