Lemma 5.12.8 *For the game automaton $\mathcal{A}_2$ over the alphabet $\{a\}$ consider the game $\Gamma(\mathcal{A}_2, v)$. Then in this game one of the players possesses a winning strategy f such that if p and q are positions of the winner and $lvr(p) = lvr(q)$, then $f(p) = f(q)$.*

Proof of the Lemma. Recall that $\Gamma(\mathcal{A}_2, v)$ is a GH-game. Consider the congruence relation E for this game. Note that $v(x) = a$ for all $x \in \mathcal{T}$. Therefore, for all positions p and q of this game, the $Node(p)$-residue of $(v, \mathcal{T})$ is the same as the $Node(q)$-residue of $(v, \mathcal{T})$. We conclude that the condition $lvr(p) = lvr(q)$ implies, by the Forgetful Determinacy Theorem, that $f(p) = f(q)$. This proves the lemma.

From this lemma we see that a winning strategy in the game $\Gamma(\mathcal{A}_2, v)$ is among the functions that depend on the last visitation records. Hence, there exists a winning strategy that belongs either to the set of all functions from $D(S)$ (displays on S) to S or to the set of all functions from $D(S)$ to $\{0, 1\}$. Let f be a function (strategy) from the former set and let g be a function (strategy) from the latter set. Consider the play

$$s_0, d_1, s_1, d_2, s_2, \ldots$$

consistent with these two functions f and g. Let p_i be the ith position of *Pathfinder* in this sequence. So

$$p_0 = s_0,\ p_1 = s_0 d_1 s_1, \ldots.$$

Consider the sequence

$$lvr(p_0), lvr(p_1), lvr(p_2), \ldots.$$

There exists an i and an $m \neq 0$ such that $lvr(p_i) = lvr(p_{i+m})$. Then it should be the case that $g(lvr(p_i)) = g(lvr(p_{i+m}))$. Since f and g are functions that depend on last visitation records and the above play is consistent with f and g, the play must eventually be periodic. Hence we can compute the period and find out whether or not the strategy f wins against g or the strategy g wins against f. The set of all functions from $D(S)$ (displays on S) to S or from $D(S)$ to $\{0, 1\}$ is finite. One of these functions, by the lemma above, is a winning strategy. We conclude that playing these strategies against each other, we can algorithmically find a desired winning strategy. Now $\mathcal{A}_2$ accepts $(v, \mathcal{T})$ if and only if *Automaton* has a winning strategy. We now leave the details of the proof to the reader. □

Corollary 5.12.1 *The equality and universality problems for Rabin automata are decidable.*

Proof. This follows, given the solutions to the complementation and the emptiness problems, the proofs of similar statements about Büchi automata. □

Exercise 5.12.5 *Prove the corollary above.*

6 Applications of Rabin Automata

Rabin automata have applications in many areas of mathematics and computer science. In this chapter our goal is to show how results about Rabin automata can be applied to prove that some theories of well-studied mathematical structures are decidable. This chapter consists of ten sections. The first four sections introduce the notions of algebraic structure, the monadic second order logic, the truth of formulas in algebraic structures, isomorphisms, and theories of classes of structures. Section 5 is devoted to proving that the monadic second order theory of two successor functions, known as $S2S$, is decidable. In particular, the section shows the relationship between definable relations in the monadic second order logic of two successors and languages accepted by Rabin automata.

All of the next sections use the decidability of $S2S$. Section 6 proves that the monadic second order theory of ω many successor functions is decidable. In Section 7 we prove that the monadic second order theory of countable linearly ordered sets is decidable. Section 8 shows that the monadic second order theory of countable unary algebras is decidable. In Section 9 we study Cantor's discontinuum, and prove that the theory of Cantor's discontinuum is decidable in a logic weaker than the monadic second order logic. We also prove that the theory of the topological space of the real interval $[0, 1]$ is decidable. Finally, in the last section, we introduce and study some known properties of Boolean algebras. We prove that the theory of all countable Boolean algebras with quantifications over ideals is decidable.

We note that the basic results of this chapter are decidability results. The proofs of these results involve algorithms whose correctness are based on some known algebraic facts about the structures. Thus, for example, in studying the theories of linearly ordered sets, we use (and prove) the fact that any countable linearly ordered set can be embedded into the linearly ordered set of rational numbers. In studying theories of unary algebras, we introduce enveloping unary algebras and use (and prove) the fact that any countable unary algebra can be embedded into an enveloping unary algebra. In the study of Cantor's discontinuum, we prove some topological results about the Cantor discontinuum. In the study of theories of Boolean algebras, we use (and prove) Stone's representation theorem. We show that clopen sets of Cantor's discontinuum form a Boolean algebra. We also use (and prove) the fact that any countable Boolean algebra is isomorphic to a factor of the Boolean algebra of clopen sets of Cantor's discontinuum. Thus, from this point of view, all the decidability results of this chapter can be considered as those obtained by exploiting the interplay between algebraic properties of structures and algorithms. All the decidability results provided in this chapter were proved by M. Rabin in 1969 in his famous paper "Decidability of Second-Order Theories and Automata on Infitite Trees."

6.1 Structures and Types

The goal is to develop a language powerful enough to reason about structures that arise in mathematics. To do this we first need to classify structures by their types. Then we develop a language, similar to the language of the monadic second order logic of one successor, that allows us to talk about properties of structures of the same type. We have already had experience in developing languages, so we will feel quite comfortable not going into much detail.

Examples of structures are linearly ordered sets, partially ordered sets, equivalence relations, (ω, S) and the tree (T, r_0, r_1). In this section we present a general definition of a structure. At this stage we can informally say that a *structure* is a set together with certain operations and relations which are defined on the set. Thus, the tuple $(\omega, S, \leq)$ is a structure that consists of the set ω, the successor operation S and the ordering relation $\leq$ on ω. Similarly, $(Z, +, \times, \leq)$ is also a structure that consists of the set Z, the addition operation, the multiplication operation, and the less than or equal to relation. For our purposes, we need to be more formal and give an exact definition of structures.

Definition 6.1.1 *A* **type** *is a sequence (which may be finite)*

$$F_0^{n_0}, F_1^{n_1}, \ldots, P_0^{m_0}, P_1^{m_1}, \ldots, c_0, c_1, \ldots,$$

where each $F_i^{n_i}$ *is called an* **operation symbol,** *each* $P_j^{m_j}$ *is called a* **relation symbol,** *and each* c_k *is called a* **constant.** *For the operation symbol* $F_i^{n_i}$, *the natural number* n_i *is called the* **arity of the operation symbol.** *Similarly, for the relation symbol* $P_j^{m_j}$, *the natural number* m_j *is called the* **arity of the relation symbol.** *If the sequence above is finite then the type is called a* **finite type.**

In order to specify a structure of the given type, we first need to pick up a nonempty set, say D, which will be called the **domain** of the structure. We also need to associate with each operational symbol $F_i^{n_i}$ an operation, denoted by $F_i^{n_i,D}$, on the domain D. The arity of the operation is n_i. In addition, we need to associate with each relational symbol $P_j^{m_j}$ a relation, denoted by $P_j^{m_j,D}$, on the domain D. The arity of the relation is m_j. Finally, we should pick up elements c_k^D from the domain which are associated with the constant symbols c_k. Hence, what we have is the structure

$$(D, F_0^{n_0,D}, F_1^{n_1,D}, \ldots, P_0^{m_0,D}, P_1^{m_1,D}, \ldots, c_0^D, c_1^D, \ldots).$$

A point here is that the structure we have just considered is *not* uniquely determined by the type. This is because each symbol $F_i^{n_i}$, for example, can be associated with many other operations on D. Let us now give a formal definition and then have some examples. Of course, we have the fixed type given above.

Definition 6.1.2 *A* **structure** *of the given type is the sequence*

$$(D, F_0^{n_0,D}, F_1^{n_1,D}, \ldots, P_0^{m_0,D}, P_1^{m_1,D}, \ldots, c_0^D, c_1^D, \ldots).$$

such that we have the following:

1. *D is a nonempty set called the* **domain.**
2. *Each $F_i^{n_i,D}$ is a fixed operation on the domain D. The arity of the operation is n_i.*
3. *Each $P_j^{m_j,D}$ is a fixed relation on the domain D. The arity of the relation is m_j.*
4. *Each c_k^D is a fixed element on the domain D called a* **constant.**

We denote this structure by $\mathcal{D}$.

We note that the order of operations, predicates and constants in the structure follows the same order of the corresponding operation symbols, relation symbols and constant symbols of the given type. Also, if it causes no confusion, we often denote the operation (relation, constant) $F_i^{n_i,D}$ by the same symbol $F_i^{n_i}$ as occurs in the type. Let us now have several examples.

Example 6.1.1 *Let the type be f, where f is the operation symbol of arity 1. This is called a* **unary operation symbol.** *Some structures of this type are the following:*

1. *(ω, S), where S is the successor function on ω.*
2. *$(\omega, x \to x^2)$, where the function $x \to x^2$ sends each number n to n^2.*

3. (Z, f), *where* $f(i) = 2i$ *for all* $i \in Z$.
4. (Q, f), *where* Q *is the set of all rational numbers and* $f(q) = 2 \times q - q^2$ *for all* $q \in Q$.
5. *Of course, the structure* $(\omega, +)$, *where* $+$ *is addition, is not a structure of the given type because* $+$ *is a binary (hence not unary) operation.*

Example 6.1.2 *Let the type be* R, *where* R *is a relation symbol of arity* 2. *Some structures of this type are the following:*

1. $(\omega, \leq)$, *where* $\leq$ *is the ordering relation on* ω.
2. $(\omega, mod(n))$, *where the relation* $mod(n)$ *is the equivalence relation on* ω *such that* $(x, y) \in mod(n)$ *if and only if* $x - y$ *is equal to* 0 *modulo* n.
3. (Z, P), *where* $(x, y) \in P$ *if and only if* $x = 2y$.
4. $(Q, \leq)$, *where* Q *is the set of all rational numbers, and* $\leq$ *is the usual ordering relation.*
5. *Of course, the structure* $(\omega, +)$, *where* $+$ *is addition, is not a structure of the given type because* $+$ *is a binary operation but not a binary relation.*

Example 6.1.3 *Recall the structure* $\mathcal{T}$ *from the previous chapter. The domain of the structure is* $\{0, 1\}^\star$. *On* $\mathcal{T}$, *two unary operations* L *and* R *are defined as follows. For all* $u \in \mathcal{T}$, $L(u) = u0$ *and* $R(u) = u1$. *The triple* $(\{0, 1\}^\star, L, R)$, *denoted by* $\mathcal{T}$, *is the* **binary tree**. *The type of this structure is*

$$f_1, \; f_2,$$

where f_1 *and* f_2 *are unary operation symbols.*

Example 6.1.4 *Consider the structure* $(\omega, S, +, \leq, 0, 10)$. *The type of this structure is*

$$f, f^2, R, c_0, c_1,$$

where f *is a unary operation symbol,* f^2 *is a binary operation symbol,* R *is a binary relation symbol, and* c_0 *and* c_1 *are constant symbols.*

Exercise 6.1.1

1. *Give examples of structures of the type* f^2, *where* f^2 *is a binary operation symbol.*
2. *Give examples of structures of the type* f^2, R^2, *where* f^2 *is a binary operation symbol and* R^2 *is a binary relation symbol.*
3. *Give examples of structures of the type* $U_0, U_1, U_2, \ldots$, *where each* U_i *is a unary predicate symbol.*
4. *Give examples of structures of the type* $c_0, c_1, \ldots$, *where each* c_i *is a constant symbol.*

6.2 The Monadic Second Order Language

We fix the type $F_0^{n_0}, F_1^{n_1}, \ldots, P_0^{m_0}, P_1^{m_1}, \ldots, c_0, c_1, \ldots$. Let us denote this type by τ. In this section our goal is to develop the **monadic second order language** of the structures of given type. Having the language, we will be able to formally express certain properties of structures of type τ and reason about the properties. At the end of this section we will explain the reasons for the terms *monadic* and *second order*.

In describing the language we will be quite formal since we have already used this type of language for other structures (e.g., (ω, S), finite linearly ordered sets). The symbols of the language of the monadic second order logic are the following.

1. We use the symbols
$$x, y, z, \ldots,$$
called **individual variables**, possibly with subscripts or superscripts. These run over domains of the structures of type τ.
2. We use the symbols
$$X, Y, Z, \ldots,$$
called **set variables**. These run over subsets of the domains of structures of type τ.
3. We use symbols $=$, $\in$, and of course the symbols from type τ:
$$F_0^{n_0}, F_1^{n_1}, \ldots, P_0^{m_0}, P_1^{m_1}, \ldots, c_0, c_1, \ldots.$$
4. We use logical connectives &, $\bigvee$, $\neg$, $\rightarrow$, and quantifiers $\exists$, $\forall$. The quantifiers $\exists$, $\forall$ can be applied to individual as well as to set variables.
5. We also use nonlogical symbols (and), left and right parentheses.

We now define the notion of a term of the monadic second order logic. Informally terms represent operations on the domains of structures obtained by compositions from the basic operations of the structures.

Basic Step. Each variable x is a term. Each constant symbol c is a term.

Inductive Step. If F is an operation symbol of arity m and $t_1, \ldots, t_m$ are terms, then $F(t_1, \ldots, t_m)$ is a term.

Thus, a string of symbols is a **term** if it can be shown to be a term by a finite number of applications of the procedure above. Each term may contain variables. If all the variables of the term t are among variables $\{x_0, x_1, \ldots, x_n\}$ we may denote this by $t(x_0, \ldots, x_n)$.

Each term defines an operation on a given structure $\mathcal{D}$ in a natural way. For example, the term

$$F^m(x_1, \ldots, x_m)$$

is the operation $F^{m,D}$ itself. The term

$$F^2(F^1(x), F^3(x, y, z))$$

defines the operation G of arity 3 as follows. For all $a, b, c \in D$, $G(a, b, c)$ is

$$F^{2,D}(F^{1,D}(a), F^{3,D}(a, b, c)).$$

We define all this more formally as follows.

Let $\mathcal{D}$ be a structure and $t(x_0, \ldots, x_n)$ be a term. The value of $t(x_0, \ldots, x_n)$ at $n+1$-tuple $(a_0, \ldots, a_n)$, denoted by $t(a_0, \ldots, a_n)$ is defined as follows:

Basic Step. If t is x_i, then $t(a_0, \ldots, a_n) = a_i$. If t is a constant c then $t(a_0, \ldots, a_n) = c^D$.

Inductive Step. If $t = F(t_1, \ldots, t_m)$, then

$$t(a_0, \ldots, a_n) = F^D(t_1(a_0, \ldots, a_n), \ldots, t_m(a_0, \ldots, a_n)).$$

Thus, every term t defines an operation $t^{\mathcal{D}}$ on the structure $\mathcal{D}$. Sometimes, if there is no confusion, we may write t instead of $t^{\mathcal{D}}$.

Exercise 6.2.1 *Consider the type that consists of two binary functional symbols f and g. Consider the structure $(Z, +, \times)$ of the type. Find the value of the following terms at specified n-tuples.*

1. $f(x, g(x, y))$ *at* $(-1, 2)$.
2. $g(x, f(x, g(x, x)))$ *at* 5.
3. $f(x, g(y, f(z, u)))$ *at* $(1, 2, 3, 4)$.
4. $g(x, g(x, g(x, x)))$ *at* 3.

Exercise 6.2.2 *Consider the structure (Z, S), where S is the successor function. Let t be a term of the type of this structure. Show that there exists a nonnegative integer n such that $t(x) = x + n$ for all $x \in Z$.*

We now define, by induction, formulas of the language of the monadic second order logic.

Basic Step. The expressions

$$t \in X,\ t_1 = t_2,\ X = Y,\ P(t_1, \ldots, t_n),$$

where $t_1, t_2, \ldots, t_n$ are terms, X and Y are set variables, and P is a predicate symbol of arity n, are all **atomic formulas**.

Inductive Step. Suppose that the formulas Φ_1 and Φ_2 have been defined. Then

1. $(\Phi_1 \& \Phi_2)$ is a formula,
2. $(\Phi_1 \bigvee \Phi_2)$ is a formula,
3. $(\Phi_1 \rightarrow \Phi_2)$ is a formula,
4. $(\neg\Phi_1)$ is a formula,
5. $(\exists x \Phi_1)$ and $(\exists X \Phi_1)$ are formulas,
6. $(\forall x \Phi_1)$ and $(\forall X \Phi_1)$ are formulas.

Now we define the notion of a free variable in a formula. We note that for a term t the set of **free variables** $FV(t)$ is simply the set of all variables that occur in t.

Basic Case. For atomic formulas $t \in X$, $x = y$, $X = Y$, $t_1 = t_2$, and $P(t_1, \ldots, t_n)$, the sets of free variables are $FV(t) \bigcup \{X\}$, $\{x, y\}$, $\{X, Y\}$, $FV(t_1) \bigcup FV(t_2)$, and $FV(t_1) \bigcup \cdots \bigcup FV(t_n)$, respectively.

Inductive Step. Suppose that the sets of free variables $FV(\Phi_1)$ and $FV(\Phi_2)$ for the formulas Φ_1 and Φ_2 have been defined. Then

$$FV(\Phi_1 \kappa \Phi_2) = FV(\Phi_1) \bigcup FV(\Phi_2), \qquad FV(\neg\Phi_1) = FV(\Phi_1),$$
$$FV(Qx\Phi_1) = FV(\Phi_1) \setminus \{x\}, \qquad FV(QX\Phi_1) = FV(\Phi_1) \setminus \{X\},$$

where $\kappa \in \{\&, \bigvee, \rightarrow\}$, $Q \in \{\forall, \exists\}$, x is an individual variable, and X is a set variable.

A formula is a **sentence** if it has no free variables. Thus, we have defined the language of the monadic second order logic. In summary, one can quite informally say that the language we have defined consists of the type, variables, logical connectives, terms, formulas, and sentences.

We also need a language weaker than the language of the monadic second order logic. This weaker language is defined exactly as the language of the monadic second order logic but does not contain set variables, and the membership symbol $\in$. Thus, the formulas of this language are defined as follows. The expressions $t_1 = t_2$ and $P(t_1, \ldots, t_n)$, where t_1 and t_2 are terms, and P is a predicate symbol of arity n, are all **atomic formulas**. Suppose, by induction, that the formulas Φ_1 and Φ_2 have been defined. Then $(\Phi_1 \& \Phi_2)$, $(\Phi_1 \bigvee \Phi_2)$, $(\Phi_1 \rightarrow \Phi_2)$, $(\neg\Phi_1)$, $(\exists x \Phi_1)$ and $(\forall x \Phi_1)$ are all formulas. We call this language the language of the **first order logic**. Clearly, the language of the first order logic is contained in the language of the monadic second order logic.

Quite informally, the first order logic is a set of statements about properties of the elements of structures, while the second order monadic logic is a set of statements about properties of the elements and subsets of structures. The word *order* can thus be understood as follows. Elements of structures are first order objects. Subsets and relations of structures are the second order objects. The third order objects are sets of relations. In general, objects of order n are sets that contain objects of order $n-1$. The word *monadic* is used because in the monadic second order language the second order variables are set variables only.

6.3 Satisfiability and Theories

In this section we discuss the relationship between languages and structures. The relationship is based on the notion of satisfiability, or equivalently truth, of the formulas under a given interpretation of variables. We assume that we have fixed the type τ. We also fix a structure $\mathcal{D}$ whose type is τ. Suppose that to each individual variable x_i and a set variable X_j an element b_i and a set B_j of the domain D has been assigned, respectively. In other words, we have a fixed **interpretation**

$$intr : x_i \to b_i \quad intr : X_j \to B_j$$

of the variables. By induction on the complexity of the formula Φ, we define **satisfaction** of Φ on the structure $\mathcal{D}$ under the interpretation. We recall that any term t can be thought as an operation $t^{\mathcal{D}}$ on the domain $\mathcal{D}$. Now we provide the definition. Note that the definition assumes that the interpretation *intr* is given.

Definition 6.3.1
Basic Step.

- $\mathcal{D}$ **satisfies** *the atomic formula* $(t(x_1, \ldots, x_n) \in X_j)$ *if in* $\mathcal{D}$ *we indeed have* $t^{\mathcal{D}}(b_1, \ldots, b_n) \in B_j$.
- $\mathcal{D}$ **satisfies** *the atomic formula* $t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_m)$ *if* $t_1^{\mathcal{D}}(b_1, \ldots, b_n) = t_2^{\mathcal{D}}(b_1, \ldots, b_m)$.
- $\mathcal{D}$ **satisfies** *the atomic formula* $(X_i = X_j)$ *if* $B_i = B_j$.
- $\mathcal{D}$ **satisfies** *the atomic formula* $P(t_1(x_1, \ldots, x_{m_1}), \ldots, t_n(x_1, \ldots, x_{m_n}))$ *if it is indeed the case that the n-tuple*

$$(t_1^{\mathcal{D}}(b_1, \ldots, b_{m_1}), \ldots, t_n^{\mathcal{D}}(b_1, \ldots, b_{m_n}))$$

belongs to the relation $P^{\mathcal{D}}$.

Inductive Step. *We consider separately each case corresponding to the inductive step in the definition of a formula.*

- $\mathcal{D}$ **satisfies** $(\Phi_1 \bigvee \Phi_2)$ *if* $\mathcal{D}$ *satisfies either* Φ_1 *or* Φ_2.
- $\mathcal{D}$ **satisfies** $(\Phi_1 \& \Phi_2)$ *if* $\mathcal{D}$ *satisfies both* Φ_1 *and* Φ_2.

- $\mathcal{D}$ **satisfies** $(\Phi_1 \to \Phi_2)$ *if* $\mathcal{D}$ *does not satisfy* Φ_1 *or the condition that* $\mathcal{D}$ *satisfies* Φ_1 *implies that* $\mathcal{D}$ *satisfies* Φ_2.
- $\mathcal{D}$ **satisfies** $\neg(\Phi_1)$ *if* $\mathcal{D}$ *does not satisfy* Φ_1.
- $\mathcal{D}$ **satisfies** $(\exists x_i \Phi_1)$ *if there exists* $b \in D$ *such that* $\mathcal{D}$ *satisfies the formula* Φ_1 *under the new interpretation intr′ which is the same as intr except its value on* x_i *is* b.
- $\mathcal{D}$ **satisfies** $(\exists X_i \Phi_1)$ *if there exists* $B \subseteq D$ *such that* $\mathcal{D}$ *satisfies the formula* Φ_1 *under the new interpretation intr′ which is the same as intr except its value on* X_i *is* B.
- $\mathcal{D}$ **satisfies** $(\forall x_i \Phi_1)$ *if* $\mathcal{D}$ *satisfies* $\neg(\exists x_i(\neg\Phi_1))$.
- $\mathcal{D}$ **satisfies** $\forall X_i \Phi_1)$ *if* $\mathcal{D}$ *satisfies* $\neg(\exists X_i(\neg\Phi_1))$.

From the definition we see that the satisfaction of sentences does not depend on interpretations. Every sentence is either satisfied or is not satisfied in the structure, and does not depend on *intr*. For a formula Φ whose variables are among $x_1, \ldots, x_t$ and $X_1, \ldots, X_p$, we usually write $\Phi(X_1, \ldots, X_p, x_1, \ldots, x_t)$. We write

$$\mathcal{D} \models \Phi(B_1, \ldots, B_p, b_1, \ldots, b_t)$$

if the structure $\mathcal{D}$ satisfies this formula under the interpretation *intr* such that $intr(X_j) = B_j$, $intr(x_i) = b_i$, where $j = 1, \ldots, p$ and $i = 1, \ldots, t$.

We need a definition.

Definition 6.3.2 *We say that the formulas* $\Phi(X_1, \ldots, X_m, y_1, \ldots, y_k)$ *and* $\Psi(X_1, \ldots, X_m, y_1, \ldots, y_k)$ *are* **equivalent** *in a given structure* $\mathcal{D}$ *if for all subsets* $B_1, \ldots, B_m \subset D$ *and all elements* $b_1, \ldots, b_k \in D$ *the structure* $\mathcal{D}$ *satisfies* $\Phi(B_1, \ldots, B_m, b_1, \ldots, b_k)$ *if and only if* $\mathcal{D}$ *satisfies* $\Psi(B_1, \ldots, B_m, b_1, \ldots, b_k)$.

Exercise 6.3.1 *Consider the structure* $\mathcal{T} = (T, L, R)$. *Let the term* $t_1(x)$ *be* $r(t_1'(x))$ *and the term* $t_2(y)$ *be* $r'(t_2'(y))$, *where* $r, r' \in \{L, R\}$. *Show that* $t_1(x) = t_2(y)$ *is equivalent to the formula* $\exists x_1 \exists y_1 (t_1'(x) = x_1 \ \& \ t_2'(y) = y_1 \ \& \ r(x_1) = r'(y_1))$ *in structure* $\mathcal{T}$.

Definition 6.3.3 *Let* $\mathcal{K}$ *be a class of structures.* **The monadic second order theory of** $\mathcal{K}$ *is the set of all sentences in the monadic second order logic satisfiable (true) in all the structures from* $\mathcal{K}$. *We denote it by* $Th(\mathcal{K})$. *Similarly,* **the first order theory of** $\mathcal{K}$ *is the set of all sentences in the first order logic satisfiable (true) in all the structures from* $\mathcal{K}$. *We denote this theory by* $Th_1(\mathcal{K})$.

Thus, using the definition one can talk about the monadic second order theory of all linearly ordered sets, partially ordered sets or different types of mathematical structures such as groups, rings, boolean algebras, etc. When the class $\mathcal{K}$ contains only one structure, say $\mathcal{D}$, then usually the theory of the class $\mathcal{K}$, that is, $Th(\mathcal{K})$ is denoted by $Th(\mathcal{D})$. So, one can talk about theories of the structures $(Q, \leq)$, $(Z, +)$, $(\omega, S, +, \times)$, etc.

Definition 6.3.4 *The monadic second order theory of the structure $\mathcal{T} = (\{0, 1\}^\star, L, R)$ of two successor functions is denoted by S2S.*

Our purpose is to show that the monadic second order theory of $\mathcal{T}$ is decidable. In other words, we will show that there exists an effective procedure which, for any given monadic second order sentence Φ, decides if this sentence is true in $\mathcal{T}$ or not. Before we proceed to this task we will need one additional definition and proposition (discussed in the next section) that will be used later.

6.4 Isomorphisms

A concept that is very often used in mathematics is the concept of *identification* of structures. Informally, two structures can be *identified* if one is a "copy" of the other. Thus, two structures that are identified should have the same algebraic properties. For example, two finite linearly ordered sets that have the same number of elements can be identified (see the section on the monadic second order theory of strings in the finite automata chapter). We formalize the concept of *identifying* structures in the following definition.

Definition 6.4.1 *Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be structures of type τ. A one-to-one mapping f from the domain D_1 onto the domain D_2 is called an* **isomorphism** *if the map f preserves the basic operations and relations as follows:*

1. *For all constants $c \in \tau$, $f(c^{\mathcal{D}_1}) = c^{\mathcal{D}_2}$. In other words, f "preserves" the constants in $\mathcal{D}_1$ and $\mathcal{D}_2$.*
2. *For any n-ary operation symbol $F \in \tau$, and all $a_1, \ldots, a_n \in D_1$, we have*
$$f(F^{\mathcal{D}_1}(a_1, \ldots, a_n)) = F^{\mathcal{D}_2}(f(a_1), \ldots, f(a_n)).$$
In other words, the mapping f "preserves" the operations.
3. *For any n-ary relation symbol $P \in \tau$, and all $a_1, \ldots, a_n \in D_1$, $P^{\mathcal{D}_1}(a_1, \ldots, a_n)$ is true in $\mathcal{D}_1$ if and only if $P^{\mathcal{D}_2}(f(a_1), \ldots, f(a_n))$ is true in $\mathcal{D}_2$. In other words, the mapping f "preserves" the relations.*

If f is an isomorphism between $\mathcal{D}_1$ and $\mathcal{D}_2$, then the structure $\mathcal{D}_1$ is called **isomorphic to** *the structure $\mathcal{D}_2$.*

It is not hard to see that isomorphic structures have the same theories. We prove a slightly more general fact in the following proposition.

Proposition 6.4.1 *Let f be an isomorphism from the structure $\mathcal{D}_1$ onto $\mathcal{D}_2$. Then for all formulas $\Phi(X_1, \ldots, X_m, y_1, \ldots, y_k)$, subsets $B_1, \ldots, B_m \subseteq D_1$ and elements $b_1, \ldots, b_k \in D_1$, the structure $\mathcal{D}_1$ satisfies $\Phi(B_1, \ldots, B_m, b_1, \ldots, b_k)$ if and only $\mathcal{D}_2$ satisfies $\Phi(f(B_1), \ldots, f(B_m), f(b_1), \ldots, f(b_k))$, where $f(B)$ is the image of the set B in D_2 under f.*

Proof. The proof can be presented by induction on the complexity of the formula $\Phi(X_1, \ldots, X_m, b_1, \ldots, b_k)$. The base case when the formula is atomic follows directly from the definition of isomorphism. The cases when Φ is obtained from less complex formulas Φ_1 and Φ_2 using logical connectives are proved easily from the definition of satisfiability. Now assume that Φ is of the form $\exists X_1 \Psi(X_1, \ldots, X_m, y_1, \ldots, y_k)$. Suppose that $\mathcal{D}_1$ satisfies the formula $\exists X_1 \Psi(X_1, B_2, \ldots, B_m, b_1, \ldots, b_k)$. Then for some $B_1 \subset \mathcal{D}_1$, the structure $\mathcal{D}_1$ satisfies the formula $\Psi(B_1, B_2 \ldots, B_m, b_1, \ldots, b_k)$. Now applying the induction hypothesis to $\Psi(B_1, B_2, \ldots, B_m, b_1, \ldots, b_k)$, we see that $\mathcal{D}_2$ satisfies $\Psi(f(B_1), f(B_2), \ldots, f(B_m), f(b_1), \ldots, f(b_k))$. Hence $\mathcal{D}_2$ satisfies $\exists X_1 \Psi(X_1, f(B_2), \ldots, f(B_m), f(b_1), \ldots, f(b_k))$. The other cases are proved similarly. □

Exercise 6.4.1 *Finish the proof of the proposition.*

Exercise 6.4.2 *Show that the following facts are true:*

1. *Every structure is isomorphic to itself.*
2. *If $\mathcal{D}_1$ is isomorphic to $\mathcal{D}_2$, then $\mathcal{D}_2$ is isomorphic to $\mathcal{D}_1$.*
3. *If $\mathcal{D}_1$ is isomorphic to $\mathcal{D}_2$ and $\mathcal{D}_2$ is isomorphic to $\mathcal{D}_3$, then $\mathcal{D}_1$ is isomorphic to $\mathcal{D}_3$.*

Exercise 6.4.3 *Show that the following structures are isomorphic:*

1. *$(\omega, +)$ and $(2\omega, +)$, where $+$ is the addition operation, and 2ω is the set of all even natural numbers.*
2. *$(Q, \leq)$ and $((0, 1)_r, \leq)$, where $(0, 1)_r$ is the set of all rational numbers between 0 and 1 not including either 0 or 1.*

Exercise 6.4.4 *Show that if two structures with finite domains satisfy the same first order sentences, then the structures are isomorphic.*

6.5 Definability in $\mathcal{T}$ and Decidability of S2S

In this section we will concentrate on the monadic second order theory of the structure of two successors $\mathcal{T} = (T, L, R)$. In particular, we will be interested in the issue about the relationship between the monadic second order language of $\mathcal{T}$ and Rabin automata. We show that the relations in $\mathcal{T}$ definable in the monadic second order logic can be identified in a certain natural way with languages of Σ-valued trees accepted by Rabin automata.

6.5.1 Σ-Valued Trees as Structures. Let Σ be an alphabet. We will show how Σ-valued trees can be viewed as mathematical structures which are, in some sense, richer than the structure $\mathcal{T}$. Suppose that $(v, \mathcal{T})$ is a Σ-valued tree. Take a symbol σ from Σ. Now the symbol σ defines a subset Q_σ on the tree $\mathcal{T}$ in the following way. A node $u \in \mathcal{T}$ belongs to the subset Q_σ if and only if $v(u) = \sigma$. Let us consider an example.

Example 6.5.1 *Suppose that $\Sigma = \{a, b, c\}$. Consider a Σ-valued tree $(v, \mathcal{T})$ defined as follows:*

$$v(u) = \begin{cases} a & \text{if } \exists n(|u| = 3n), \\ b & \text{if } \exists n(|u| = 3n+1), \\ c & \text{if } \exists n(|u| = 3n+2). \end{cases}$$

This valuation defines the following subsets:

$$Q_a = \{u \mid |u| = 3n, n \in \omega\},$$
$$Q_b = \{u \mid |u| = 3n+1, n \in \omega\},$$
$$Q_c = \{u \mid |u| = 3n+2, n \in \omega\}.$$

In this example, the Σ-valued tree $(v, \mathcal{T})$ defines the structure whose domain consists of all binary strings, and whose type is determined by the successor functions L and R, the unary relations Q_a, Q_b, and Q_c. In other words, we have the structure

$$(\{0,1\}^\star, L, R, Q_a, Q_b, Q_c).$$

This structure is indeed richer than $\mathcal{T}$ just because it contains more information about the tree than the original structure $\mathcal{T}$ itself.

We explain this in a general setting. Given a Σ-valued tree $(v, \mathcal{T})$, with $\Sigma = \{a_1, \ldots, a_n\}$, we *expand* $\mathcal{T}$ by considering the structure

$$(\mathcal{T}_2, L, R, Q_{a_1}, \ldots, Q_{a_n}),$$

where $\Sigma = \{a_1, \ldots, a_n\}$. We denote this structure by $\mathcal{T}_v$. The type of $\mathcal{T}_v$ thus consists of two unary operation symbols and n unary relation symbols.

There is another way to look at the structures of type $\mathcal{T}_v$. We explain this using the next example.

Example 6.5.2 *The alphabet is $\{a, b, c\}$. We identify the alphabet with the subset of the alphabet $\{0,1\}^2$ in such a way that*

$$a = \begin{pmatrix}1\\0\end{pmatrix}, \quad b = \begin{pmatrix}0\\1\end{pmatrix}, \quad c = \begin{pmatrix}1\\1\end{pmatrix}.$$

Now the valuation v considered in Example 6.5.1 can be expressed as

$$v(u) = \begin{cases} \begin{pmatrix}1\\0\end{pmatrix} & \text{if } \exists n(|u| = 3n), \\ \begin{pmatrix}0\\1\end{pmatrix} & \text{if } \exists n(|u| = 3n+1), \\ \begin{pmatrix}1\\1\end{pmatrix} & \text{if } \exists n(|u| = 3n+2). \end{cases}$$

Let us analyze this example in detail. The valuation v defines the pair (X_1, X_2) of subsets of $\mathcal{T}$ as follows. A node u belongs (does not belong) to X_1 if and only if the first coordinate of the letter $v(u)$ is 1 (0). Similarly, $u \in \mathcal{T}$ belongs (does not belong) to X_2 if and only if the second coordinate of $v(u)$ is 1 (0). Hence we see that

$$X_1 = \{u \mid |u| = 3n, n \in \omega\} \bigcup \{u \mid |u| = 3n+2, n \in \omega\},$$
$$X_2 = \{u \mid |u| = 3n+1, n \in \omega\} \bigcup \{u \mid |u| = 3n+2, n \in \omega\}.$$

Consider the sets X_1 and X_2 just above defined. The pair $\bar{X} = (X_1, X_2)$ determines a valuation $v_{\bar{X}}$ as follows. For all $u \in \mathcal{T}$,

$$v_{\bar{X}}(u) = \begin{pmatrix}\epsilon_1\\ \epsilon_2\end{pmatrix},$$

where $\epsilon_i = 1$ if and only if $u \in X_i$. Then for every $u \in \mathcal{T}$, $v_{\bar{X}}(u)$ belongs to $\{0,1\}^2$ and equals $v(u)$. Note that since

$$a = \begin{pmatrix}1\\0\end{pmatrix}, \quad b = \begin{pmatrix}0\\1\end{pmatrix}, \quad c = \begin{pmatrix}1\\1\end{pmatrix},$$

we also have $v_{\bar{X}} = v_1$.

Thus, informally we can conclude with the following comments about the above example. If we know v, then we know the structure $\mathcal{T}_v$. If we know $\mathcal{T}_v$, we know v. If we know v, we know the pair (X_1, X_2). If we know the pair (X_1, X_2), then we know v. Roughly speaking, the three objects, v, $\mathcal{T}_v$, and (X_1, X_2) are essentially the same and possess, in some respect, the same information.

6.5.2 Definable Relations. Consider the tree structure $\mathcal{T}$. Let $P(\mathcal{T})$ be the set of all subsets of $\mathcal{T}$. In this subsection we are interested in relations in $\mathcal{T}$ that can be expressed in the monadic second order language of the structure $\mathcal{T}$. We formally define this concept in the next definition.

Definition 6.5.1 *Let R be a subset of $P(\mathcal{T})^{m-k} \times \mathcal{T}^k$. We say that R is* **definable** *if there exists a formula $\Phi(B_1, \ldots, B_{m-k}, x_{m-k+1}, \ldots, x_m)$ such that the relation R coincides with*

$$\{(B_1, \ldots, B_{m-k}, b_{m-k+1}, \ldots, b_m) \mid \mathcal{T} \models \Phi(B_1, \ldots, B_{m-k}, b_{m-k+1}, \ldots, b_m)\}.$$

Thus, R is definable if there exists a formula such that R consists of all the tuples that make the formula true in the tree $\mathcal{T}$. We consider several examples of definable relations on $\mathcal{T}$.

Our first example shows that the usual subset relation among subsets of $\mathcal{T}$ is a definable relation.

Example 6.5.3 *The formula $X \subseteq Y$ is defined as*

$$\forall z(z \in X \rightarrow z \in Y).$$

Thus, when X and Y are thought to be A and B respectively, where A and B are subsets of $\mathcal{T}$, the formula $X \subseteq Y$ is satisfied under this interpretation of X and Y if and only if A is indeed a subset of B.

The next example shows that all the subsets that are closed with respect to the unary operations L and R are definable. We say that $A \subset \mathcal{T}$ is **algebraically closed** if $L(a), R(a) \in A$ for all $a \in A$.

Example 6.5.4 *Consider the formula $Sub(X)$:*

$$\forall x(x \in X \rightarrow L(x) \in X \;\&\; R(x) \in X).$$

Thus, assume that we interpret X as a subset A of the tree $\mathcal{T}$. Then $Sub(A)$ is satisfied if and only if for all elements $a \in A$ we have $L(a), R(a) \in A$. Thus, $Sub(A)$ is satisfied if and only if A is algebraically closed.

We give an example of a closed set in $\mathcal{T}$. Suppose A is the set of all nodes that occur after a given node u, that is $A = \{a \mid u \leq a\}$. Then certainly for all a, if $a \in A$, then $a0, a1 \in A$. Hence $\mathcal{T} \models Sub(A)$, and A is algebraically closed.

We recall that we have the naturally defined prefix relation on $\mathcal{T}$. We denoted this relation by $\leq$. It turns out, as the next example shows, that the prefix relation on the nodes of the tree is also definable.

Example 6.5.5 *We define the following formula denoted by $x \leq y$:*

$$\forall X(Sub(X) \;\&\; x \in X \rightarrow y \in X).$$

Then for any two nodes x, y of $\mathcal{T}$, $x \leq y$ if and only if x is a prefix of y.

Thus, we see that the partial order $\leq$ is a definable relation on $\mathcal{T}$.

In the next example, we show that the lexicographic ordering on the tree $\mathcal{T}$ is definable. The lexicographic ordering $\preceq$ is defined as follows. For all $u, v \in \mathcal{T}$, u is lexicographically less that or equal to v if $u = v$ or u is a prefix of v or the first symbol of v that is not equal to u is 1. Thus, if the first (from left to right) symbol where v differs from u is 1, then $u \preceq v$.

Example 6.5.6 *We define the following formula $x \preceq y$:*

$$x \leq y \bigvee \exists z(L(z) \leq x \;\&\; R(z) \leq y).$$

It is not hard to see $a \preceq b$ is true in $\mathcal{T}$ if and only if a is lexicographically equal to or less than b.

We leave the reader to prove the following exercise.

Exercise 6.5.1 *Show that $\preceq$ is a linear ordering on the set $\mathcal{T}$.*

Definability of the lexicographic ordering allows us to define finite subsets of the binary tree $\mathcal{T}$.

Example 6.5.7 *Consider the following formula $Finite(X)$:*

$$\forall Y(Y \subset X \& \exists x(x \in Y) \rightarrow \exists x_1 \exists x_2 \forall y(y \in Y \rightarrow x_1 \preceq y \;\&\; y \preceq x_2)).$$

This formula states that $Finite(X)$ is satisfied if and only if every nonempty subset Y of X has minimal and maximal elements with respect to the lexicographic ordering.

Exercise 6.5.2 *Show that the set of all paths through the tree $\mathcal{T}$ is definable.*

Exercise 6.5.3 *Let n be a fixed positive number. Show that the set of all finite $X \subset \mathcal{T}$ such that X has nk elements for some k and X is a subset of a path is definable.*

6.5.3 From Rabin Automata to Formulas. Let $\mathcal{A} = (S, \{s_0\}, M, \mathcal{F})$ be a Rabin automaton over the alphabet Σ. We can suppose that $\Sigma = \{0, 1\}^m$ for some $m \in \omega$. Let $B_1, \ldots, B_{m-k}$ be subsets of $\mathcal{T}$, and $b_{m-k+1}, \ldots, b_m$ be some elements of $\mathcal{T}$. We sometimes denote the sequence

$$B_1, \ldots, B_{m-k}, b_{m-k+1}, \ldots, b_m$$

by $\bar{B}\bar{b}$. Each such sequence and a node $u \in \mathcal{T}$ define a symbol $v(u)$ of the alphabet Σ:

$$v(u) = (\epsilon_1, \ldots, \epsilon_m),$$

where for each j, $\epsilon_j = 1$ if and only if $u \in B_j$ or $u = b_j$. Thus, we have a valuation v of the tree $\mathcal{T}$. We denote this Σ-valued tree by

$$\mathbf{tree}(\bar{B}, \bar{b}).$$

The opposite is also true: any Σ-valued tree $(v, \mathcal{T})$ defines an m-tuple of sets $(X_1, \ldots, X_m)$, where for each i, $1 \leq i \leq m$, and each $u \in \mathcal{T}$, u is in X_i (not in X_i) if and only if the ith component of $v(u)$ is 1 (0). So, we see that there is a natural one-to-one correspondence between all Σ-valued trees and m-tuples of subsets of $\mathcal{T}$. We note how we used the fact that m is fixed and is such that $\Sigma = \{0, 1\}^m$.

The following theorem shows that the notion of acceptance for Rabin automata is expressible in the monadic second order formalism.

Theorem 6.5.1 *There exists a procedure which, given a Rabin automaton $\mathcal{A} = (S, M, T, \mathcal{F})$ over $\Sigma = \{0,1\}^m$, constructs a formula $\Phi(X_1, \ldots, X_m)$, where $X_1, \ldots, X_m$ are set variables, such that for all subsets $\bar{B} = B_1, \ldots, B_m \subset \mathcal{T}$ the following property holds:*

$$\mathcal{A} \text{ accepts } \mathbf{tree}(\bar{B}) \text{ if and only if } (\mathcal{T}, L, R) \text{ satisfies } \Phi(\bar{B}).$$

Proof. The proof follows the ideas of the proof of the similar theorem for Büchi automata. We can assume that the initial state I contains one state only. Since S is a finite set we can also suppose that

$$S = \{0, 1, \ldots, p\}$$

with 0 being the initial state. Let $\sigma \in \Sigma$ be of the form

$$\begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \vdots \\ \epsilon_m \end{pmatrix},$$

where each $\epsilon_i \in \{0, 1\}$. We define the formula $\Phi_\sigma(x, \bar{X})$, where $\bar{X}$ is $X_1, \ldots, X_m$, as follows:

$$\Phi_\sigma(x, X_1, \ldots, X_m) = x \in^{\epsilon_1} X_1 \& \ldots x \in^{\epsilon_m} X_m,$$

where $\in^\epsilon$ is $\in$ if $\epsilon = 1$, and $\notin$ otherwise.

Informally, this formula codes the letter $\sigma \in \Sigma$ by saying that the value of $tree(X)$ at node x is σ. We note the following fact. Let $B_1, \ldots, B_m$ be subsets of $\mathcal{T}$. Then for every $u \in \mathcal{T}$ there must exist some $\sigma \in \Sigma$ such that $\Phi_\sigma(u, \bar{B})$ holds. We conclude that the formula

$$\forall x \left(\bigvee_{\sigma \in \Sigma} \Phi_\sigma(x, \bar{B}) \right)$$

is satisfied in $(\mathcal{T}, r_0, r_1)$. We also recall that for each Σ-valued tree $(v, \mathcal{T})$ there exists a sequence $\bar{B} = B_1, \ldots, B_m$ of subsets of $\mathcal{T}$ such that $\mathbf{tree}(B_1, \ldots, B_m)$ is exactly $(v, \mathcal{T})$.

Let $Y_0, Y_1, \ldots, Y_p$ be set variables. The desired formula involves these set variables. The intention is that each Y_i represents the state i of the automaton $\mathcal{A}$. In the desired formula these set variables will be existentially quantified. We write down the following formula and denote it by $D(\bar{Y})$, where $\bar{Y}$ is $Y_0, \ldots, Y_p$:

$$\&_{i \neq j}^{p} \neg \exists z (z \in Y_i \& z \in Y_j)) \;\&\; \forall x \left(\bigvee_{j \leq p} x \in Y_j \right).$$

The intention is that we want to express the fact that the automaton $\mathcal{A}$ cannot be in two distinct states simultaneously.

We define another formula $\Phi_{\sigma,i}(x, \bar{X}, \bar{Y})$ and explain its meaning. The formula is

$$x \in Y_i \;\&\; \Phi_\sigma(x, \bar{X}) \rightarrow \bigvee_{(j,k) \in M(i,\sigma)} (L(x) \in Y_j \;\&\; R(x) \in Y_k).$$

Informally, the formula corresponds to the fact that if $\mathcal{A}$ is in state i and the next input signal is σ, then the automaton splits itself into two (left and right) copies such that the left copy is in state j and the right copy is in state k so that $(j, k) \in M(i, \sigma)$. The following note concerns this formula. Suppose that $u \in \mathcal{T}$ and $B_1, \ldots, B_m \subset \mathcal{T}$. Let $\sigma \in \Sigma$ be such that $(\mathcal{T}, L, R)$ satisfies $\Phi_\sigma(u, \bar{B}, \bar{Y})$. Then if the formula

$$\exists Y_0 \ldots \exists Y_p (\Phi_{\sigma,i}(u, \bar{B}, \bar{Y}))$$

is true, there exists a (j, k) such that $L(u) \in Y_j$, $R(u) \in Y_k$ and $(j, k) \in M(i, \sigma)$.

Finally, the last formula we need is the formula $F(\bar{Y})$, which states that for any path π, there exists a $Q \in \mathcal{F}$ and an $x \in \pi$ such that the following properties hold:

1. $\forall y (y \geq x \rightarrow \bigvee_{j \in Q} y \in Y_j)$.
2. For any $j \in Q$ and for any $z \geq x$ if $z \in \pi$, there exists a $y \geq z$ for which $y \in Y_j$ and $y \in \pi$.

It is not hard to see that the formula F is expressible in the monadic second order logic. This formula is intended to code the notion of successful computation.

Now we write down the desired formula $\Phi(X_1, \ldots, X_m)$:

$$\exists Y_0 \ldots Y_p (D(\bar{Y}) \;\&\; 0 \in Y_0 \;\&\; \forall x (\&_{i \in S, \sigma \in \Sigma} \Phi_{\sigma,i}(x, \bar{X}, \bar{Y}) \;\&\; F(\bar{Y}))).$$

Our goal is to show that this formula satisfies the theorem. We need to prove that for all subsets $B_1, \ldots, B_m \subseteq \mathcal{T}$ the automaton $\mathcal{A}$ accepts $\mathbf{tree}(B_1, \ldots, B_m)$ if and only if $\mathcal{T} \models \Phi(B_1, \ldots, B_m)$.

Take subsets $B_1, \ldots, B_m$. Consider the Σ-tree

$$\mathbf{tree}(B_1, \ldots, B_m).$$

Now let us assume that the Σ-valued tree $\mathbf{tree}(B_1, \ldots, B_m)$ is an input of the Rabin automaton $\mathcal{A}$.

Suppose that $\mathcal{A}$ accepts $\mathbf{tree}(B_1, \ldots, B_m)$. Therefore, there exists a run

$$\mathbf{r} : \mathcal{T} \rightarrow S$$

such that for any path π the set $\{s \mid \mathbf{r}(x) = s \text{ for infinitely many } x \in \pi\}$ belongs to $\mathcal{F}$.

We need to prove that

$$\mathcal{T} \models \Phi(B_1, \ldots, B_m),$$

that is, we need to show that there are subsets $D_0, \ldots, D_p$ on the tree $\mathcal{T}$ such that the interpretation $Y_i \to D_i, i = 0, \ldots, p$, makes the formula $\Phi(B_1, \ldots, B_m)$ true in $\mathcal{T}$.

Here is how we define each $D_i, i = 0, \ldots, p$:

$$D_i = \{x \in T \mid \mathbf{r}(x) = i\}.$$

The formula $\Phi(B_1, \ldots, B_m)$ under this interpretation of $Y_i \to D_i, i = 0, \ldots, p$, is satisfied in $\mathcal{T}$.

Now suppose that $\Phi(B_1, \ldots, B_m)$ is satisfied in $\mathcal{T}$. We want to show that $\mathcal{A}$ accepts the string $\mathbf{tree}(B_1, \ldots, B_m)$. There are subsets $D_0, \ldots, D_p$ of $\mathcal{T}$ such that the formula $\Phi(B_1, \ldots, B_m)$ becomes satisfied in $\mathcal{T}$ when we interpret the variables $Y_0, \ldots, Y_p$ as $D_0, \ldots, D_p$, respectively.

For every $x \in T$, we consider the set $D_{\mathbf{r}(x)}$ such that $u \in D_{\mathbf{r}(x)}$, where $1 \leq \mathbf{r}(x) \leq p$. Hence we have a mapping $\mathbf{r}$ from T into S. Now using the definition of $\Phi(\bar{X})$, one can check that the function $\mathbf{r}(x)$, $x \in T$, is a run of the automaton $\mathcal{A}$ on the tree $\mathbf{tree}(\mathcal{T}, B_1, \ldots, B_m)$. Moreover, the run $\mathbf{r}$ is a successful run. □

Exercise 6.5.4 *Prove the theorem above in greater detail.*

6.5.4 From Formulas to Rabin Automata. Our goal is to show the converse of the theorem proved in the previous subsection. In other words, given a formula of the second order monadic logic of the structure $\mathcal{T}$, we want to construct a Rabin automaton whose successful runs correspond to interpretations of the variables that make the formula satisfied. We consider several examples to explain the idea.

Example 6.5.8 *Consider the formula $x_2 \in X_1$. We define a Rabin automaton $\mathcal{A}$ over the alphabet $\{0, 1\}^2$ as follows:*

1. *The set of states is $S = \{s_g, f\}$.*
2. *s_g is the "guessing" state and is the initial state.*
3. *The transition diagram M is defined as:*
   (a) $M(f, \binom{0}{0}) = M(f, \binom{1}{0}) = \{(f, f)\}$.
   (b) $M(s_g, \binom{0}{0}) = M(s_g, \binom{1}{0}) = \{(s_g, f), (f, s_g)\}$.
   (c) $M(s_g, \binom{1}{1}) = \{(f, f)\}$.
4. $\mathcal{F} = \{\{f\}\}$.

The connection between the automaton and the formula $x_2 \in X_1$ is the following. For all $B_1 \subset T$ and $b_2 \in T$, the automaton $\mathcal{A}$ accepts the tree $\mathbf{tree}(B_1, b_2)$ if and only if $b_2 \in B_1$. In other words, $\mathbf{tree}(B_1, b_2) \in L(\mathcal{A})$ if and only if $\mathcal{T} \models (b_2 \in B_1)$.

Example 6.5.9 *Consider the atomic formula $r_0(x_1) = x_2$. We define an automaton $\mathcal{A}$ over the alphabet $\{0, 1\}^2$ as follows.*

1. *The set of states is $S = \{s_g, s_1, f\}$.*
2. *s_g is the "guessing" state and is the initial state.*
3. *The transition digram M is defined as:*
   (a) $M(f, \binom{0}{0}) = \{(f, f)\}$.
   (b) $M(s_g, \binom{0}{0}) = \{(s_g, f), (f, s_g)\}$.
   (c) $M(s_g, \binom{1}{0}) = \{(s_1, f)\}$.
   (d) $M(s_1, \binom{0}{1}) = \{(f, f)\}$.
4. $\mathcal{F} = \{\{f\}\}$.

The connection between the automaton and the formula $r_0(x_1) = x_2$ is the following. For all $b_1 \subset T$ and $b_2 \in T$, the automaton $\mathcal{A}$ accepts the tree $\mathbf{tree}(b_1, b_2)$ if and only if $L(b_1) = b_2$. In other words, $\mathbf{tree}(b_1, b_2) \in L(\mathcal{A})$ if and only if $\mathcal{T} \models L(b_1) = b_2$.

Now we give a definition. The definition requires some notation. From now on, $\bar{X}$ and $\bar{x}$ denote the sequence $X_1, \ldots, X_{m-k}$ of set variables and the sequence $x_{m-k+1}, \ldots, x_m$ of individual variables, respectively. We use similar notations for sequences of sets and elements in $\mathcal{T}$. For example $\bar{B} \subset A$ simply means that $B_1, \ldots, B_{m-k}$ is a sequence of subsets of A.

Definition 6.5.2 *Let $\Phi(\bar{X}, \bar{x})$ be a formula and let $\mathcal{A}$ be a Rabin automaton over $\{0, 1\}^m$. The automaton $\mathcal{A}$* **represents** *$\Phi(\bar{X}, \bar{x})$ if for all subsets $\bar{B} \subset T$ and elements $\bar{b} \in T$, the automaton $\mathcal{A}$ accepts $\mathbf{tree}(\bar{B}, \bar{b})$ if and only if $\mathcal{T}$ satisfies $\Phi(\bar{B}, \bar{b})$.*

The two examples above show that the formulas $x_2 \in X_1$ and $L(x_1) = x_2$ are represented by automata.

Exercise 6.5.5 *Show that the following formulas are represented by Rabin automata.*

1. *$Sub(X)$:*

$$Sub(X) = \forall x(x \in X \to L(x) \in X \;\&\; R(x) \in X),$$

2. $x \le y$:
$$\forall X(Sub(X) \,\&\, x \in X \to y \in X).$$

3. $t_1(x) = t_2(y)$, *where t_1 and t_2 are fixed terms of the structure $\mathcal{T}$.*

4. $t(x) \in Y$, *where t is a fixed term.*

Lemma 6.5.1 *Suppose that Rabin automata $\mathcal{A}_1$ and $\mathcal{A}_2$ represent the formulas $\Phi_1(\bar{X}, \bar{x})$ and $\Phi_2(\bar{X}, \bar{x})$, respectively. Then there exist Rabin automata representing*

$$\Phi_1(\bar{X}, \bar{x})\mu\Phi_2(\bar{X}, \bar{x}),\ \neg\Phi_1(\bar{X}, \bar{x}),\ Q_i x_i \Phi_1(\bar{X}, \bar{x}),\ \textit{and}\ Q_j X_j \Phi_1(\bar{X}, \bar{x}),$$

where $\mu \in \{\bigvee, \&, \to\}$, $Q_j \in \{\forall, \exists\}$, $j = 1, \ldots, m-k$, $i = m-k+1, \ldots, m$.

Proof. Given Rabin automata $\mathcal{A}_1$ and $\mathcal{A}_2$, we can consider the automata $\mathcal{A}_1 \oplus \mathcal{A}_2$, $\mathcal{A}_1 \times \mathcal{A}_2$, and $\mathcal{A}_1^c$ that accept the union $L(\mathcal{A}_1) \bigcup L(\mathcal{A}_2)$, the intersection $L(\mathcal{A}_1) \bigcap L(\mathcal{A}_2)$, and the complement of $L(\mathcal{A}_1)$, respectively. Using the assumption that for each $i = 1, 2$ the automaton $\mathcal{A}_i$ represents $\Phi_i(\bar{X}, \bar{x})$, and using the fact that Rabin recognizable languages are closed under union, intersection, and complementation, we see that the automata

$$\mathcal{A}_1 \oplus \mathcal{A}_2,\ \mathcal{A}_1 \times \mathcal{A}_2,\ \mathcal{A}_1^c$$

represent the formulas

$$\left(\Phi_1(\bar{X}, \bar{x}) \bigvee \Phi_2(\bar{X}, \bar{x})\right),\quad \Phi_1(\bar{X}, \bar{x})\&\Phi_2(\bar{X}, \bar{x}),\quad \neg\Phi_1(\bar{X}, \bar{x}),$$

respectively. This can be proved in a standard way as we did for Büchi automata.

Now suppose that $\Phi(\bar{X}, \bar{x})$ is $\exists X_i \Phi_1(\bar{X}, \bar{x})$. Without loss of generality, we can assume that $X_i = X_1$. Consider the Rabin automaton $\mathcal{A}_1$ over the alphabet $\Sigma = \{0, 1\}^m$ which represents the formula $\Phi_1(\bar{X}, \bar{x})$. The alphabet Σ is $\Sigma_1 \times \Sigma_2$, where $\Sigma_1 = \{0, 1\}$ and $\Sigma_2 = \{0, 1\}^{m-1}$. By the Projection Theorem about Rabin recognizable languages, there exists an automaton $\mathcal{B}$ which accepts the projection $pr_2(L(\mathcal{A}_1))$ of the set $L(\mathcal{A}_1)$. Then it is not hard to see that $\mathcal{B}$ represents $\exists X_1 \Phi_1(\bar{X}, \bar{x})$.

Similarly, one can prove that there exists an automaton which represents $\exists x_j \Phi_1(\bar{B}, b_{m-k+1}, \ldots, x_j, \ldots, b_m)$. □

Exercise 6.5.6 *Finish the proof of the lemma in greater detail.*

Lemma 6.5.2 *Let Φ be an atomic formula. There exists an automaton which represents Φ.*

Proof. The first two examples at the beginning of this subsection show that the lemma is true for the atomic formulas $x_2 \in X_1$ and $L(x_1) = x_2$. For the other atomic formulas see Exercise 6.5.5. □

From the above lemmas we have the following theorem.

Theorem 6.5.2 *There exists a procedure which for every monadic second order formula $\Phi(\bar{X}, \bar{x})$ constructs a Rabin automaton $\mathcal{A}$ representing the formula.*

Proof. We first note that the operations that produce Rabin automata accepting the union, intersection, complements, and projections of Rabin recognizable languages can be carried out effectively. Now the proof of the theorem is by induction on the complexity of the formula $\Phi(\bar{X}, \bar{x})$. The lemma above proves the theorem for atomic formulas, that is for the basic step of our induction. Lemma 6.5.1 of this subsection proves the inductive step and hence the theorem.

6.5.5 Definability and Decidability. Consider the set $P(\mathcal{T})$ of subsets of $\mathcal{T}$. Let R be a collection of m-tuples of subsets of $\mathcal{T}$. We recall that $R \subset P(\mathcal{T})^m$ is **definable** if there exists a monadic second order formula $\Phi(X_1, \ldots, X_m)$ such that $R = \{(B_1, \ldots, B_m) | \mathcal{T}_2 \models \Phi(B_1, \ldots, B_m)\}$. The relationship between $\{0, 1\}^m$-valued trees and m-tuples of subsets of $\mathcal{T}$ suggests the following definition.

Definition 6.5.3 *The set $R \subset P(\mathcal{T})^m$ is* **Rabin definable** *if there exists a Rabin automaton $\mathcal{A}$ such that the language*

$$L_R = \{\mathbf{tree}(\bar{B}) \mid \bar{B} \in R\}$$

is accepted by the Rabin automaton $\mathcal{A}$.

Thus, by this definition any set R of m-tuples of sets naturally determines the language L_R of $\{0, 1\}^m$-valued trees. The two theorems proved in the previous two subsections give us the following fundamental result that connects Rabin recognizable languages with definable relations.

Theorem 6.5.3 *A set $R \subset P(\mathcal{T})^m$ is definable if and only if R is Rabin definable.*

Proof. The proof is in fact provided in the previous two subsections. Theorem 6.5.1 shows that any Rabin definable relation is definable. Similarly, Theorem 6.5.2 shows that any definable relation is Rabin definable. The theorem is proved.

Theorem 6.5.4 *The monadic second order theory of two successors, that is $S2S$, is decidable.*

Proof. Let Ψ be a sentence. We want to check whether or not Ψ belongs to $S2S$. We can assume that Ψ is equivalent to a formula either of the form $\exists x \Phi(x)$ or of the form $\exists X \Phi(X)$. Consider the case when the sentence Ψ has the form $\exists X \Phi(X)$. The case when Ψ is of the form $\exists x \Phi(x)$ is treated similarly. There exists a Rabin automaton $\mathcal{A}$ that represents $\Phi(X)$. Therefore, for all subsets $B_1 \subset \mathcal{T}$, the structure $\mathcal{T}$ satisfies $\Phi(B_1)$ if and only if the Rabin automaton $\mathcal{A}$ accepts $\mathbf{tree}(B_1)$. Thus, there exists a $B_1 \subset \mathcal{T}$ such that $\mathcal{T}$ satisfies $\Phi(B_1)$ if and only if there exists a tree of the form $\mathbf{tree}(B_1)$ accepted by $\mathcal{A}$. It follows that $\exists X \Phi(X)$ is true in $\mathcal{T}$

if and only if $L(\mathcal{A}) \neq \emptyset$. Thus, we have reduced the satisfiability problem for $\exists X \Phi(X)$ to the emptiness problem for a Rabin automaton representing $\Phi(X)$. Since the emptiness problem for Rabin automata is decidable, we see that $S2S$ is also decidable. This proves the theorem.

6.6 The Structure with ω Successors

The structure with ω successors is more complex than the structure $\mathcal{T}$ with two successors. Informally, the structure has infinitely many successor functions. Intuitively the structure with infinitely many successors has more information than the structure $\mathcal{T}$. However, we will show in this section that the structure with infinitely many successors can be interpreted in $\mathcal{T}$.

Formally, the structure with ω successors, denoted by $\mathcal{T}_\omega$, is defined as follows.

1. The domain T_ω is the set of all finite words over the infinite alphabet $\{0, 1, 2, 3, \ldots\}$. In other words,
$$T_\omega = \{0, 1, 2, 3, \ldots\}^*.$$
2. The structure has infinitely many unary *successor* operations denoted by $r_0, r_1, r_2, \ldots$. Each r_i is defined as follows. For all $u \in T_\omega$,
$$r_i(u) = ui.$$
3. The structure contains the prefix relation $\leq$. For all $u, v \in T_\omega$, $u \leq v$ if and only if either $u = v$ or u is a prefix of v.
4. Finally the structure contains the lexicographic ordering $\preceq$. For all $u, v \in T_\omega$, $u \preceq v$ if and only if there exists a prefix z of both u and v such that for some $i < j$, $r_i(z) \leq u$ and $r_j(z) \leq v$.

Thus, the structure $\mathcal{T}_\omega$ we have just defined is written as:
$$\mathcal{T}_\omega = (T_\omega, r_0, r_1, \ldots, \leq, \preceq).$$

We note that unlike the case with two successors, the relations $\leq$ and $\preceq$ belong to the type of the structure $\mathcal{T}_\omega$. Our goal is to show that the monadic second order theory of the structure $\mathcal{T}_\omega$, denoted by $S\omega S$, is decidable.

In order to show that $S\omega S$ is decidable we proceed as follows.

1. We will construct a definable subset D of $\mathcal{T}$.
2. By induction on i, we will construct a unary function f_i on D such that f_i is definable.

3. We will also construct two definable relations $\leq_1$ and $\preceq_1$ on D.
4. We will then guarantee that the structure $\mathcal{T}_\omega$ is isomorphic to the structure $(D, f_0, f_1, \ldots, \leq_1, \preceq_1)$.

Given the fact that $\mathcal{T}_\omega$ is isomorphic to the structure $(D, f_0, f_1, \ldots, \leq_1, \preceq_1)$, by Proposition 6.4.1, these two structures have the same theory. Having these D, $f_0, \ldots, f_i, \ldots, \leq_1$, and $\preceq_1$ defined, we then can show that the monadic second order theory of $\mathcal{T}_\omega$ is decidable.

The lemma below shows that it suffices to construct the set D, functions f_i, relations $\leq_1$ and $\preceq_1$ that satisfy the conditions above.

Lemma 6.6.1 *If there exist D, f_i, $i \in \omega$, $\leq_1$ and $\preceq_1$ that satisfy conditions* (1), (2), (3), *and* (4) *stated above, then the theory $S\omega S$ is decidable.*

Proof. The idea is quite simple. We take any sentence Φ of the structure $\mathcal{T}_\omega$ and transform it into a sentence $\Phi^{(t)}$ of the structure $\mathcal{T}$. The transformation should preserve satisfaction: Φ is satisfied in $\mathcal{T}_\omega$ if and only if $\Phi^{(t)}$ is satisfied in $\mathcal{T}$. Since $S2S$ is decidable, we then see that $S\omega S$ is also decidable.

Here now is the process for the transformation of Φ into $\Phi^{(t)}$. The process uses the fact that the functions f_i, relation $\leq_1$, $\preceq_1$ and the domain D are all definable. First, we transform any term q of the language of $\mathcal{T}_\omega$ into the term q^t by replacing each r_i occurring in q with f_i. Then we have the following:

- The atomic formula $q \in X$ is transformed into the formula $q^t \in X$, where q is a term
- The atomic formula $q_1 = q_2$, where q_1 and q_2 are terms, is transformed into the formula $q_1^t = q_2^t$.
- The formulas $x \leq y$ and $x \preceq y$ are transformed into $x \leq_1 y$ and $x \preceq_1 y$, respectively.
- The formula $(\Phi_1 \& \Phi_2)$ is transformed into $(\Phi_1^{(t)} \& \Phi_2^{(t)})$.
- The formula $(\Phi_1 \bigvee \Phi_2)$ is transformed into $(\Phi_1^{(t)} \bigvee \Phi_2^{(t)})$.
- The formula $(\Phi_1 \rightarrow \Phi_2)$ is transformed into $(\Phi_1^{(t)} \rightarrow \Phi_2^{(t)})$.
- The formula $(\neg\Phi)$ is transformed into $\neg\Phi^{(t)}$.
- The formula $\forall X \Phi$ is transformed into $\forall X(X \subset D \rightarrow \Phi^{(t)})$. Similarly, the formula $\forall x \Phi$ is transformed into $\forall x(x \in D \rightarrow \Phi^{(t)})$.
- The formula $\exists X \Phi$ is transformed into $\exists X(X \subset D \& \Phi^{(t)})$. Similarly, the formula $\exists x \Phi$ is transformed into $\exists x(x \in D \& \Phi^{(t)})$.

Now it is not hard to see that for any sentence Φ, Φ is in $S\omega S$ if and only if $\Phi^{(t)}$ is in $S2S$. □

Exercise 6.6.1 *Finish the proof of the lemma in greater detail.*

Now our goal is to find the set D and functions f_i, $i \in \omega$, that satisfy the conditions (1), (2), (3), and (4) above.

Let D be the set

$$D = \{\lambda\} \bigcup \{1^{n_1}01^{n_2}0 \dots 1^{n_k}0 \mid k \geq 1, 1 \leq i \leq k, n_i \geq 1\}.$$

The set D contains, for example, all strings of the form 10, 110, 1110, 1^n0, $n > 0$.

Lemma 6.6.2 *The set D is definable.*

Proof. Note that $y \in D$ if and only if either $y = \lambda$ or $R(\lambda) \leq y$ and there is a proper prefix x of y such that $L(x) = y$ and for every proper prefix x_1 of y if $L(x_1) < y$, then $R(L(x_1)) < y$. So now consider the formula $\phi(y)$:

$$(y = \lambda) \vee [(R(\lambda) \leq y \;\&\; \exists x(x < y \;\&\; L(x) = y)$$
$$\&\; \forall x_1(L(x_1) < y \rightarrow R(L(x_1)) < y)].$$

We leave the reader to check that $y \in D$ if and only if $\mathcal{T}$ satisfies $\phi(y)$. We leave it to the reader to check the rest of the proof.

Exercise 6.6.2 *Show that the formula $\phi(y)$ considered in the lemma above defines the set D.*

We are now ready to define functions f_i, $i \in \omega$ on the set D. To define f_i, we need first to define the relations $\leq_1$ and $\preceq_1$. Well, the definitions of $\leq_1$ and $\preceq_1$ are quite easy. We say that $x \leq_1 y$ if and only if $x, y \in D$ and $x \leq y$, where $\leq$ is the prefix relation on $\mathcal{T}$. Thus, $\leq_1$ is simply the restriction of $\leq$ on the set D. The ordering $\preceq_1$ is also defined to be the restriction of the original $\preceq$ to the set D.

Lemma 6.6.3 *Let $x \in D$. Then the nodes $x10, x110, x1110, \dots$ have the following properties:*

1. *The nodes belong to D.*
2. *If $y \in D$ is distinct from x and*

$$\mathcal{T} \models x \leq_1 y \;\&\; \forall z \in D\left(x \leq_1 z \;\&\; z \leq_1 y \rightarrow z = x \bigvee z = y\right),$$

then $y = x1^n0$ for some $n \geq 1$. Moreover,

$$x10 \preceq_1 x110 \preceq_1 x1110 \preceq_1 \cdots.$$

Proof. We leave it to the reader to prove the lemma in the exercise below. □

Exercise 6.6.3 *Prove the lemma above.*

For each $x \in D$, we call the elements

$$x10, x110, x1110, \dots$$

D-immediate successors of x. Now we define the operations $f_0, f_1, \dots$ by induction on i.

Basic Step. $f_0(x) = y$ if and only if $x, y \in D$ and y is the smallest D-immediate successor of x with respect to the lexicographical ordering $\preceq_1$ such that $x \preceq_1 y$.

Induction Step. Suppose that $f_0, \dots, f_i$ have been defined. Then $f_{i+1}(x) = y$ if and only if $x, y \in D$ and y is the smallest D-immediate successor of x with respect to the lexicographical ordering $\preceq_1$ such that $y \neq f_k(x)$ for all $k \leq i$.

Exercise 6.6.4 *Let $x \in D$. Prove that $f_i(x) = x1^{i+1}0$ for all i.*

The next lemma (and the exercise) shows that each function f_i is definable.

Lemma 6.6.4 *Each function f_i, $i \in \omega$, is definable.*

Proof. Clearly, f_0 is definable because so are the set D and the relation $\leq_1$. Assume that $f_0, \dots, f_i$ are definable. Then clearly f_{i+1} is definable since the definition of f_{i+1} involves the definitions of D, $f_0, \dots, f_i$, and $\leq_1$ and $\preceq_1$. This proves the lemma.

Exercise 6.6.5 *Write down, by induction, the formulas defining each of the functions f_i, $i \in \omega$.*

Lemma 6.6.5 *The structure $(D, f_0, f_1, \dots, \leq_1, \preceq_1)$ is isomorphic to the structure $\mathcal{T}_\omega$.*

Proof. We define a mapping g from $\mathcal{T}_\omega$ on D as follows. Let u be in T_ω. Then

$$u = r_{i_0}(\dots(r_{i_n}(\lambda))\dots)$$

for some sequence $r_{i_0}, \dots, r_{i_n}$ of the successor functions. Note that $\lambda \in D$. Then we set $g(u)$ to be

$$f_{i_0}(\dots(f_{i_n}(\lambda))\dots).$$

It is not hard to see that g is indeed an isomorphism from $\mathcal{T}_\omega$ onto $(D, f_0, f_1, \dots, \leq_1, \preceq_1)$. The lemma is proved.

From these lemmas we obtain the following theorem.

Theorem 6.6.1 *The theory $S\omega S$ is decidable.* □

Exercise 6.6.6 *Let $\mathcal{T}_n$ be the structure with exactly n successor functions, $n > 2$. Consider SnS, the monadic second order theory of $\mathcal{T}_n$. Prove that SnS is decidable.*

6.7 Applications to Linearly Ordered Sets

We recall that a partially ordered set $(A, \leq)$ is linearly ordered if for all $x, y \in A$ either $x \leq y$ or $y \leq x$. We refer the reader to the first chapter to go through some examples of linearly ordered sets. The goal of this section is to prove that the monadic second order theory of all countable linearly ordered sets is decidable. In order to prove this result we need to present two simple but interesting algebraic theorems about linearly ordered sets. The first result states that any countable linearly ordered set can be embedded into the linearly ordered set of rational numbers. The second result states that two dense countable linearly ordered sets with no greatest and smallest elements are isomorphic. The proofs of these results are not hard but constitute a basis for the known back and forth argument constructions in model theory and algebra. The first subsection will be devoted to proving these algebraic facts. In the second subsection we will show that the monadic second order theory of all (countable) linearly ordered sets is decidable.

6.7.1 Two Algebraic Facts. We begin with the following definition, important in achieving the goal of this section. Roughly, the definition formalizes the concept of one linearly ordered set being inside some other linearly ordered set.

Definition 6.7.1 *A linearly ordered set $(B, \leq)$* **is embedded into** *a linearly ordered set $(A, \leq)$ if there exists a mapping f from B into A such that*

1. *for all $x, y \in B$, if $x \leq y$, then $f(x) \leq f(y)$;*
2. *for all distinct $x, y \in A$, $f(x) \neq f(y)$.*

The function f is called an **embedding** *of $(B, \leq)$ into $(A, \leq)$.*

Example 6.7.1 *Every finite linearly ordered set is embedded into $(\omega, \leq)$.*

To see this take a finite linearly ordered set $(A, \leq)$. List all elements $a_0 < \cdots < a_n$ of A in the order of A. Map each a_i into i. The mapping is an embedding of $(A, \leq)$ into $(\omega, \leq)$. In fact, one can show that any finite linearly ordered set can be embedded into any infinite linearly ordered set.

Example 6.7.2 *The linearly ordered set $(\omega, \leq)$ is embedded into $(Z, \leq)$. In turn, $(Z, \leq)$ is embedded into $(Q, \leq)$, where Q is the set of all rational numbers.*

Exercise 6.7.1 *Let Ł be an infinite linearly ordered set. Show that all finite linearly ordered sets can be embedded into Ł.*

Informally, if a linearly ordered set $(B, \leq)$ is embedded into linearly ordered set $(A, \leq)$ then we can assume that $(A, \leq)$ is bigger than $(B, \leq)$. A natural question arises as to whether there exists the largest (countable) linearly ordered set. The next theorem answers the question positively.

Theorem 6.7.1 *Any countable linearly ordered set $(A, \leq)$ can be embedded into $(Q, \leq)$, that is the linearly ordered set of rational numbers ordered naturally.*

Proof. Since A is countable we count all elements of A without repetition:

$$a_0, a_1, a_2, \ldots, a_n, \ldots.$$

Note that the sequence above is not necessarily in increasing order with respect to the ordering in A. Now we build our embedding from $(A, \leq)$ into $(Q, \leq)$ by stages. At each stage we define a mapping f_t on a_t and set f_t to be equal to f_{t-1} on all $a_0, \ldots, a_{t-1}$. Thus f_t will extend the previously defined mapping f_{t-1}. We then set f to be the mapping obtained by taking the union of all f_ts. The construction then will guarantee that f is the function that sets up an embedding from $(A, \leq)$ into $(Q, \leq)$.

Stage 0. We send a_0 to any rational number we like, say q_0. So we set $f_0(a_0) = q_0$.

Stage 1. We take a_1. There are two cases to consider. The first case is that $a_0 < a_1$. In this case we assign to a_1 any rational number we like, say q_1, which is greater than q_0. The second case is that $a_0 > a_1$. In this case we assign to a_1 any rational number we like, say q_1, which is now less than q_0. In either case we set $f_1(a_1) = q_1$ and $f_1(a_0) = f_0(a_0)$. Clearly, f_1 extends f_0.

Stage $t + 1$. Assume that we have defined the function f_t at the previous stage. Assume that $f_t(a_0) = q_0, \ldots, f_t(a_t) = q_t$. Let us list all elements from $\{a_0, \ldots, a_t\}$ in strictly increasing order with respect to the ordering $\leq$ in A:

$$a_{i_0} \leq a_{i_1} \leq \cdots \leq a_{i_t}.$$

By the inductive assumption on the function f_t, we can also assume that we have the following sequence of rational numbers in increasing order (with respect to the ordering of rationals):

$$q_{i_0} \leq q_{i_1} \leq \cdots \leq q_{i_t}.$$

Now take a_{t+1}. We want to assign a rational number q_{t+1} to the element a_{t+1} so that for all x, y on which f_{t+1} is defined, $x \leq y$ if and only if $f_{t+1}(x) \leq f_{t+1}(y)$. For a_{t+1} we now have three cases.

Case 1. a_{t+1} is greater than all $q_0, \ldots, q_t$. In this case we assign to a_{t+1} any rational number we like, say q_{t+1}, which is greater than all $q_0, \ldots, q_t$.

Case 2. a_{t+1} is less than all $q_0, \ldots, q_t$. In this case we assign to a_{t+1} any rational number we like, say q_{t+1}, which is less than all $q_0, \ldots, q_t$.

Case 3. Assume that a_{t+1} is between a_{i_k} and $a_{i_{k+1}}$ for some $0 \leq k \leq t - 1$. In this case we assign to a_{t+1} any rational number we like, say q_{t+1}, which is between q_{i_k} and $q_{i_{k+1}}$. Note that such a rational number exists since between any two distinct rational numbers there exists another one.

Now set $f_{t+1}(a_{t+1}) = q_{t+1}$ and leave the value of f_{t+1} on all $a_0, \ldots, a_t$ as before and go on to the next stage.

Thus, we have described our construction at stage $t + 1$. We set f to be the union of all f_ts, $t \in \omega$, constructed. In other words in order to compute the value of f on an element a, we do the following. We find the stage t at which $a_t = a$. Compute $f_t(a_t)$. Set $f(a)$ to be $f_t(a_t)$.

Now we leave it to the reader to check that f is indeed a desired isomorphic embedding from $(A, \leq)$ into $(Q, \leq)$. □

Exercise 6.7.2 *Show that the mapping f constructed in the proof of the theorem sets up an isomorphic embedding.*

Exercise 6.7.3 *Prove that $(\omega, \leq)$ cannot be embedded into $(\omega^-, \leq)$, where ω^- is the set of negative integers.*

Exercise 6.7.4 *Give an example of a countable linearly ordered set $(\mathcal{A}, \leq)$ with the following properties:*

1. *Any countable linearly ordered set can be embedded into $(A, \leq)$.*
2. *The linearly ordered set $(A, \leq)$ is not isomorphic to the linearly ordered set $(Q, \leq)$ of rationals.*

We now will prove the second fact about linearly ordered sets. The facts basically tells us that any linearly ordered set which exhibits properties of the rationals $(Q, \leq)$ is in fact isomorphic to the rationals. The linearly order set of the rational numbers $(Q, \leq)$ has the following two properties:

1. (*Density*) For all $x, y \in Q$ if $x < y$, then there exists a $z \in Q$ such that $x < z < y$.
2. The linearly ordered set $(Q, \leq)$ possesses neither a greatest nor a smallest element, that is, for any $x \in Q$, there exist elements $y, z \in Q$ such that $x < y$ and $z < x$.

Definition 6.7.2 *A linearly ordered set $(A, \leq)$ is Q-**like** if it is dense and possesses neither a greatest nor a smallest element.*

Now we prove our second algebraic fact about linearly ordered sets.

Theorem 6.7.2 *Two countable Q-like linearly ordered sets are isomorphic. In particular, every Q-like countable linearly ordered set is isomorphic to the linearly ordered set of rationals $(Q, \leq)$.*

Proof. The proof uses the idea of the proof from the previous theorem. So let $(A, \leq)$ and $(B, \leq)$ be two countable Q-like linearly ordered sets. We prove that these two are isomorphic based on the known *back and forth* argument, a refined version of the proof from the previous theorem. We construct an isomorphism from $(A, \leq)$ onto $(B, \leq)$ by stages. At even stages we make sure that elements of A are being assigned to elements of B and at odd stages we make sure that elements of B are covered by elements of A.

Since A and B are countable we count, without repetitions, all elements of A and B:

$$a_0, a_1, a_2, \ldots, a_n, \ldots, \qquad b_0, b_1, b_2, \ldots, b_n, \ldots,$$

respectively. We call the first sequence the A-list and the second sequence the B-list. Here is the construction.

Stage 0. We send a_0 to b_0. Set $f_0(a_0) = b_0$.

Stage 1. We take b_1. There are two cases to consider. The first case is that $b_0 < b_1$. In this case we assign to b_1 the first number a_{i_1} in the A-list which is greater than a_0. The second case is that $b_0 > b_1$. In this case we assign to b_1 the first a_{i_1} in the A-list which is less than a_0. In either case we set $f_1(a_{i_1}) = b_1$. Note that in either case the element a_{i_1} exists.

Stage $t+1 = 2k$. Assume that we have defined the function f_t at the previous stage. List all the elements in the domain of f_t in increasing order with respect to the ordering in A,

$$a_{i_0} < a_{i_1} < \cdots < a_{i_t}.$$

By the inductive assumption on function f_t, we can assume that we have the following sequence of elements in B listed in increasing order with respect to the ordering in B,

$$b_{i_0} < b_{i_1} < \cdots < b_{i_t},$$

so that $f_t(a_{i_0}) = b_{i_0}, \ldots, f_t(a_{i_t}) = b_{i_t}$. The induction hypothesis also allows us to assume that the elements $a_0, \ldots, a_{k-1}$ belong to the domain of f_t. Now take the first element $a_{i_{t+1}}$ in the A-list which does not belong to the domain of f_t. We want to assign an element $b_{i_{t+1}}$ to $a_{i_{t+1}}$ so that for all x, y on which f_{t+1} is defined, $x \leq y$ if and only if $f_{t+1}(x) \leq f_{t+1}(y)$. For $a_{i_{t+1}}$ we now have three cases.

Case 1. $a_{i_{t+1}}$ is greater than all $a_{i_0}, \ldots, a_{i_t}$. In this case we assign to $a_{i_{t+1}}$ the first element in the B-list, say $b_{i_{t+1}}$, not in the range of f_t greater than all $b_{i_0}, \ldots, b_{i_t}$.

Case 2. $a_{i_{t+1}}$ is less than all $a_{i_0}, \ldots, a_{i_t}$. In this case we assign to $a_{i_{t+1}}$ the first element in the B-list, say $b_{i_{t+1}}$ not in the range of f_t less than all $b_{i_0}, \ldots, b_{i_t}$.

Case 3. Assume that $a_{i_{t+1}}$ is between a_{i_k} and $a_{i_{k+1}}$ for some $1 \leq k \leq t - 1$. In this case we assign to $a_{i_{t+1}}$ the first element, say $b_{i_{t+1}}$, in the B-list which is between b_{i_k} and $b_{i_{k+1}}$.

We note that in each of the cases above the element $b_{i_{t+1}}$ desired exists because $(B, \leq)$ is a Q-like linearly ordered set. Now set $f_{t+1}(a_{i_{t+1}}) = b_{i_{t+1}}$ and leave the value of f_{t+1} on all $a_0, \ldots, a_{i_t}$ as before. Go to the next stage.

Stage $t + 1 = 2k + 1$. Do exactly the same as above by replacing elements in the A-list with the elements in the B-list. Go to the next stage.

Now we set f to be the union of all f_ts, $t \in \omega$, constructed. In other words, in order to compute the value of f on an element a, we do the following. We find the stage t at which the construction assigns an element b to a. Note that such a stage t exists. Compute $f_t(a)$. Set $f(a)$ to be $f_t(a)$.

We leave it to the reader to check that f is indeed a desired isomorphism from $(A, \leq)$ onto $(B, \leq)$. □

Exercise 6.7.5 *Finish the proof of the theorem above by showing that the function f constructed is indeed an isomorphism.*

Exercise 6.7.6 *Give examples of two uncountable Q-like linearly ordered sets which are not isomorphic.*

6.7.2 Decidability. In this part we use the two algebraic facts proved in the previous subsection in order to show that the monadic second order theory of countable linearly ordered sets is decidable. Here is the main theorem of this section.

Theorem 6.7.3 *The monadic second order theory of all countable linearly ordered sets is decidable.*

Proof. We begin by explaining the idea. We show that there exists a definable subset D of the binary tree $\mathcal{T}$ and a definable relation $\leq_D$ on D such that $(D, \leq_D)$ is a linearly ordered set isomorphic to the linearly ordered set $(Q, \leq)$ of rational numbers. Then by the theorem about embeddings of linearly ordered sets into $(Q, \leq)$ (see Theorem 6.7.1), we have the following. For every linearly ordered set $(B, \leq)$ there exists a subset $C \subset D$ such that $(B, \leq)$ and $(C, \leq_D)$ are isomorphic. Therefore, the set of all sentences of the monadic second order logic true in all countable linearly ordered sets coincides with the set of all sentences that are true in all $(C, \leq_D)$, where $C \subset D$. Hence the idea is to take any sentence F of the monadic second order language of linearly ordered sets and transform it into a sentence $F^{(t)}$ of $S2S$. The transformation should preserve the truth value of the sentences. In other words, $F^{(t)}$ is in $S2S$ if and only if F is true in all linearly ordered sets.

Now we implement the idea described above. Let D be

$$D = \{u101 \mid u \in \mathcal{T} \text{ and the string 101 occurs in } u101 \text{ just once}\}.$$

Lemma 6.7.1 *The set D is definable.*

Proof. It is easy to check that $u \in D$ if and only if there exists a $v \leq u$ such that the following conditions are satisfied:

1. $r_1(r_0(r_1(v))) = u$.
2. For all $v_1 \leq u$ it is not true that $r_1(r_0(r_1(v_1))) < v$.

Clearly, the statement above can be expressed in the monadic second order logic of two successors. The lemma is proved.

We denote the formula that defines the set D in the lemma above by $D(x)$. Let $\preceq_D$ be the restriction of $\preceq$ to the set D. Since $\preceq$ and D are definable we see that $\preceq_D$ is also a definable relation.

Lemma 6.7.2 *The pair set $(D, \preceq_D)$ is isomorphic to the linearly ordered set $(Q, \leq)$ of rational numbers.*

Proof. Since $\preceq_D$ is obtained by restricting $\preceq$ to the D and $\preceq$ is a linear ordering on the set of all nodes of the tree $\mathcal{T}$, clearly $(D, \preceq_D)$ is a linearly ordered set. We need to show that $(D, \preceq_D)$ is Q-like. Then by Theorem 6.7.2, the lemma will be proved.

Let $u101$ be in D. Then $u1101$ and $u00101$ are both in D. Note that $u101 \preceq_D u1101$ and $u00101 \preceq_D u101$. We conclude that $(D, \preceq_D)$ has neither maximal nor minimal elements. Now assume that $u101 \preceq_D v101$. Then for some w we have the following: $u101 = w0u_1101$ and $v101 = w1v_2101$. Then clearly $w1v_200101 \in D$. We conclude that $u101 \preceq_D w1v_200101 \preceq_D v101$. Hence the linearly ordered set $(D, \preceq_D)$ is Q-like. By Theorem 6.7.2, $(D, \preceq_D)$ is isomorphic to $(Q, \leq)$. The lemma is proved.

Now we need to prove the theorem. Let F be a formula of the monadic second order logic of linearly ordered sets. We transform F into the formula $F^{(t)}$ by induction as follows.

Basic Step. Atomic formulas $x \leq y$ and $x \in X$ are transformed into $x \preceq_D y$ and $x \in X$, respectively.

Induction Step. If Φ is of the form $\Phi_1 \tau \Phi_2$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1$, then we set $\Phi^{(t)}$ to be $\Phi_1^{(t)} \tau \Phi_2^{(t)}$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1^{(t)}$, respectively. If Φ is any of the formulas

$$\forall x \Phi_1(x), \ \forall X \Phi_1(X),$$

then we transform Φ into

$$\forall Z \forall x(Z \subseteq D \,\&\, x \in Z \rightarrow \Phi_1^{(t)}(x)), \quad \forall Z \forall X(Z \subseteq D \,\&\, X \subseteq Z \rightarrow \Phi_1^{(t)}(X)),$$

respectively. If Φ is any of the formulas

$$\exists x \Phi_1(x), \ \exists X \Phi_1(X),$$

then we transform it into

$$\forall Z \exists x (Z \subseteq D \to x \in Z \,\&\, \Phi_1^{(t)}(x)), \quad \forall Z \exists X (Z \subseteq D \to X \subseteq Z \,\&\, \Phi_1^{(t)}(X)),$$

respectively. Now the reader can check that Φ is true in all countable linearly ordered sets if and only if the transformed formula $\Phi^{(t)}$ belongs to $S2S$. Thus, we can conclude that the monadic second order theory of all countable linearly ordered sets is decidable (see the exercise below for details). □

Exercise 6.7.7 *Consider the transformation from Φ into $\Phi^{(t)}$ in the proof above. Prove that for every sentence Φ of the monadic order logic of linearly ordered sets, Φ is true in all countable linearly ordered sets if and only if the transformed formula $\Phi^{(t)}$ belongs to $S2S$.*

Exercise 6.7.8 *Call a linearly ordered set $(A, \leq)$* **well-ordered** *if every nonempty subset of A has a minimal element with respect to the ordering $\leq$. Do the following:*

1. *Show that $(\omega, \leq)$ is a well-ordered set.*
2. *Show that if L_1 and L_2 are well-ordered sets, then so are $L_1 \times L_2$ and $L_1 + L_2$. (See the first chapter for the definitions of $+$ and $\cdot$ operations.)*
3. *Show that the monadic second order theory of all countable well-ordered sets is decidable.*

Exercise 6.7.9 *A* **tree** *is a partially ordered set $(A, \leq)$ such that for all $x \in A$ the set $\{y \mid y \leq x\}$ is linearly ordered with respect to the ordering $\leq$ of A. Prove that the monadic second order theory of all finite trees is decidable.*

Exercise 6.7.10 *A* **forest** *is a partially ordered set $(A, \leq)$ such that there exist pairwise disjoint subsets $\{B_i\}_{i \in I}$ such that*

1. $A = \bigcup_{i \in I} B_i$;
2. *for each $i \in I$, the partially ordered set $(B_i, \leq)$ is a tree;*
3. *for all distinct $i, j \in I$ and all $x \in B_i$, $y \in B_j$, the elements x and y are not $\leq$-comparable.*

Show that the monadic second order theory of all finite forests is decidable.

Exercise 6.7.11 *A partially ordered set $(A, \leq)$ is a* **linear atlas** *if there exist pairwise disjoint infinite subsets $\{B_i\}_{i \in I}$ such that*

1. $A = \bigcup_{i \in I} B_i$;
2. *for all $i \in I$, $(B_i, \leq)$ is a linearly ordered set;*
3. *for all distinct $i, j \in I$, all $x \in B_i$, and $y \in B_j$, the elements x and y are not comparable.*

Show that the monadic second order theory of all countable linear atlasses is decidable.

6.8 Application to Unary Algebras

In this section we consider the class of structures known as the class of unary algebras. The section shows that the monadic second order theory of the class of unary algebras is decidable. The proof, as in the previous two sections, consists of two parts. First we provide some algebraic facts about unary algebras. In particular, we show that there exists, in some sense, universal unary algebras into which all unary algebras can be embedded. Second, based on the algebraic facts, we provide a reduction of the monadic second order theory of unary algebras to $S2S$. This reduction is more sophisticated than the ones used in the previous two sections.

6.8.1 Unary Structures. Unary algebras are simple mathematical structures that consist of domains and unary operations on the domains. Here is a formal definition.

Definition 6.8.1 *A* **unary algebra** *is a pair (A, f) consisting of a set A called the* **domain** *and a unary operation $f : A \to A$ on the set A.*

So we see that the language of the class of unary algebras contains just one functional symbol of arity 1. One can give many examples of unary algebras. Here are some of them:

1. The unary algebra (ω, S) whose domain is ω and the unary operation is the successor function.
2. The unary algebra $(\omega, x \to x^2)$, where the unary operation maps every number n to n^2.
3. The unary algebra $(Q, x \to 5x)$, where the unary operation maps every rational number q to $5 \times q$.
4. $(R, \sin(x))$, where R is the set of all real numbers and $\sin(x)$ is the sine function.

Our goal is to show that the set of all sentences of the monadic second order logic which are true in all countable unary algebras is decidable.

We need to develop some terminology for unary algebras. So let (A, f) be a unary algebra. Take an $a \in A$. Consider the sequence:

$$f^0(a), f^1(a), f^2(a), \ldots, f^n(a), \ldots,$$

where $f^0(a) = a$ and $f^{k+1}(a) = f(f^k(a))$ for all $k \geq 1$. We call this sequence the **orbit of** a. Set $O(a) = \{f^i(a) \mid i \in \omega\}$.

Definition 6.8.2 *Two elements a and b of a unary algebra (A, f) are* **connected** *if for some $n, m \in \omega$, $f^n(a) = f^m(b)$. If a and b are connected we denote it by $a \sim b$.*

Hence a and b are equivalent if their orbits meet. Thus, if $O(a) \bigcap O(b) \neq \emptyset$, then a and b are connected. It is not hard to prove the following lemma.

Lemma 6.8.1 *The relation $\sim$ is an equivalence relation.* □

Exercise 6.8.1 *Prove the lemma.*

Definition 6.8.3 *A unary algebra (B, g) is a* **subalgebra** *of the unary algebra (A, f) if $B \subset A$ and for all $b \in B$, $f(b) = g(b)$.*

Thus, for example any orbit $O(a)$ of the unary algebra (A, f) can be considered as a subalgebra of (A, f) because $f(x) \in O(a)$ for all $x \in O(a)$.

Let $X \subset A$ be an $\sim$-equivalence class of the algebra (A, f). Clearly, if $x \in X$, then $f(x) \in X$. Therefore, X is closed under the unary operation f. This allows us to consider the unary algebra (X, g), where $g(x) = f(x)$ for all $x \in X$. Thus, (X, g) is a subalgebra of the original algebra (A, f). From the definition of $\sim$ we see that (X, g) satisfies the following property. For all $x, y \in X$ there exist $n, m \in \omega$ such that $f^n(x) = f^m(y)$. This observation suggests the following definition.

Definition 6.8.4 *An algebra (A, f) is* **connected** *if for all $a, b \in A$ there exist $n, m \in \omega$ such that $f^n(a) = f^m(b)$.*

Let (A, f_1) and (B, f_2) be unary algebras such that $A \bigcap B = \emptyset$. Using these two algebras we can form a new algebra $(A \bigcup B, f)$, where $f(x) = f_1(x)$ if $a \in A$, and $f(x) = f_2(x)$ if $x \in B$. We call this algebra the **sum** of (A, f_1) and (B, f_2). Similarly, we can define the sum of infinitely many unary algebras

$$(A_1, f_1), (A_2, f_2), \ldots$$

where $A_i \bigcap A_j = \emptyset$ for all $i \neq j$. Thus, the sum is the algebra

$$\left(A_1 \bigcup A_2 \bigcup A_2 \bigcup A_3, \ldots, f\right),$$

where for all $a \in A_1 \bigcup A_2 \bigcup A_2 \bigcup A_3 \bigcup \cdots$, we have $f(a) = f_i(a)$ if $a \in A_i$. The next lemma shows the reason for introducing the sum of unary algebras.

Lemma 6.8.2 *Every unary algebra (A, f) is a sum of connected unary algebras.*

Proof. Consider the sequence $A_1, A_2, \ldots$ of all $\sim$-equivalence classes of the algebra (A, f). Each A_i is closed with respect to f. Consider the restriction of f to the set A_i. Let f_i be the restriction. Each (A_i, f_i) forms a connected algebra as noted above. The union of all A_is is A. Hence the sum of connected unary algebras (A_i, f_i) is in fact the original unary algebra (A, f). The lemma is proved.

6.8.2 Enveloping Algebras. This subsection explains enveloping algebras. Informally, these algebras are those that contain all connected algebras as their subalgebras. More formally, we begin with the following technical notion. An n-**cycle** is the algebra $(\{0, \ldots, n-1\}, f)$, where $f(0) = 1, \ldots, f(n-2) = n-1$, $f(n-1) = 0$. An ω-**cycle** is the algebra $(\{0, 1, 2, \ldots\}, S)$, where S is the successor function.

Definition 6.8.5 *An algebra is called* **prime** *if it is isomorphic to either an n-cycle for some $n \in \omega$ or the ω-cycle.*

The next lemma proves that every algebra contains a prime subalgebra thus justifying the name given to prime algebras.

Lemma 6.8.3 *Every unary algebra $\mathcal{A}$ contains a prime subalgebra.*

Proof. Let $a \in A$. Then the set $\{f^m(a) \mid m \in \omega\}$ forms a subalgebra of $\mathcal{A}$. This subalgebra is either isomorphic to the ω-cycle or contains a subalgebra isomorphic to an n-cycle. The lemma is proved.

Definition 6.8.6 *The* **signature** *of a connected algebra is n, $n \in \omega$, if it contains a prime subalgebra isomorphic to the n-cycle. Otherwise the signature is ω.*

The next lemmas show that the signature of any connected algebra is well defined.

Lemma 6.8.4 *The signature of every connected algebra is uniquely determined.*

Proof. Let (A, f) be a connected algebra. Take an $a \in A$. Consider the orbit $O(a)$ of a. If the orbit is infinite, then (A, f) contains a subalgebra isomorphic to the ω-cycle. Since (A, f) is connected, the signature of (A, f) must be ω. If the orbit is finite, then it contains a prime subalgebra isomorphic to some n-cycle. Since A is connected any other orbit must contain the same prime subalgebra. This proves the lemma.

Now we explain enveloping algebras. Informally, the enveloping algebra of signature n, where n is a natural number or ω, is an algebra into which any connected algebra of the same signature can be embedded. This resembles the fact that any linearly ordered set can be embedded into $(Q, \leq)$.

Definition 6.8.7 *Let (A, f) be a prime algebra. The* **enveloping algebra** *(E, g) of (A, f) is defined as follows. Let N be the set of all positive natural numbers. Let $N^\star$ be the set of all finite strings over N. Consider*

$$E = A \cdot N^\star.$$

On E we define the unary function g by the rule: $g(ai_1 \ldots i_k) = ai_1 \ldots i_{k-1}$ if $k \geq 1$; if $k = 0$, then $g(a) = f(a)$.

We note that each element of E is of the form $ai_1 \ldots i_k$. Note that A is certainly a subset of E. In Figure 6.1 we present the enveloping algebra, when $A = \{x, y\}$ and $f(x) = y$, $f(y) = x$. An arrow from a to b means that $g(a) = b$.

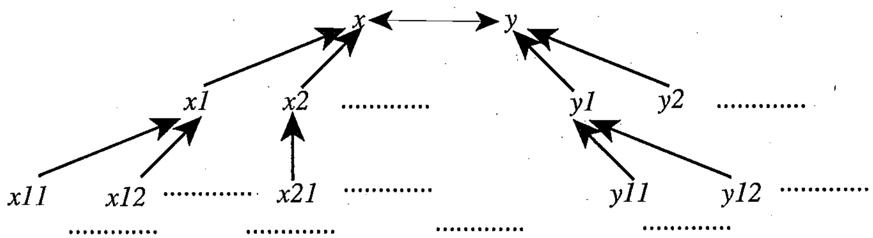

Figure 6.1: An enveloping algebra.

We now need one definition in order to state some properties of enveloping algebras.

Definition 6.8.8 *We say that a unary algebra (B, h)* **is embedded** *into a unary algebra (E, g) if there exists a mapping ϕ from B into E such that*

- *for all $b \in B$, we have $\phi(h(b)) = g(\phi(b))$;*
- *for all $b_1 \neq b_2$ in B, we have $\phi(b_1) \neq \phi(b_2)$.*

The next lemma lists several properties of the enveloping algebra (E, g).

Lemma 6.8.5 *The enveloping algebra (E, g) of (A, f) satisfies the following properties:*

1. *The signature of (E, g) coincides with the signature of (A, f).*
2. *For each $y \in E$ there exist infinitely many x such that $g(x) = y$.*
3. *Let (B, h) be a connected algebra of the signature of (A, f). Then (B, h) can be embedded into (E, g).*

Proof. The proof of (1) follows from the definition of the signature. In order to prove (2) take any element $y \in E$. Then the unary operation g maps $y1, y2, y3, \ldots$ into y. We conclude that y has infinitely many x for which $g(x) = y$. We leave it to the reader to prove the last part of the lemma. □

Exercise 6.8.2 *Finish the proof of the lemma above.*

Thus, we conclude this subsection with the next results which, roughly speaking, states that the sums of enveloping algebras are universal objects in the class of all unary algebras.

Theorem 6.8.1 *Every unary algebra can be embedded into a sum of enveloping algebras.*

Proof. Let (A, f) be a unary algebra. Then we have already shown that this algebra is a sum of connected algebras $(A_1, f_1), (A_2, f_2), \ldots$. Consider the enveloping algebra (E_i, g_i) for each connected algebra (A_i, f_i). Clearly, $A_i \subset E_i$ and (A_i, f_i) is a subalgebra of (E_i, g_i). Moreover, $E_i \bigcap E_j = \emptyset$ for all $i \neq j$. Also note that the mapping q_i that maps each $a \in A_i$ into a itself is an embedding of (A_i, f_i) into (E_i, g_i). Hence, the algebra (A, f) is embedded into the sum of enveloping algebras $(E_1, g_1), (E_2, g_2), \ldots$. This proves the theorem.

6.8.3 Decidability. In this subsection we use the algebraic facts proved in the previous subsections in order to show that the monadic second order theory of all countable unary algebras is decidable. Below is the main theorem of this section. We note that the proof of the theorem contains some exercises whose proofs are quite simple and follow from the definitions that will be provided.

Theorem 6.8.2 *The monadic second order theory of all countable unary algebras is decidable.*

Proof. The idea of proving the theorem is the following. We will interpret the theory of unary algebras in $S\omega S$. We already know that $S\omega S$ is interpreted in $S2S$. Therefore, the theory of unary algebras will be decidable. Roughly speaking, the interpretation of the theory of unary algebras in $S\omega S$ will be done as follows. We construct a formula $F(x, y, Z)$ in the language of $\mathcal{T}_\omega$ so that the following properties hold:

1. For every subset C of $\mathcal{T}_\omega$, the set of pairs (x, y) for which $F(x, y, C)$ holds true determines a unary operation. Let us denote the unary operation by f_C.
2. By (1), the structure $(Dom(f_C), f_C)$ is a unary algebra.
3. The unary algebra $(Dom(f_C), f_C)$ is a sum of enveloping algebras.
4. For every unary algebra (A, f) that is a sum of enveloping unary algebras, there exists a $C \subset \mathcal{T}_\omega$ such that $(Dom(f_C), f_C)$ is isomorphic to (A, f).

From the results of the previous subsection we therefore can conclude the following. Let (A, f) be a unary algebra. Then (A, f) can be embedded into a unary algebra (E, f) which is a sum of enveloping algebras. By the assumption on $F(x, y, Z)$ there exists a set $C \subset \mathcal{T}_\omega$ such that the unary algebra $(Dom(f_C), f_C)$ is isomorphic to (E, f). Therefore, there must exist a subset C_1 of the set $Dom(f_C)$ such that (A, f) is isomorphic to (C_1, f_{C_1}), where f_{C_1} is the restriction of f_C to the set C_1. Thus, a sentence is true in all unary algebras if and only if the statement relativized to all sets C and subsets C_1 of C that are subalgebras of $(Dom(f_C), f_C)$ is true. Consequently, the existence of the formula $F(x, y, Z)$ will allow us to transform any sentence of the monadic second order logic of unary algebras into a sentence of $\mathcal{T}_\omega$. This transformation will preserve the satisfaction properties of formulas. We will formally show how to make this transformation at the end of the proof. Let us now concentrate on constructing the formula $F(x, y, Z)$.

We explain how to construct $F(x, y, Z)$. The explanation will be clear enough to see how to write down the formula $F(x, y, Z)$. Let C be a subset of $\mathcal{T}_\omega$ such that the following properties hold:

1. C is contained in the set $\{0^n10^m \mid n, m \geq 1\}$. Note that the set $\{0^n10^m | n, m \geq 1\}$ is definable in the language of $\mathcal{T}_\omega$.
2. For every $n \in \omega$, the set C contains at most one word of the form 0^n10^m.

Note that there exists a formula $\Phi_1(X)$ in the language of $\mathcal{T}_\omega$ such that $\Phi_1(C)$ is true if and only if C satisfies the two properties above.

Exercise 6.8.3 *Write down the formula $\Phi_1(X)$ whose existence is claimed above.*

Now suppose that C satisfies the two conditions above. Take a natural number n. If there exists an m such that $0^n10^m \in C$, then let

$$A_n = \{0^n10^i \mid i = 0, 1, 2, \ldots, m\}.$$

If there does not exist an m such that $0^n10^m \in C$, then let

$$A_n = \{0^n10^i \mid i \in \omega\}.$$

Note that the sets $A_0, A_1, A_2, \ldots$ are pairwise disjoint. Now set $B_n = A_n \cdot N^\star$. Thus $x \in B_n$ if and only if $x = a_n i_1 \ldots i_k$, where $a_n \in A_n, i_1, \ldots, i_k$ are positive integers and $k \in \omega$. Define

$$B(C) = B_0 \bigcup B_1 \bigcup B_2 \bigcup \cdots.$$

Clearly, the set $B(C)$ depends on the choice of C. Note that there exists a formula $\Phi_2(x, Z)$ such that $\Phi_2(a, C)$ holds if and only if $\Phi_1(C)$ holds and $a \in B(C)$.

Exercise 6.8.4 *Write down the formula $\Phi_2(x, Z)$ whose existence is claimed above.*

As we noted, for C that satisfies the formula $\Phi_1(X)$, the sets $A_0, A_1, \ldots$ are pairwise disjoint. Hence the sets $B_0, B_1, \ldots$ are also pairwise disjoint. The domain of the unary algebra $(Dom(f_C), f_C)$ will be the set $B(C)$. We now need to define the function f_C on the set $B(C)$. The idea in defining f_C is that each B_n will be an enveloping algebra, the function f_C will be the predecessor function on all elements of B_n not of the form 0^n10^i. The definition of f_C on 0^n10^i will be different depending on whether or not 0^n10^i is in C. Here is a more formal definition of f_C. Take x in $B(C)$. There exists an n such that x is in B_n. Then x is of the form 0^n10^iz. Assume that $z \neq \lambda$. Then $f_C(x) = pred(x)$. If $z = \lambda$, then we proceed as follows. If $0^n10^i \notin C$, then $f(x) = 0^n10^{i+1}$; otherwise, e.g., if $0^n10^i \in C$, then $f_C(x) = 0^n1$. In other words, f_C is the function on B_n which acts as the predecessor on all strings of the type 0^n10^iz, where $z \in N^\star$, and makes a cycle of length i on all strings $0^n1, \ldots, 0^n10^i$ if 0^n10^i belongs to C, or makes an ω-cycle if no 0^n10^i belongs to C, $i \in \omega$. Thus we have given a definition of the unary algebra (B, f_C). Note that this algebra depends on the choice of C and is a sum of enveloping algebras.

Now we are ready to define the formula $F(x, y, Z)$. The formula states that the triple (a, b, C) satisfies the formula if and only if the following holds:

1. C satisfies the following properties:
   (a) $C \subset \{0^n10^m | n, m \in \omega\}$.
   (b) For every $n \in \omega$, C contains at most one word of the form 0^n10^m.
2. The element a belongs to $B(C)$.
3. The element b possesses the following properties:
   (a) If $a = 0^n10^iz$ and $z \neq \lambda$, then $b = pred(a)$.
   (b) If $a = 0^n10^i$ and $x \notin C$, then $b = r_0(a)$.
   (c) If $a = 0^n10^m$ and $x \in C$, then $b = 0^n1$.

As already noted, properties $1(a)$, $1(b)$ and 2 can be defined in the monadic second order logic of ω-successors. It is also not hard to see that properties $3(a)$, $3(b)$ and $3(c)$ can also be expressed in this logic. Hence we can define the desired formula $F(x, y, Z)$.

Exercise 6.8.5 *Write down the formula $F(x, y, Z)$ whose existence is claimed above.*

Lemma 6.8.6 *For any unary algebra (A, f) which is a sum of enveloping algebras there exists a C such that the algebra $(Dom(f_C), f_C)$ is isomorphic to (A, f).*

Proof. From the definition of the formula $F(x, y, Z)$ it is not hard to see that there exists $C \subset \mathcal{T}_\omega$ such that the algebra $(Dom(f_C), f_C)$ is isomorphic to (A, f). □

Define the following formula $Al(U, Z)$ using the formula $F(x, y, Z)$:

$$\forall x \forall y (F(x, y, Z) \rightarrow (x \in U \rightarrow y \in U)).$$

Here is an interesting lemma about the formula $Al(U, Z)$.

Lemma 6.8.7

1. *For all subsets U, C of $\mathcal{T}_\omega$, $Al(U, C)$ is true in $\mathcal{T}_\omega$ if and only if U is closed with respect to the unary operation f_C, and hence (U, f_C) is a subalgebra of $(Dom(f_C), f_C)$.*

2. *For any unary algebra (A, f) there exists $U, C \subseteq T_\omega$ such that (U, f_C) is a subalgebra of the unary algebra $(Dom(f_C), f_C)$ and (U, f_C) is isomorphic to (A, f).*

Proof. The proof of Part (1) follows directly from the definitions of the formula $Al(U, Z)$, formula $F(x, y, Z)$, and the unary algebra $(Dom(f_C), f_C)$. Part (2) follows from Lemma 6.8.6 and the fact that any unary algebra can be embedded into a sum of enveloping unary algebras. This proves the lemma.

Let Φ be a formula of the monadic second order logic of unary algebras. We transform Φ into the formula $\Phi^{(t)}$ by induction as follows:

Basic Step. Atomic formulas $f(x) = y$ and $x \in X$ are transformed into $F(x, y, Z)$ and $x \in X \;\&\; X \subset U$, respectively.

Induction Step. If Φ is of the form $\Phi_1 \tau \Phi_2$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1$, then we set $\Phi^{(t)}$ to be $\Phi_1^{(t)} \tau \Phi_2^{(t)}$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1^{(t)}$, respectively. If Φ is any of the formulas

$$\forall x \Phi_1(x), \quad \forall X \Phi_1(X)$$

then $\Phi^{(t)}$ is

$$\forall x(x \in U \rightarrow \Phi_1^{(t)}(x)), \quad \forall X(X \subset U \rightarrow \Phi_1^{(t)}(X)).$$

Similarly, if Φ is any of the formulas

$$\exists x \Phi_1(x), \quad \exists X \Phi_1(X),$$

then we replace Φ with

$$\exists x(x \in U \;\&\; \Phi_1^{(t)}(x)), \quad \exists X(X \subset U \;\&\; \Phi_1^{(t)}(X)),$$

respectively.

The next lemma basically states that a sentence Φ of the monadic second order logic of unary algebras is true in all countable unary algebras if and only if the relativization of Φ to all sets C and subsets C_1 of C that are subalgebras of $(Dom(f_C), f_C)$ is true. Here is the lemma.

Lemma 6.8.8 *For every sentence Φ of the monadic order logic of unary algebras, Φ is true in all countable unary algebras if and only if the formula*

$$\forall U \forall Z(Al(U, Z) \rightarrow \Phi^{(t)})$$

belongs to $S\omega S$.

Proof. The proof follows immediately from the definitions of the formulas $F(x, y, Z)$, $Al(U, Z)$ and the transformation from Φ into $\Phi^{(t)}$. We leave the details of the proof to the reader. □

Exercise 6.8.6 *Finish the proof of the last lemma in detail.*

Thus, the lemmas above give us the proof of the theorem. □

6.9 Applications to Cantor's Discontinuum

In this section we give other applications of the decidability of $S2S$. We introduce and study objects related to the structure known as Cantor's discontinuum. Cantor's discontinuum is one of the fundamental structures often used in many areas of mathematics and computer science (analysis, topology, geometry, Boolean algebras, logic, game theory, fractals, set theory, etc.). This section begins with an excursion into Cantor's discontinuum. Then, in the next subsections, we will prove several decidability results about theories of structures that can be derived from Cantor's discontinuum.

6.9.1 A Brief Excursion to Cantor's Discontinuum. We begin this section with a known construction that produces a set called Cantor's discontinuum. Then we will show that the set produced can be identified with the set of all paths through the binary tree.

Let us take the interval $[0, 1]$, the set of all real numbers between 0 and 1 including the endpoints. We construct Cantor's discontinuum by stages. At each stage t we define the set C_t which will be a subset of $[0, 1]$. Then Cantor's discontinuum will be the set of all reals that belong to each C_t, $t \in \omega$. Here is the construction:

Stage 0. We set $C_0 = [0, 1]$.

Stage 1. Take the open interval $(\frac{1}{3}, \frac{2}{3})$, that is the set of all reals between $\frac{1}{3}$ and $\frac{2}{3}$ not including the endpoints. Then C_1 is the set of all reals in C_0 which do not belong to the open interval $(\frac{1}{3}, \frac{2}{3})$. Thus, $C_1 = C_0 \setminus (\frac{1}{3}, \frac{2}{3})$. Clearly, $C_1 \subset C_0$.

Stage 2. Consider C_1 which is the union of the two closed intervals $[0, \frac{1}{3}]$ and $[\frac{2}{3}, 1]$. Take the middle third of each of these intervals, that is take the open intervals $(\frac{1}{3^2}, \frac{2}{3^2})$ and $(\frac{7}{3^2}, \frac{8}{3^2})$ (without endpoints). Then C_2 is the set of all reals in C_1 that do not belong to $(\frac{1}{3^2}, \frac{2}{3^2}) \bigcup (\frac{7}{3^2}, \frac{8}{3^2})$. Clearly, $C_2 \subset C_1 \subset C_0$.

Stage $t + 1$. We assume, by induction, that C_t has been constructed and $C_t \subset C_{t-1}$. Also the induction hypothesis tells us that C_t is the union of certain closed intervals, that is,

$$C_t = \left[0, \frac{1}{3^{t-1}}\right] \cup \left[\frac{2}{3^{t-1}}, \frac{3}{3^{t-1}}\right] \cup \cdots \cup \left[\frac{3^{t-1} - 1}{3^{t-1}}, 1\right].$$

Thus, C_t is a disjoint union of 2^t closed intervals. Let $I_1, \ldots, I_k$ be all the intervals participating in the union. So $k = 2^t$. Each I_m is of the form $[\frac{x}{3^{t-1}}, \frac{x+1}{3^{t-1}}]$. Let J_m be the middle third of the interval I_m, that is, $J_m = (\frac{3x+1}{3^t}, \frac{3x+2}{3^t})$. Then, set

$$C_{t+1} = C_t \setminus (J_1 \cup J_2 \cup \cdots \cup J_k).$$

Clearly, $C_{t+1} \subset C_t$, and C_{t+1} is a union 2^{t+1} closed intervals. This ends this stage of the construction.

Now we define the set C as the intersection of all C_ts constructed:

$$C = \bigcap_{t\in\omega} C_t.$$

Now our goal is to present some of the basic properties of the set C. We note that the set C is not empty since the real numbers $\frac{i}{3^t}$, $i = 0, \ldots, 3^t$ belongs to C_t for all $t \in \omega$. Now we will show that reals in C can be identified with paths through the binary tree $\mathcal{T}$ in a certain precise sense. To do this we recast the construction of the set C.

Let us consider the first three stages of the construction of C. At *stage* 0 we have one closed interval, denoted by C_0. At the next stage, *stage* 1, the set C_1 is split into two disjoint intervals I_0 and I_1 so that $I_0 = [0, \frac{1}{3}]$ and $I_1 = [\frac{2}{3}, 1]$. At the next stage, the set C_2 is split into four disjoint intervals, let us denote them by $I_{00}, I_{01}, I_{10}, I_{11}$ so that

$$I_{00} = \left[0, \frac{1}{3^2}\right], \quad I_{01} = \left[\frac{2}{3^2}, \frac{3}{3^2}\right], \quad I_{10} = \left[\frac{6}{3^2}, \frac{7}{3^2}\right], \quad \text{and } I_{11} = \left[\frac{8}{3^2}, 1\right].$$

Note that I_{00} and I_{01} are subsets of I_0, and I_{10} and I_{11} are subsets of I_1.

In general, at *stage* t of the construction of C, the set C_t is a union of 2^t closed intervals I_u so that the following properties hold:

1. $u \in \{0, 1\}^\star$.
2. The length of u is t.
3. If $u \neq v$ and $|u| = |v| = t$, then $I_u \bigcap I_v = \emptyset$.
4. For all $u \in \{0, 1\}^\star$, if $|u| = t - 1$, then $I_{u0} \bigcup I_{u1} \subset I_u$.

Thus, we have the following lemma whose proof is left to the reader.

Lemma 6.9.1 *The mapping $u \to I_u$ has the following properties:*

1. *If $|u| = t$, then I_u is one of the closed intervals that participates in the union defining the set C_t. Moreover, the length of the interval I_u is $3^{-|u|}$.*
2. *If $u \leq v$, then I_v is a proper subset of I_u.*
3. *If u and v are not prefixes of each other, then $I_u \bigcap I_v = \emptyset$.* □

Exercise 6.9.1 *Prove the lemma.*

Now let us take an infinite string $\alpha = \alpha(0)\,\alpha(1)\,\alpha(2)\ldots$ so that $\alpha \in \{0, 1\}^\omega$. Consider the sequence of closed intervals:

$$I_{\alpha(0)} \supset I_{\alpha(0)\alpha(1)} \supset I_{\alpha(0)\alpha(1)\alpha(2)} \supset I_{\alpha(0)\alpha(1)\alpha(2)\alpha(3)} \supset \cdots.$$

Since the length of the interval $I_{\alpha(0,n)}$ converges to 0, where $\alpha(0, n) = \alpha(0)\ldots\alpha(n-1)$, the intersection of all these intervals is not empty and consists of exactly one real. Denote this real by r_α. Thus,

$$\bigcap_{n\in\omega} I_{\alpha(0,n)} = \{r_\alpha\}.$$

We note that $r_\alpha \in C$ because r_α belongs to every C_t.

Exercise 6.9.2 *Prove that for all α, $\beta \in \{0, 1\}^\omega$, if $\alpha \neq \beta$, then $r_\alpha \neq r_\beta$.*

Now let us take $r \in C$. Then $r \in C_t$ for all $t \in \omega$. Now for every $t \in \omega$, let u_t be such that $r \in I_{u_t}$ and the length of u_t is t. Note that such u_t exists and is unique for every t. Moreover, u_t is a proper prefix of u_{t+1}. Hence we can consider the sequence $\alpha \in \{0, 1\}^\omega$ such that $\alpha(0, t) = u_t$ for all t. Hence $r = r_\alpha$. Thus,

$$C = \{r_\alpha \mid \alpha \in \{0, 1\}^\omega\},$$

and we conclude that we can identify the set C with the set of all infinite sequences of the alphabet $\{0, 1\}^\omega$. Now we are ready to give the following definition.

Definition 6.9.1 Cantor's discontinuum *is the set of all infinite sequences from $\{0, 1\}^\omega$. We denote this set by CD.*

Clearly, there exists a one-to-one correspondence between CD and all paths of the tree $\mathcal{T}$. Indeed, let

$$a_0 a_1 a_2 \ldots$$

be an element of CD, where each a_i is a member of $\{0, 1\}$. Then we assign to this element the set

$$\{\lambda, r_{a_0}(\lambda),\ r_{a_0}(r_{a_1}(\lambda)),\ r_{a_0}(r_{a_1}(r_{a_2}(\lambda))), \ldots\},$$

where $r_0 = L$ and $r_1 = R$. It is obvious that this set is a path of $\mathcal{T}$. Similarly, to any path

$$\{\lambda, r_{a_0}(\lambda),\ r_{a_0}(r_{a_1}(\lambda)),\ r_{a_0}(r_{a_1}(r_{a_2}(\lambda))), \ldots\},$$

we assign the element

$$a_0 a_1 a_2 \ldots$$

of the CD. This shows that there exists a one-to-one correspondence between sets of paths in $\mathcal{T}_2$ and subsets of CD. Therefore, from now on, we identify Cantor's discontinuum with the set of all paths through the binary tree $\mathcal{T}$.

6.9.2 Cantor's Discontinuum as a Topological Space. Certain subsets of CD are of particular interest. These are, for example, subsets known as **open subsets** of CD. One of the basic reasons to be interested in CD and its open subsets is that they allow one to introduce the notions of limit, continuity, continuous functions, and metrics in Cantor's discontinuum. The other reason to be interested in CD is that some known structures of mathematics, e.g., boolean algebras, the real numbers and many others, can be represented in CD in one or another way. The topics concerning limits, continuity, continuous functions and metrics in Cantor's discontinuum are beyond the scope of this book. Therefore, we will mainly deal with the decidability of the theories of structures that can be expressed in terms of CD and its subsets.

Let β be an element of CD. Assume that

$$\beta = a_0 a_1 a_2 a_3 \ldots.$$

We can consider the following sequence of subsets of CD:

$$\{a_0\alpha \mid \alpha \in CD\},\ \{a_0a_1\alpha \mid \alpha \in CD\},\ \{a_0a_1a_2\alpha \mid \alpha \in CD\},\ldots.$$

Each of the sets above is called an **open basic set**. Clearly, each of the above open basic sets contains β. So we give a formal definition of a basic open set.

Definition 6.9.2 *Let $x \in \{0,1\}^\star$. Then the set*

$$U_x = \{x\alpha \mid \alpha \in CD\}$$

is called a **basic open set**.

Thus for example, U_0 and U_1 are two basic open sets. U_0 contains all α in CD that begin with 0; U_1 contains all α in CD that begin with 1.

Definition 6.9.3 *A subset $B \subset CD$ is* **open** *if either $B = \emptyset$ or for every element $\alpha \in B$ there exists a basic open set U such that $\alpha \in U$ and $U \subset B$.*

We give some examples of open sets in CD.

Example 6.9.1 *CD itself is an open set.*

Example 6.9.2 *$B = U_{00} \bigcup U_{11}$ is an open set. Indeed if $\alpha \in B$, then α begins with either* 00 *or* 11. *In the first case $\alpha \in U_{00} \subset B$; in the second case $\alpha \in U_{11} \subset B$.*

It turns out that one can give a very nice characterization of open sets of CD. To do this we first need a definition.

Definition 6.9.4 *Let $X \subset \{0,1\}^\star$. Then $U_X = \bigcup_{x\in X} U_x$.*

Here now is the characterization of open sets in CD.

Theorem 6.9.1 *Let B be a nonempty subset of CD. Then the following are equivalent:*

1. *B is an open set.*
2. *B is a union of basic open sets.*
3. *$B = U_X$ for some $X \subset \{0,1\}^\star$.*

Proof. We prove the direction from (1) to (2). Let B be an open set. Then for every element $\alpha \in B$ there exists a basic open set $U(\alpha)$ such that $\alpha \in U(\alpha)$ and $U(\alpha) \subset B$. Clearly, $B = \bigcup_{\alpha\in B} U(\alpha)$. Hence (2) is proved.

We now prove the direction from (2) to (3). Let B be a union of basic open sets. Take an element $\alpha \in B$. Then there exists a basic open set U_x such that $U_x \subset B$ and $\alpha \in B$. Let $\lambda = x_0 \le x_1 \le x_2 \le \cdots \le x_n$ be all prefixes of x. Among these prefixes take the x_i such that $U_{x_i} \subset B$ but $U_{x_{i-1}} \not\subset B$. Denote this x_i by $x(\alpha)$. Now set

$$X = \{x(\alpha) | \alpha \in B\}.$$

We claim that $U_X = B$. Indeed if β is in U_X, then $\beta \in U_{x(\alpha)}$ for some $\alpha \in B$. Since $U_{x(\alpha)} \subset B$, we conclude that $\beta \in B$. If $\alpha \in B$, then clearly $\alpha \in U_{x(\alpha)} \subset U_X$. This proves the direction from (2) to (3).

We now prove the direction from (3) to (1). So let $B = U_X$. Then

$$B = \bigcup_{x\in X} U_x.$$

Take an $\alpha \in B$. Then there exists a $y \in X$ such that $\alpha \in U_y$. From the definition of U_X we see that $U_y \subset B$ and α is contained in the basic open set U_y. Thus, the theorem is proved.

Theorem 6.9.2

1. *The union of any collection of open sets is an open set.*
2. *The intersection of any finite number of open sets is an open set.*

Proof. We prove the first part of the theorem. Let B_i, $i \in I$, be a collection of open sets indexed by I. Let B be $\bigcup_{i\in I} B_i$. Take any $\alpha \in B$. Then there exists an i such that $\alpha \in B_i$. Since B_i is an open set, there exists a basic open set U_x such that $\alpha \in U_x$ and $U_x \subset B_i$. Hence $U_x \subset B$. Hence B is an open set.

We prove the second part of the theorem. Let B_1 and B_2 be open sets. Consider $B_1 \bigcap B_2$. Let $\alpha \in B_1 \bigcap B_2$. Then there exist two basic open sets $U_{x_1} \subset B_1$ and $U_{x_2} \subset B_2$ such that $\alpha \in U_{x_1}$ and $\alpha \in U_{x_2}$. Then it must be the case that either $U_{x_1} \subset U_{x_2}$ or $U_{x_2} \subset U_{x_1}$. Hence either U_{x_1} or U_{x_2} is a subset of $B_1 \bigcap B_2$. Hence the intersection of B_1 and B_2 is an open set. In order to show that the intersection of any finite number of open sets is an open set, one can use induction on the number of open sets. The theorem is proved.

Exercise 6.9.3 *Let B_i, $i \in I$, be a collection of open sets indexed by I. Let $X_i \subset \{0,1\}^*$ be such that $B_i = U_{X_i}$. Set $X = \bigcup_i X_i$. Prove that the equality $\bigcup_{i \in I} U_i = U_X$ holds.*

Exercise 6.9.4 *Let U_X and U_Y be open sets. Consider the set $X \bigcap Y$. Is it true that the equality $U_X \bigcap U_Y = U_{X \bigcap Y}$ holds?*

Another important notion concerning the subsets of CD is the notion of a closed set. Here is the definition.

Definition 6.9.5 *A set $B \subset CD$ is* **closed** *if $CD \setminus B$ is an open set.*

Thus, every closed set in CD is of the form $CD \setminus U_X$, for some subset X of $\{0,1\}^*$. We now formulate the theorem about closed sets that is dual to Theorem 6.9.2 about open sets. We leave the proof to the reader.

Theorem 6.9.3

1. *The intersection of any collection of closed sets is a closed set.*
2. *The union of a finite number of closed sets is a closed set.* □

Exercise 6.9.5 *Prove the theorem above.*

6.9.3 Expressing Subsets of *CD* in *S2S*. We wish to define subsets of CD in the monadic second order theory of two successors. The problem of expressing subsets of CD in this logic is the following. Each element of CD is a path on the binary tree. Hence the path is already a subset of the binary tree. Thus, subsets of CD are sets containing subsets of the binary tree. Thus, from this point of view, subsets of CD are third order objects of the tree $\mathcal{T}$ (elements of $\mathcal{T}$ are the first order objects, subsets of $\mathcal{T}$ are the second order objects). We know that the monadic second order logic of the binary tree does not include variables for third order objects. Hence, on its face, the logic is not powerful enough to talk about third order objects, e.g., sets of subsets. In order to overcome this problem we use an indirect way of coding subsets of CD into the monadic second order logic of the binary tree $\mathcal{T}$ with two successors.

As an example of such an indirect coding we show how we can define closed subsets of CD in the monadic second order theory of $\mathcal{T}$. Consider the formula

$$X \subset Y \;\&\; Path(X).$$

We denote this formula by $cl(X, Y)$. This formula states that X is a path and X is a subset of Y. Let A be a subset of $\mathcal{T}$. Then we can consider the set

$$\{\alpha \mid \alpha \text{ is a path on } \mathcal{T} \text{ and is a subset of } A\}.$$

In other words, this set consists of all paths α which make the formula $cl(\alpha, A)$ true in $\mathcal{T}$. Note that this set depends on A. Hence, the formula $cl(X, Y)$ defines the mapping f_{cl} from the set of all subset of $\mathcal{T}$ into the set of subsets of CD as follows. For all $A \subset \mathcal{T}$, let

$$f_{cl}(A) = \{\alpha | \mathcal{T} \models cl(\alpha, A)\}.$$

Thus, to every $A \subset \mathcal{T}$ the function f_{cl} assigns the set of all paths α that satisfy the formula

$$\alpha \subset A \;\&\; Path(\alpha).$$

Since each path α is identified with an element of CD, we see that the collection of all α that are subsets of A is a subset of CD. The next theorem gives us an interesting property about the formula $cl(X, Y)$ and the associated map f_{cl}. Briefly, the theorem states that f_{cl} ranges over all closed subsets of CD.

Theorem 6.9.4 *For every subset A of $\mathcal{T}$, the set $f_{cl}(A)$ is closed. Moreover, for every closed set $C \subset CD$, there is a subset $A \subset \mathcal{T}$ such that $f_{cl}(A) = C$.*

Proof. We prove the first part of the theorem. Let A be a subset of $\mathcal{T}$ and let α denote a path in $\mathcal{T}$. Consider the set $f_{cl}(A)$. Then $\alpha \in f_{cl}(A)$ if and only if every $y \in \alpha$ belongs to A. Hence $\alpha \notin f_{cl}(A)$ if and only if for some $y \in \mathcal{T}$ and $\beta \in \{0,1\}^\omega$ we have $\alpha = y\beta$ and $y \notin A$. Thus, consider the set $X = \mathcal{T} \setminus A$. Then, as we have already shown, the following equality holds:

$$CD \setminus f_{cl}(A) = U_X.$$

Note that U_X is a set of paths in $\mathcal{T}$, and hence a subset of CD. By Theorem 6.9.1, the set U_X is open and hence $f_{cl}(A)$ is closed.

Now we prove the second part of the theorem. Assume that $C \subset CD$ is a closed set. Let A be the set of all $x \in \mathcal{T}$ such that x belongs to some path $\alpha \in C$. In other words,

$$A = \bigcup_{\alpha \in C} \alpha.$$

Then, we claim that $C = f_{cl}(A)$. If $\alpha \in C$, then $\alpha \subset A$. Therefore, the formula $cl(A, \alpha)$ is true. Hence $\alpha \in f_{cl}(A)$. Assume now that $\alpha \in f_{cl}(A)$. We want to show that $\alpha \in C$. If $\alpha \notin C$, then, since the complement of C is open, there exists a $y \in \mathcal{T}$ such that $\alpha \in U_y \subset CD \setminus C$. Hence $y \notin A$. However, by assumption $\alpha \in f_{cl}(A)$ and therefore $cl(A, \alpha)$ is satisfied. In particular $\alpha \subset A$ and hence $y \in A$. This is a contradiction. We conclude that $\alpha \in C$. The theorem is proved.

Apart from open and closed subsets of CD, there are many other classes of subsets that have attracted the attention of mathematicians and computer scientists. For example, subsets known as *Borel sets* are well known. These sets have been studied in logic, set theory, game theory, and in some areas of computer science. Borel sets define a certain natural hierarchy on *complexity* of subsets of CD from a topological point of view. The most simple or accessible Borel sets which belong to the lowest level of the hierarchy are open sets and closed sets. Each next level of sets in the hierarchy is then defined by taking infinite countable unions, intersections and complements of those sets that belong to the lower level in the hierarchy. Here we will not discuss the Borel sets and their hierarchy as they are not in the scope of this book. However, we will consider Borel sets that are obtained by using countable unions of closed subsets of CD. Such sets are known as F_σ-sets. Here is a formal definition.

Definition 6.9.6 *A subset S is called an* F_σ**-set** *if it is a countable union of closed subsets of CD.*

It turns out that it is possible to express F_σ-sets in terms of the monadic second order logic of the structure $\mathcal{T}$ of two successors. The idea is similar to the one where we expressed closed subsets by means of the formula $cl(X, Y)$.

Let $Finite(X)$ be the formula, defined in Example 6.5.7, such that for all $A \subset T$, $F(A)$ is true if and only if A is a finite subset of $\mathcal{T}$. We now define the formula $F_\sigma(X, Y)$ as

$$Path(X) \ \& \ Finite(X \bigcap Y).$$

This formula states that X is a path and the intersection of X with Y is a finite set. Let A be a subset of $\mathcal{T}$. Then we can consider the set

$$\{\alpha \mid \alpha \text{ is a path on } \mathcal{T} \text{ and the set } \alpha \bigcap A \text{ is finite}\}.$$

In other words the above set contains all paths α which make the formula $F_\sigma(\alpha, A)$ true in $\mathcal{T}$. Hence, the formula $F_\sigma(X, Y)$ defines the mapping f_σ from the set of all subsets of $\mathcal{T}$ into the set of subsets of CD as follows. For all $A \subset \mathcal{T}$, let

$$f_\sigma(A) = \{\alpha \mid \mathcal{T} \models F_\sigma(\alpha, A)\}.$$

Thus, to every $A \subset \mathcal{T}$ the function f_σ assigns the set of all paths α that satisfy the formula

$$Finite(\alpha \bigcap A) \ \& \ Path(\alpha).$$

Since each path α is identified with an element of CD, we see that the collection of all α that have finite intersection with A is a subset of CD. The next theorem gives us an interesting property about the formula $F_\sigma(X, Y)$ and the associated map f_σ. Briefly, the theorem states that f_σ ranges over all F_σ-subsets of CD.

Theorem 6.9.5 *For every $A \subset \mathcal{T}$, the set $f_\sigma(A)$ is an F_σ-set. Moreover, for every F_σ-set $C \subset CD$, there exists a subset $A \subset \mathcal{T}$ such that $f_\sigma(A) = C$.*

Proof. Let us prove the first part of the theorem. Suppose that $\alpha \in f_\sigma(A)$. Then α is a path and the number of elements in $A \bigcap \alpha$ is finite, say n. For every number m consider the set

$$P_m = \{\beta \mid \beta \text{ is a path and } \beta \bigcap A \text{ has at most } m \text{ elements}\}.$$

In particular, $\alpha \in P_n$. It is not hard to see that $f_\sigma(A) = \bigcup_{n \in \omega} P_n$. We claim that each P_n is a closed set. Indeed, consider the set

$$X_n = \{x \in \mathcal{T} \mid x \text{ has more than } n \text{ prefixes belonging to } A\}.$$

Clearly, U_{X_n} is an open set. Moreover, the $CD \setminus U_{X_n} = P_n$ for all n. Hence each P_n is closed. Therefore, $f_\sigma(A)$ is an F_σ-set. This proves the first part of the theorem.

Now we prove the second part of the theorem. So assume that $C \subset CD$ is an F_σ-set. Then there exists a sequence $P_0, P_1, P_2, \ldots$ of closed sets such that

$$C = P_0 \bigcup P_1 \bigcup P_2 \bigcup \cdots.$$

We can assume that $P_0 \subseteq P_1 \subseteq P_2 \subseteq P_3 \subseteq \cdots \subseteq CD$ (see Theorem 6.9.3). Now let

$$A_n = \bigcup_{\alpha \in P_n} \alpha.$$

Note that $A_i \subseteq A_{i+1}$ for all $i \in \omega$. Moreover, from the proof of the previous theorem we conclude that the equality

$$f_{cl}(A_n) = P_n$$

holds for all $n \in \omega$.

Now we want to find a set $A \subset \mathcal{T}$ for which $f_\sigma(A) = C$. Take a path β not in C. Then the path β is not in P_n for every n. This implies that $A_n \bigcap \beta$ is a finite set for every n. Indeed, by the definition of A_n, if $x \in A_n$, then any prefix of x is in A_n. Therefore, if the set $A_n \bigcap \beta$ were an infinite set, then $\beta \subset A_n$ and therefore β would belong to P_n. This is a contradiction to the choice of β. Now, using that $\beta \notin C$, we define the sequence

$$x_0(\beta), x_1(\beta), x_2(\beta), \ldots$$

of elements in $\mathcal{T}$ by stages as follows.

Stage 0. $x_0(\beta)$ is the minimal element x with respect to the prefix ordering $\leq$ in $\mathcal{T}$ such that $x \in \beta$ and $x \notin A_0$.

Stage $s+1$. Suppose that $x_0(\beta), \ldots, x_s(\beta)$ have been defined. Then $x_{s+1}(\beta)$ is the minimal element x with respect to the prefix ordering $\leq$ in $\mathcal{T}$ such that $x \in \beta$, $x_s(\beta) < x$, and $x \notin A_{s+1}$.

Thus, we have defined the infinite sequence $x_0(\beta), x_1(\beta), x_2(\beta), \ldots$ of nodes of the tree $\mathcal{T}$. Note that for all $m \geq 1$ and $y > x_m(\beta)$ we have $y \notin A_m$. Also note that no such y could be of the form $x_m(\beta')$ for some $\beta' \neq \beta$ and $\beta' \notin C$. Now we define the set B as

$$B = \{x_s(\beta) \mid \beta \notin C, \ s \in \omega\}.$$

We now claim that the equality $f_\sigma(B) = C$ holds. To prove this suppose that $\beta \notin C$. Then $x_s(\beta) \bigcap B \neq \emptyset$ for all s. Hence the intersection $\beta \bigcap B$ has infinitely many elements. Therefore, $\beta \notin f_\sigma(B)$. We conclude that $f_\sigma(B) \subset C$.

Assume that $\alpha \in C$. Then $\alpha \subset A_n$ for some n. Therefore, since $A_m \subset A_{m+1}$ for all m, $\alpha \subset A_{n+k}$ for all $k \in \omega$. Hence for a β that does not belong to C, if $x_m(\beta) \in \alpha$, then $0 \leq m < n$. Now we claim that the set $\alpha \bigcap B$ has at most n elements. This will establish that $\alpha \in f_\sigma(B)$. So assume that $\beta_0, \ldots, \beta_n$ are such that all $\beta_0, \ldots, \beta_n$ are not in C, and $x_{m_0}(\beta_0), \ldots, x_{m_n}(\beta_n)$ are pairwise distinct elements that belong to α. Then, as we noted above, each m_i must be less than n. Hence for some distinct $i, j \leq n$, we should have $m_i = m_j$. Let $m = m_i$. This implies that $x_m(\beta_i) \in \alpha$ and $x_m(\beta_j) \in \alpha$. Hence the nodes $x_m(\beta_i)$ and $x_m(\beta_j)$ are comparable with respect to the prefix order $\leq$. Say $x_m(\beta_i) < x_m(\beta_j)$. But, as noted above, this cannot happen. The theorem is thus proved.

6.9.4 Decidability Results. In this subsection we prove several decidability results about some structures and formal languages that can be derived from Cantor's discontinuum. One of the natural structures that can be derived from CD is the structure

$$(CD, \preceq),$$

where for all $\alpha, \beta \in CD$, we have $\alpha \preceq \beta$ if and only if $\alpha = \beta$ or there exists w, a finite prefix of both α and β, such that $w0 \in \alpha$ and $w1 \in \beta$. Intuitively, this is the natural left to right ordering of all paths through the binary tree. Clearly, $(CD, \preceq)$ is a linearly ordered set. We now define the language L appropriate to $(CD, \preceq)$. The language is defined in the usual way but with some modifications. The language contains **individual variables** $x, y, z, \ldots$, that are intended to run over elements of CD, the symbol $\preceq$ representing the order on CD, logical connectives $\&, \bigvee, \neg, \rightarrow$, and set variables of two types. The first type of set variables are $C_1, C_2, C_3, \ldots$ and range over closed subsets of CD; the second type of set variables are $D_1, D_2, D_3, \ldots$ and range over F_σ-subsets of CD. The language contains quantifiers $\exists, \forall$ that can be applied to the individual as well as to the set variables of both types. The language also has the symbol $\in$ for representing membership. The formulas and sentences of this language L are defined in the natural way. We leave the definition of formulas to the reader.

Definition 6.9.7 *Denote the set of all sentences of the language L true in $(CD, \preceq)$ by $Th(CD)$. Call it* **the theory of Cantor's discontinuum.**

Here is our first decidability result.

Theorem 6.9.6 *The theory $Th(CD)$ of Cantor's discontinuum is decidable.*

Proof. The idea of the proof of the theorem is quite simple. We need to transform formulas of the language L into the formulas of the monadic second order theory of two successors. The transformation of a formula Φ to a formula $\Phi^{(t)}$ should naturally preserve their satisfaction in $(CD, \preceq)$ and $(\mathcal{T}, L, R)$, respectively. We recall from the previous section that we have the formula $cl(X, Y)$ which is $X \subset Y \,\&\, Path(X)$. This defines all the closed sets of CD. We also have the formula $F_\sigma(X, Y)$ which is $Finite(X \bigcap Y) \,\&\, Path(X)$. This defines all the F_σ-subsets of CD. We now transform Φ into $\Phi^{(t)}$ by induction on the complexity of Φ. If Φ is of the form $x_i \leq x_j$, then $\Phi^{(t)}$ is

$$(Path(B_i) \,\&\, Path(B_j)) \vee (\exists x(L(x) \in B_i \,\& R(x) \in B_j)).$$

If Φ is of the form $x_i \in C_j$ or $x_i \in D_j$, then $\Phi^{(t)}$ is

$$Path(B_i) \,\&\, cl(B_i, C_j) \quad \text{or} \quad Path(B_i) \,\&\, F_\sigma(B_i, C_j),$$

respectively. If Φ is of the form $\Phi_1 \tau \Phi_2$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1$, then we set $\Phi^{(t)}$ to be $\Phi_1^{(t)} \tau \Phi_2^{(t)}$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1^{(t)}$, respectively.

If Φ is any of the formulas

$$\forall x_i \Phi_1(x_i), \quad \forall C_i \Phi_1(C_i), \quad \forall D_i \Phi_1(D_i),$$

then $\Phi^{(t)}$ is

$$\forall B_i(Path(B_i) \rightarrow \Phi_1^{(t)}(B_i)), \quad \forall C_i(\Phi_1^{(t)}(C_i)), \quad \forall D_i(\Phi_1^{(t)}(D_i)).$$

Similarly, if Φ is any of the formulas

$$\exists x_i \Phi_1(x_i), \quad \exists C_i \Phi_1(C_i), \quad \exists D_i \Phi_1(D_i),$$

then we replace Φ with

$$\exists B_i(Path(B_i) \,\&\, \Phi_1^{(t)}(B_i)), \quad \exists C_i(\Phi_1^{(t)}(C_i)), \quad \exists D_i(\Phi_1^{(t)}(D_i)),$$

respectively. Now the reader can check that for all sentences Φ, we have $\Phi \in Th(CD)$ if and only if $\Phi^{(t)} \in S2S$. The theorem is proved.

We now consider another natural structure that can be obtained from Cantor's discontinuum. Consider the set M_σ of all F_σ-sets. Let D_1, D_2 be elements of M_σ. Hence D_1 and D_2 are of the form:

$$D_1 = P_1^1 \cup P_2^1 \cup P_3^1 \cup \cdots \quad \text{and} \quad D_2 = P_1^2 \cup P_2^2 \cup P_3^2 \cup \cdots,$$

where each P_i^1, P_i^2 is a closed set. Then

$$D_1 \bigcup D_2 = P_1^1 \cup P_1^2 \cup P_2^1 \cup P_2^2 \cup \cdots \quad \text{and} \quad D_1 \bigcap D_2 = \bigcup_{i,j \geq 1} (P_i^1 \cap P_j^2).$$

Hence the set M_σ of all F_σ-sets is closed under the operations of union and intersection. We also know that the set M_c that consists of all closed sets is closed under the operations of finite union and intersection (see Theorem 6.9.3). Therefore, it is quite natural to consider the structure

$$\mathcal{A} = \left(M_\sigma, \bigcup, \bigcap, M_c\right).$$

Thus, the domain of $\mathcal{A}$ consists of all F_σ-sets. The type of the structure consists of two binary operations $\bigcup$ and $\bigcap$, and one unary relation M_c. Now we can consider the first order theory $Th_1(\mathcal{A})$ of this structure, that is the set of all sentences of the first order logic that are true in the structure $\mathcal{A}$. It turns out that the following result can be easily derived from the previous theorem.

Theorem 6.9.7 *Consider the structure* $\mathcal{A} = (M_\sigma, \bigcup, \bigcap, M_c)$. *The first order theory* $Th_1(\mathcal{A})$ *of this structure is decidable.*

Proof. Assume that $x_0, x_1, \ldots$ are variables of the first order logic of the structure $\mathcal{A}$. We associate the variables x_i with the variables D_i of the language L of the structure $(CD, \preceq)$. Now the union and intersection operations of F_σ-sets of CD are definable in the language L. Similarly, the union and intersection operations of closed sets are definable in the language L. Hence we can replace the atomic formulas $x_i \bigcup x_j = x_k$ and $x_i \bigcap x_j = x_k$ with the formulas $D_i \bigcup D_j = D_k$ and $D_i \bigcap D_j = D_k$ of the language L, respectively. We can also replace the quantifiers $\exists x_i$ and $\forall x_i$ with $\exists D_i$ and $\forall D_i$, respectively. Also, if a sentence of the first order theory of $\mathcal{A}$ contains the formula $M_c(x_i)$ so that x_i is quantified with $\exists x_i$, then this is replaced by $\exists C_i$. For example, the sentence $\forall x_i \exists x_j (x_i = x_j \& M_c(x_i))$ is replaced with $\forall D_i \exists C_j (D_i = C_j)$. Hence we can transform any sentence Φ of the first order logic of the structure $\mathcal{A}$ into a sentence $\Phi^{(t)}$ of the language L. Moreover, $\Phi \in Th_1(\mathcal{A})$ if and only if $\Phi^{(t)} \in Th(CD)$. This proves the theorem. □

Exercise 6.9.6 *Give a formal definition of the transformation of* Φ *into* $\Phi^{(t)}$ *used in the proof of the theorem.*

The next result concerns the interval [0, 1] of real numbers, the natural order $\leq$ on this interval, and the topology on this interval. The topology of this interval is defined by closed subsets of [0, 1] and F_σ-subsets of [0, 1]. For completeness we recall the following definitions. A subset $U \subset [0, 1]$ is **open** if for any $x \in U$ there exists a real number $\epsilon > 0$ such that $(x - \epsilon, x + \epsilon) \subset U$. A set $U \subseteq [0, 1]$ is **closed** if $[0, 1] \setminus U$ is open. A countable union of closed subsets of [0, 1] is an F_σ-set. Now consider the language L defined for $(CD, \preceq)$. The language L can be considered as a language of the structure [0, 1] where the binary relation of L is interpreted as the natural order $\leq$ on reals, variables $C_0, C_1, \ldots$ are interpreted as closed subsets of [0, 1], and the variables $D_0, D_1, \ldots$ are interpreted as F_σ-subsets of [0, 1]. Our goal is to show that the theory $Th([0, 1])$ of the structure $([0, 1], \leq)$ in the language L is decidable. It is noteworthy that the structure $([0, 1], \leq)$ together with the topology of its closed sets as well as F_σ-sets is among one of the fundamental structures that arise in mathematics, especially in analysis and topology. It turns out that we can prove the decidability of $Th([0, 1])$ by again using Cantors' discontinuum.

Consider CD. Let $\alpha = \alpha(0)\alpha(1)\ldots$ be in CD. With α we can associate the real number $r^{(\alpha)}$ defined as follows:

$$r^{(\alpha)} = \frac{\alpha(0)}{2} + \frac{\alpha(1)}{2^2} + \cdots + \frac{\alpha(n)}{2^{n+1}} + \cdots.$$

Note that the mapping $\alpha \to r^{(\alpha)}$ is onto, since for every $r \in [0, 1]$ there exists an α such that $r = r^{(\alpha)}$. However, this mapping is not one-to-one because for some r there exist exactly two distinct α and β such that $r = r^{(\alpha)} = r^{\beta)}$. Indeed take $u \in \mathcal{T}$ and consider $\alpha = u1000000\ldots$ and $\beta = u0111111\ldots$. Then $r^{(\alpha)} = r^{(\beta)}$. This suggests the following. Say that α and β in CD are $\sim$-equivalent if there exists a $u \in \mathcal{T}$ such that $\alpha = u1000000\ldots$ and $\beta = u0111111\ldots$. The relation $\sim$ is indeed an equivalence relation. Now we can consider the set $CD^\sim$ consisting of all $\sim$-equivalence classes. Note that the mapping $\alpha \to r^{(\alpha)}$ induces a one-to-one function $\alpha_\sim \to [0, 1]$ from $CD^\sim$ onto [0, 1], where $\alpha_\sim$ is the $\sim$-class that contains α. Also note that the $\preceq$ relation on CD induces a linear order, also denoted by $\preceq$, on the set $CD^\sim$. The reader can now prove the following lemma.

Lemma 6.9.2 *The mapping* $\alpha_\sim \to r^{(\alpha)}$ *from* $CD^\sim$ *onto* [0, 1] *satisfies the following properties:*

1. *For all* $\alpha, \beta \in CD$, *the real numbers* $r^{(\alpha)}$ *and* $r^{(\beta)}$ *are equal if and only if* α *is* $\sim$*-equivalent to* β.

2. *For all* $\alpha, \beta \in CD$, $\alpha_\sim \preceq \beta_\sim$ *if and only if* $r^{(\alpha)} \leq r^{(\beta)}$.

Moreover, the mapping $\alpha \to r^{(\alpha)}$ *from CD onto* [0, 1] *satisfies the following properties:*

1. *For all* $C \subset CD$, C *is closed if and only if its image under the mapping is closed.*

2. *For all* $D \subset CD$, C *is an* F_σ*-set if and only if its image under the mapping is an* F_σ*-set.* □

Exercise 6.9.7 *Prove the lemma above.*

Following is the theorem stating that the theory $Th([0, 1])$ of the topological structure $([0, 1], \leq)$ in the language L is decidable.

Theorem 6.9.8 *The theory* $Th([0, 1])$ *is decidable.*

Proof. In the proof we use the ideas of the proof of Theorem 6.9.6. First of all we note that the equivalence relation $\sim$ on the tree $\mathcal{T}$ is definable in $S2S$. By induction on the complexity of formulas, we transform formulas of the language L into the formulas of the monadic second order theory of two successors. If Φ is of the form $x_i \leq x_j$, then $\Phi^{(t)}$ is

$$(Path(B_i)\ \&\ Path(B_j))$$
$$\&\ \exists B_s \exists B_k(\exists x(L(x) \in B_s\ \& R(x) \in B_k\ \&\ B_i \sim B_s\ \&\ B_j \sim B_k)).$$

If Φ is of the form $x_i = x_j$, then the formula $\Phi^{(t)}$ is $(Path(B_i)\ \&\ Path(B_j)\ \&\ B_i \sim B_j)$. If the formula Φ is of the form $x_i \in C_j$ or $x_i \in D_j$, then the formula $\Phi^{(t)}$ is $(Path(B_i)\ \&\ \exists B_k(B_k \sim B_i\ \&\ cl(B_k, C_j))$ or $(Path(B_i)\ \&\ \exists B_k(B_i \sim B_k\ \&\ F_\sigma(B_k, C_j))$, respectively. If Φ is of the form $\Phi_1 \tau \Phi_2$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1$, then we set $\Phi^{(t)}$ to be $\Phi_1^{(t)} \tau \Phi_2^{(t)}$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1^{(t)}$, respectively. Now by using the induction on the complexity of formulas, we continue as follows. If the formula Φ is any of the formulas $\forall x_i \Phi_1(x_i)$, $\forall C_i \Phi_1(C_i), \forall D_i \Phi_1(D_i)$, then $\Phi^{(t)}$ is $\forall B_i(\exists B_j(B_i \sim B_j\ \&\ Path(B_j)\ \&\ \Phi_1^{(t)}(B_j))$, $\forall C_i(\Phi_1^{(t)}(C_i)), \forall D_i(\Phi_1^{(t)}(D_i))$, respectively. Similarly, if Φ is any of the formulas $\exists x_i \Phi_1(x_i), \exists C_i \Phi_1(C_i), \exists D_i \Phi_1(D_i)$, then $\Phi^{(t)}$ is $\exists B_i \exists B_j(B_i \sim B_j\ \&\ Path(B_j)\ \&\ \Phi_1^{(t)}(B_j)), \exists C_i(\Phi_1^{(t)}(C_i)), \exists D_i(\Phi_1^{(t)}(D_i))$, respectively. Now the reader can check that for all sentences Φ, we have $\Phi \in Th([0, 1])$ if and only if $\Phi^{(t)} \in S2S$. The theorem is proved. □

Exercise 6.9.8 *Prove the theorem above in detail.*

6.10 Application to Boolean Algebras

In this final section of the chapter we show that a certain formal theory of the class of all Boolean algebras is decidable. The proof follows the ideas of the proofs from the previous sections. We first obtain certain fundamental algebraic facts about Boolean algebras. Then using the algebraic facts we obtain decidability results by transforming statements about Boolean algebras to formulas of the monadic second order theory of two successors.

6.10.1 A Brief Excursion into Boolean Algebras. In this section we study structures called Boolean algebras. The results of this section will mostly be about *countable* Boolean algebras though the results can be generalized to uncountable Boolean algebras as well. Boolean algebras are fundamental systems that arise in many areas of mathematics. In general Boolean algebras can be thought as systems (or collections) of sets that are closed under the operations of union, intersection, and complementation. As we have seen, the classes of FA recognizable languages, Büchi recognizable languages, and Rabin recognizable languages are closed under these operations. In this part of this section we study some of the basic properties of these systems from the algebraic point of view. Here is a definition of Boolean algebras.

Definition 6.10.1 *A* **Boolean algebra** *is a structure*

$$\mathcal{B} = (B, \vee, \wedge, \tilde{}, \mathbf{0}, \mathbf{1}),$$

where $\vee$, $\wedge$ are binary operations, $\tilde{}$ is a unary operation, and $\mathbf{0}$, $\mathbf{1}$ are constants, such that for all $a, b, c \in B$ the following properties hold:

1. $a \vee b = b \vee a$, $a \wedge b = b \wedge a$ *(commutativity),*
2. $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ *(associativity),*
3. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *(distributivity),*
4. $\widetilde{a \vee b} = \tilde{a} \wedge \tilde{b}$, $\widetilde{a \wedge b} = \tilde{a} \vee \tilde{b}$ *(De Morgan's Law),*
5. $a \vee a = a$, $a \vee \mathbf{0} = a$, $a \vee \mathbf{1} = \mathbf{1}$,
6. $a \wedge a = a$, $a \wedge \mathbf{0} = \mathbf{0}$, $a \wedge \mathbf{1} = a$,
7. $\tilde{\tilde{a}} = a$,
8. $a \vee \tilde{a} = \mathbf{1}$, $a \wedge \tilde{a} = \mathbf{0}$.

Often the operations $\vee$, $\wedge$ and $\tilde{}$ are called the union, intersection, and complementation operations, respectively. We now give examples of Boolean algebras.

Example 6.10.1 *Let A be a set. Consider the set $P(A)$ of all subsets of A. Then $(P(A), \cup, \cap, \tilde{}, \emptyset, A)$ is a Boolean algebra.*

Example 6.10.2 *Consider the set* $\{0, 1\}$. *Set* $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1$, $1 \vee 1 = 0$, $0 \wedge 0 = 0$, $0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$, $\tilde{0} = 1$, $\tilde{1} = 0$. *This defines a Boolean algebra.*

Example 6.10.3 *Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be Boolean algebras. Consider the Cartesian product $B_1 \times B_2$. Define $\wedge$, $\vee$, and $\tilde{}$ operations on $B_1 \times B_2$ as follows: $(a, b) \wedge (c, d) = (a \wedge c, b \wedge d)$, $(a, b) \vee (c, d) = (a \vee c, b \vee d)$, $\widetilde{(a, b)} = (\tilde{a}, \tilde{b})$. Then we have the Boolean algebra denoted by $\mathcal{B}_1 \times \mathcal{B}_2$. Note that $\mathbf{0}$ and $\mathbf{1}$ in this Boolean algebra are $(\mathbf{0}, \mathbf{0})$ and $(\mathbf{1}, \mathbf{1})$, respectively.*

The first example is important since we will later show that we can operate with $\wedge$, $\vee$ and $\tilde{}$ operations as the intersection, union and the complementation operation on a certain collection of sets. We single out such Boolean algebras in the following definition.

Definition 6.10.2 **A Boolean algebra of subsets** *is a family X of subsets of a set A such that X contains $\emptyset$, A, and is closed under the set-theoretic operations of union, intersection, and complementation.*

Thus, if $\mathcal{B}$ is a Boolean algebra of subsets, then there exists a collection X of subsets of a set A such that $\mathcal{B} = (X, \bigcup, \bigcap, \setminus, \emptyset, A)$. For example, for any subset C of a set A, the set $\{C, A \setminus C, \emptyset, A\}$ is a Boolean algebra of subsets.

We now present several properties of Boolean algebras. Let $\mathcal{B}$ be a Boolean algebra. Then $\tilde{}$ is a unary operation on B such that for all $b_1 \neq b_2$, we have

$\tilde{b}_1 \neq \tilde{b}_2$, $\tilde{\mathbf{0}} = \mathbf{1}$ and $\tilde{\mathbf{1}} = \mathbf{0}$. Indeed, if $\tilde{b}_1 = \tilde{b}_2$, then by property (7) we have $b_1 = \tilde{\tilde{b}} = \tilde{\tilde{b}}_2 = b_2$. Hence $b_1 \neq b_2$ implies that $\tilde{b}_1 \neq \tilde{b}_2$. To show that $\tilde{\mathbf{1}} = \mathbf{0}$, we use the identities $a \wedge \mathbf{1} = a$ and $a \wedge \tilde{a} = \mathbf{0}$ that hold for all a. Indeed, set $a = \mathbf{1}$. Then $\tilde{\mathbf{1}} = \tilde{\mathbf{1}} \wedge \mathbf{1} = \mathbf{0}$. Similarly, we see that $\tilde{\mathbf{0}} = \mathbf{1}$. From now on, the element $\tilde{a}$ will be called the **complement** of a.

Let $\mathcal{B}$ be a Boolean algebra. Define the binary relation $\leq$ on the domain of $\mathcal{B}$ as follows. For $a, b \in B$, $a \leq b$ if $a \wedge b = a$. Here is the next lemma showing that $\leq$ is a partial ordering with several interesting properties.

Lemma 6.10.1 *The relation $\leq$ has the following properties:*

1. *$\leq$ is a partial ordering. Moreover, for all $b \in B$, we have $\mathbf{0} \leq b \leq \mathbf{1}$.*
2. *For all $a, b \in B$, $a \leq b$ if and only if $a \vee b = b$.*
3. *For all $a, b, x \in B$, if $x \leq a$ and $x \leq b$, then $x \leq a \wedge b$.*
4. *For all $a, b, x \in B$, if $x \geq a$ and $x \geq b$, then $x \geq a \vee b$.*

Proof. We prove (1). Clearly, $a \leq a$ for all a because $a \wedge a = a$ by the axioms of the Boolean algebras. Also, if $a \leq b$ and $b \leq a$, then $a \wedge b = a$ and $b \wedge a = b$. Since $\wedge$ is commutative, we have $a = b$. Assume that $a \leq b$ and $b \leq c$. Then $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$. Hence $a \leq c$. Therefore, $\leq$ is a partial ordering. The rest of Property (1) follows from the axioms of Boolean algebras.

We now prove (2). Assume that $a \vee b = b$. Then using the axioms for Boolean algebras we get the following: $a = a \vee (b \wedge \tilde{b}) = (a \vee b) \wedge (a \vee \tilde{b}) = b \wedge (a \vee \tilde{b}) = (b \wedge a) \vee (b \wedge \tilde{b}) = b \wedge a$. Hence $a \leq b$. Similarly, one can show that if $a \wedge b = a$ then $a \vee b = b$.

Now we prove property (3). Assume that $x \leq a$ and $x \leq b$. Then $x \wedge a = x$ and $x \wedge b = x$. Then from the axioms for Boolean algebras we obtain the following: $x \wedge (a \wedge b) = (x \wedge a) \wedge b = x \wedge b = x$. Hence $x \leq a \wedge b$. The proof of Property (4) is similar. The lemma is proved.

Exercise 6.10.1 *Prove that $a \leq b$ if and only if $\tilde{b} \leq \tilde{a}$.*

Definition 6.10.3 *Let $(B, \leq)$ be a partially ordered set. Then the* **inf** *of two elements $a, b \in B$, denoted by* $\mathbf{inf}(a, b)$, *is an element c such that for all $x \in B$ the condition $x \leq a$ and $x \leq b$ implies $x \leq c$. Similarly, the* **sup** *of two elements $a, b \in B$, denoted by* $\mathbf{sup}(a, b)$ *is an element c such that for all $x \in B$ the condition $x \geq a$ and $x \geq b$ implies $x \geq c$. The partially ordered set $(B, \leq)$ is a* **lattice** *if for all $a, b \in B$* $\mathbf{sup}(a, b)$ *and* $\mathbf{inf}(a, b)$ *exist.*

Thus for a Boolean algebra $\mathcal{B}$, as the lemma above shows, the partially ordered set $(B, \leq)$ is a lattice. Also, note that any linearly ordered set is a lattice. Of course, there are partially ordered sets which are not lattices.

Exercise 6.10.2 *A lattice $(B, \leq)$ is a* **Boolean lattice** *if the following properties hold:*

1. *There exist two elements* $\mathbf{0}$ *and* $\mathbf{1}$ *such that* $\mathbf{0} \leq b \leq \mathbf{1}$ *for all $b \in B$.*
2. *For all $a, b, c \in B$ we have* $\mathbf{sup}(a, \mathbf{inf}(b, c)) = \mathbf{inf}(\mathbf{sup}(a, b), \mathbf{sup}(a, c))$ *and* $\mathbf{inf}(a, \mathbf{sup}(b, c)) = \mathbf{sup}(\mathbf{inf}(a, b), \mathbf{inf}(a, c))$.
3. *For all $a \in B$ there exists some $b \in B$ such that* $\mathbf{sup}(a, b) = \mathbf{1}$ *and* $\mathbf{inf}(a, b) = \mathbf{0}$. *In this case a and b are* **complements** *of each other.*

Show the following:

1. *If $\mathcal{B}$ is a Boolean algebra, then $(B, \leq)$ is a Boolean lattice.*
2. *If $(B, \leq)$ is a Boolean lattice, then for every $a \in B$ there exists exactly one complement b of a. Denote the complement of a by $\tilde{a}$. Show that if $(B, \leq)$ is a Boolean lattice, then* $(B, \mathbf{sup}, \mathbf{inf}, \tilde{\ }, \mathbf{0}, \mathbf{1})$ *is a Boolean algebra.*

The next exercise provides a method of constructing Boolean algebras from linearly ordered sets.

Exercise 6.10.3 *Let $(L, \leq)$ be a linearly ordered set with a minimal element. A* **half interval** *is any of the sets*

$$[a, b) = \{x \in L \mid a \leq x < b\}, \quad [a, \infty) = \{x \in L \mid a \leq x\},$$

where $a, b \in L$. Thus, for example $\emptyset$ and L are half intervals. Consider the set B_L of all finite unions of half intervals of the linearly ordered set $(L, \leq)$. Prove that B_L forms a Boolean algebra under the set-theoretic operations of union, intersection, and complementation. This algebra is called the **algebra of intervals** *of $(L, \leq)$.*

6.10.2 Ideals, Factors, and Subalgebras of Boolean Algebras. In the theory of Boolean algebras an important concept is the notion of an ideal. Ideals can be used to build new Boolean algebras from a given one. Here is a definition of ideals.

Definition 6.10.4 *A set $I \subset B$ of a Boolean algebra $\mathcal{B}$ is an* **ideal** *if the following properties hold:*

1. $\mathbf{0} \in I$.
2. *For all $x \in I$ and $y \in B$, if $y \leq x$, then $y \in I$.*
3. *For all $x, y \in I$, $x \vee y \in I$.*

Clearly, $\{\mathbf{0}\}$ and B are ideals of any Boolean algebra $\mathcal{B}$. These are called trivial ideals. Nontrivial ideals are called **proper ideals**. Here are some examples of nontrivial ideals.

Example 6.10.4 *Consider the power set $P(A)$. Fix $X \subset A$. Consider the set $I(X)$ defined as $\{V \mid V \subseteq X\}$. Then $I(X)$ is an ideal of the Boolean algebra $P(A)$ of all subsets of the set A.*

Example 6.10.5 *Consider the power set $P(A)$. Consider the set $Fin(A)$ of all finite subsets of A. Then $Fin(A)$ is an ideal of $P(A)$.*

It turns out that every element $b \in B$ of a Boolean algebra $\mathcal{B}$ defines an ideal. Indeed, consider the set $I(a) = \{x \mid x \leq a\}$. Then this set is an ideal and is called the **principal ideal** generated by a.

Exercise 6.10.4 *Show that $I(a) = \{x \mid x \leq a\}$ is an ideal of $\mathcal{B}$.*

Let I be an ideal of a Boolean algebra $\mathcal{B}$. We can identify the elements a, b of $\mathcal{B}$ modulo I as follows: $a \sim_I b$ if and only if $(a \setminus b) \vee (b \setminus a) \in I$, where $a \setminus b$ is called the **difference** of a from b and equals $a \wedge \tilde{b}$. Thus informally, $a \sim_I b$ means that a and b cannot be distinguished if we do not count those parts of a and b which are in I. It turns out that the relation $\sim_I$ has some nice algebraic properties needed to build new Boolean algebras.

Lemma 6.10.2 *Let I be an ideal of a Boolean algebra $\mathcal{B}$. Then $\sim_I$ has the following properties:*

1. *The relation $\sim_I$ is an equivalence relation.*
2. *For all $a_1, a_2, b_1, b_2 \in B$, if $a_1 \sim_I a_2$ and $b_1 \sim_I b_2$, then*

$$(a_1 \vee b_1) \sim_I (a_2 \vee b_2), \quad (a_1 \wedge b_1) \sim_I (a_2 \wedge b_2), \quad \text{and } \tilde{a}_1 \sim_I \tilde{b}_1.$$

Proof. We prove the first part. It is clear that $\sim_I$ is a reflexive and symmetric relation. Assume that $a \sim_I b$ and $b \sim_I c$. Consider $a \setminus c$. Then we have the following:

$$\begin{aligned} a \setminus c = a \wedge \tilde{c} &= (a \wedge \tilde{c}) \wedge (b \vee \tilde{b}) = (a \wedge \tilde{c} \wedge b) \vee (a \wedge \tilde{c} \wedge \tilde{b}) \\ &\leq (\tilde{c} \wedge b) \vee (a \wedge \tilde{b}) = (b \setminus c) \vee (a \setminus b). \end{aligned}$$

Since $b \setminus c$ and $a \setminus b$ are in I, and I is an ideal, we have $(b \setminus c) \vee (a \setminus b) \in I$. Again using the fact that I is an ideal we conclude that the inequality $a \setminus c \leq (b \setminus c) \vee (a \setminus b)$ implies that $a \setminus c \in I$. One can prove in a similar manner that $c \setminus a \in I$. Hence $a \sim_I c$. We have proved the first part of the lemma.

Now we prove the second part of the lemma. Let us show that $(a_1 \vee b_1) \sim_I (a_2 \vee b_2)$. Consider $(a_1 \vee b_1) \setminus (a_2 \vee b_2)$. Then

$$\begin{aligned} (a_1 \vee b_1) \setminus (a_2 \vee b_2) &= (a_1 \vee b_1) \wedge (\widetilde{a_2 \vee b_2}) = (a_1 \vee b_1) \wedge \tilde{a}_2 \wedge \tilde{b}_2 \\ &= (a_1 \wedge \tilde{a}_2 \wedge \tilde{b}_2) \vee (b_1 \wedge \tilde{a}_2 \wedge \tilde{b}_2) \leq (a_1 \setminus a_2) \vee (b_1 \setminus b_2). \end{aligned}$$

Hence $(a_1 \vee b_1) \setminus (a_2 \vee b_2) \in I$. Similarly, $(a_2 \vee b_2) \setminus (a_1 \vee b_1)$. Therefore, $(a_1 \vee b_1) \sim_I (a_2 \vee b_2)$. We leave it to the reader to prove the rest of the lemma. □

Exercise 6.10.5 *Finish the proof of the lemma above.*

For an ideal I of a Boolean algebra $\mathcal{B}$, consider the set B_I that consists of all $\sim_I$-equivalence classes. Thus, $B_I = \{a_I \mid a \in B\}$, where a_I is the $\sim_I$-equivalence class containing a. Define $\vee$, $\wedge$, and $\tilde{}$ operations on B_I as

$$a_I \vee b_I = (a \vee b)_I, \quad a_I \wedge b_I = (a \wedge b)_I, \quad \tilde{a_I} = \tilde{a}_I.$$

The second part of the lemma above shows that these operations are well defined, that is, are independent of representatives of the $\sim_I$-equivalence classes. Now it is not hard to see that the structure $(B_I, \vee, \wedge, \tilde{}, \mathbf{0}_I, \mathbf{1}_I)$ is a Boolean algebra. We denote it by $\mathcal{B}_I$. The algebra $\mathcal{B}_I$ is called **the factor algebra** of $\mathcal{B}$ by the ideal I.

Exercise 6.10.6 *Consider the Boolean algebra $P(A)$, where A is an infinite set. Consider the ideal $Fin = \{X \mid X \subset A$ and X is finite$\}$. Consider the factor algebra $\mathcal{B}$ of $P(A)$ with respect to Fin. Show that for all $x \in B$, if $x \neq \mathbf{0}$, then there exists an infinite sequence $x_1, x_2, \ldots$ of distinct elements such that $x \geq x_1 \geq x_2 \geq x_3 \geq \cdots$.*

Let $\mathcal{B}$ be a Boolean algebra. Consider a subset $C \subset B$. It can be the case that C is closed under the operations of the Boolean algebra $\mathcal{B}$. For example, $C = \{\mathbf{0}, \mathbf{1}\}$ is such that the operations $\vee$, $\wedge$, and $\tilde{}$ applied to elements of C again produce elements of C. In this case we say that C is a subalgebra of $\mathcal{B}$. A formal definition is as follows.

Definition 6.10.5 *A* **Boolean subalgebra** *of $\mathcal{B}$ is a nonempty subset C of B such that for all $a, b \in C$ we have $a \vee b$, $a \wedge b$, $\tilde{a} \in C$.*

Note that if C is a subalgebra of $\mathcal{B}$, then for any $c \in C$, $c \vee \tilde{c}, c \wedge \tilde{c} \in C$. Hence any subalgebra contains $\mathbf{0}$ and $\mathbf{1}$ of the original Boolean algebra $\mathcal{B}$.

Theorem 6.10.1 *Let A be a subset of a Boolean algebra $\mathcal{B}$. Then there exists a minimal, with respect to the set-theoretic inclusion, Boolean subalgebra $\mathcal{C}$ of $\mathcal{B}$ that contains A. Moreover, any element $x \in C$ can be written in the form*

$$x = \bigvee_{i \leq s} a_{i,1}^{\epsilon_{i,1}} \wedge \cdots \wedge a_{i,t_i}^{\epsilon_{i,t_i}},$$

where $s \geq 1$, each $a_{i,j}$ is in A, $\epsilon_{i,j} \in \{0, 1\}$, and $a^0 = \tilde{a}$, $a^1 = a$.

Proof. The proof is quite easy. Note that the intersection of any collection of Boolean subalgebras of $\mathcal{B}$ is again a Boolean subalgebra. Thus, we can consider all the Boolean subalgebras that contain A. Then the intersection C of these Boolean algebras is a Boolean algebra. The Boolean subalgebra $\mathcal{C}$ (whose domain is the set C) is the minimal one with respect to the set-theoretic inclusion. Now note that any Boolean subalgebra that contains A also contains the elements of the form $x = \bigvee_{i \leq s} a_{i,1}^{\epsilon_{i,1}} \wedge \cdots \wedge a_{i,t_i}^{\epsilon_{i,t_i}}$, where $s \geq 1$ and $a_{i,j} \in A$. Moreover the reader can check that the set of all elements of this type forms a Boolean subalgebra. Hence this proves the last part of the theorem. □

Exercise 6.10.7 *Give a proof of the theorem above in greater detail.*

Let A be the subset of a Boolean algebra $\mathcal{B}$. Consider the minimal subalgebra $\mathcal{C}$ that contains A. In this case we say that A **generates** the Boolean algebra $\mathcal{C}$. Hence we have the following result which follows from the theorem above.

Corollary 6.10.1 *Let A be a subset of a Boolean algebra $\mathcal{A}$. Then A generates a Boolean subalgebra $\mathcal{C}$ if and only if every element x of $\mathcal{C}$ can be written in the form*

$$x = \bigvee_{i \leq s} a_{i,1}^{\epsilon_{i,1}} \wedge \cdots \wedge a_{i,t_i}^{\epsilon_{i,t_i}},$$

where $s \geq 1$ and $a_{i,j} \in A$. $\square$

6.10.3 Maximal Ideals of Boolean Algebras. One of our goals is to show that we can treat elements of a given Boolean algebra as subsets of a certain set. In order to achieve the goal we need to better understand ideals of Boolean algebras. In this part of the section we study maximal ideals.

Definition 6.10.6 *An ideal I of a Boolean algebra $\mathcal{B}$ is* **maximal** *if I is a proper ideal and every proper ideal J that contains I coincides with I.*

To give an example of a maximal ideal we define another important notion.

Definition 6.10.7 *An element a of a Boolean algebra $\mathcal{B}$ is called an* **atom** *if $a \neq \mathbf{0}$ and, for all $b \in B$, if $\mathbf{0} \leq b \leq a$, then either $b = \mathbf{0}$ or $b = a$.*

We leave the reader to prove the following exercise.

Exercise 6.10.8 *For an element a of a Boolean algebra the following properties are equivalent:*

1. *a is an atom.*
2. *For all $b \in B$, if $b \wedge a \neq \mathbf{0}$, then $a \leq b$.*
3. *For all $b, c \in B$, if $a = b \vee c$ and $b \wedge c = \mathbf{0}$, then either $a = b$ or $a = c$.*

Here now is an example of a maximal ideal.

Example 6.10.6 *Let a be an element of a Boolean algebra such that $\tilde{a}$ is an atom. Then the principal ideal $I(a)$ generated by a is maximal.*

Indeed, assume that J is a proper ideal containing $I(a)$ and $b \in J \setminus I(a)$. Note that $a \vee b \in J$, $a \neq a \vee b$ and $a \leq a \vee b$. Since J is proper, we have $a \vee b \neq \mathbf{1}$. Hence $\widetilde{a \vee b} \neq \mathbf{0}$. We also have $\widetilde{a \vee b} \leq \tilde{a}$ and $\tilde{a} \neq \widetilde{a \vee b}$. This contradicts the fact that $\tilde{a}$ is an atom.

Let $\mathcal{B}$ be a countable Boolean algebra. Take a subset $X \subset B$. We say that X is **consistent** if for all positive $n \in \omega$ and all $b_1, \ldots, b_n \in X$ we have $b_1 \vee b_2 \vee \cdots \vee b_n \neq \mathbf{1}$. Thus for example, any singleton set $\{b\}$ with $b \neq \mathbf{1}$ is consistent. Also note that if X is consistent, then X does not contain $\mathbf{1}$.

Lemma 6.10.3 *Let X be a consistent set of a Boolean algebra $\mathcal{B}$. Then for every $b \in B$ either $X \bigcup \{b\}$ or $X \bigcup \{\tilde{b}\}$ is a consistent set.*

Proof. Assume that both $X \bigcup \{b\}$ as well as $X \bigcup \{\tilde{b}\}$ are inconsistent sets. Then there exist $x_1, \ldots, x_n, y_1, \ldots, y_m$ all in X such that

$$x_1 \vee x_2 \vee \cdots \vee x_n \vee b = \mathbf{1} \text{ and } y_1 \vee y_2 \vee \cdots \vee y_m \vee \tilde{b} = \mathbf{1}.$$

Let $x = x_1 \vee x_2 \vee \cdots \vee x_n$ and $y = y_1 \vee y_2 \vee \cdots \vee y_m$. Then

$$x \vee y = (x \vee y) \vee (b \wedge \tilde{b}) = ((x \vee y) \vee b) \wedge ((x \vee y) \vee \tilde{b}) = \mathbf{1}.$$

This is a contradiction to the fact that X is consistent. The lemma is proved.

Now our goal is to give a construction that puts every consistent set X into a maximal ideal. The construction is explained in the proof of the following theorem.

Theorem 6.10.2 *Let X be a consistent set of a countable Boolean algebra. Then there exists a maximal ideal I such that $X \subset I$.*

Proof. Since $\mathcal{B}$ is a countable Boolean algebra, we can consider the sequence without repetition

$$b_0, b_1, b_2, \ldots$$

of all elements of B. Now we construct an ideal I that contains X by stages. At stage s of the construction we will put one of the elements b_s or $\tilde{b}_s$ into the set that is being constructed. Here is the construction:

Stage 0. Consider the element b_0. By the lemma above either $X \cup \{b_0\}$ or $X \cup \{\tilde{b}_0\}$ is consistent. If $X \cup \{b_0\}$ is consistent, then set $X_0 = X \cup \{b_0\}$. Otherwise, set $X_0 = X \cup \{\tilde{b}_0\}$.

Stage $s + 1$. Assume that X_s has been constructed and is consistent by the induction hypothesis. Consider the element b_{s+1}. By the lemma above either $X_s \cup \{b_{s+1}\}$ or $X_s \cup \{\tilde{b}_{s+1}\}$ is consistent. If $X_s \cup \{b_{s+1}\}$ is consistent, then set $X_{s+1} = X_s \cup \{b_{s+1}\}$. Otherwise, set $X_{s+1} = X_s \cup \{\tilde{b}_{s+1}\}$.

Now we define $I = \bigcup_{s \in \omega} X_s$. Now note that I is a consistent set. Otherwise, some X_s would be inconsistent. Also note that for every $b \in B$ either $b \in I$ or $\tilde{b} \in I$, because $b = b_s$ for some s, and at stage s either b or its complement is put into I. Now we show that I is a proper ideal. Since I is consistent, $\mathbf{1}$ does not belong to I. Also note that $\mathbf{0} \in I$. Let $x \in I$ and $y \leq x$. We need to show that $y \in I$. If $y \notin I$, then $\tilde{y} \in I$. Now consider $x \vee \tilde{y}$. Since $y \leq x$ we have $x \vee \tilde{y} = (x \vee y) \vee \tilde{y} = \mathbf{1}$. Hence I is inconsistent. Therefore, $y \in I$. Now assume that $x, y \in I$. We need to show that $x \vee y \in I$. If not, then $\widetilde{x \vee y} \in I$. Then

$x \vee y \vee \widetilde{x \vee y} = \mathbf{1}$. Hence I is inconsistent. Therefore, $x \vee y \in I$. Thus, I is an ideal.

We need to show that I is a maximal ideal. Assume that I is not maximal. Let J be a proper ideal that contains I such that $b \in J \setminus I$ for some b. Then $\tilde{b} \in I$. Hence $\tilde{b} \in J$. Therefore, $b \vee \tilde{b} \in J$. Hence J is not proper. This contradicts the assumption that I is not maximal. Hence we have shown that I is a maximal ideal that contains X. The theorem is proved.

Corollary 6.10.2 *For any countable Boolean algebra $\mathcal{B}$ and any $b \neq \mathbf{1}$ in $\mathcal{B}$ there exists a maximal ideal that contains b.* □

Corollary 6.10.3 *For any countable Boolean algebra $\mathcal{B}$ and any $b \neq \mathbf{0}$ in $\mathcal{B}$ there exists a maximal ideal that does not contain b.*

Proof. Take $\tilde{b}$. Then $\tilde{b} \neq \mathbf{1}$. By the previous corollary there exists a maximal ideal that contains $\tilde{b}$. The ideal clearly does not contain b. The corollary is proved.

Corollary 6.10.4 *A proper ideal of a countable Boolean algebra I is maximal if and only if for all $b \in B$ either $b \in I$ or $\tilde{b} \in I$.*

Proof. Let I be a proper maximal ideal. If for some b neither $b \in I$ nor $\tilde{b} \in I$, then either $I \bigcup \{b\}$ or $I \bigcup \{\tilde{b}\}$ is consistent. Hence we can construct a proper ideal containing I. This contradicts the assumption that I is maximal. Assume that for all $b \in B$ either $b \in B$ or $\tilde{b} \in B$ but I is not a maximal ideal. Let J be a proper maximal ideal containing I such that $a \in I \setminus J$ for some a. Then $\tilde{a} \in I$. Hence $a \vee \tilde{a} = \mathbf{1}$. This contradicts the assumption that J is proper. The corollary is proved.

Exercise 6.10.9 *Let $\mathcal{B}$ be a Boolean algebra. A subset $F \subset B$ is a* **filter** *if the following properties hold:*

1. $\mathbf{1} \in I$.
2. *For all $x \in I$ and $y \in B$, if $y \geq x$, then $y \in I$.*
3. *For all $x, y \in I$, $x \wedge y \in I$.*

Prove the following:

1. *F is a filter if and only if the set $\tilde{F} = \{\tilde{x} \mid x \in F\}$ is an ideal.*
2. *Every proper filter is contained in a maximal filter.*

6.10.4 The Stone Representation Theorem. In this section we prove one of the fundamental results about Boolean algebras. The result basically tells us that we can think of the operations of a Boolean algebra as the set-theoretic operations of union, intersection and complementation on some family of subsets of a certain set. Hence all the set-theoretic laws that hold for the set-theoretic operations also hold for the operations that define Boolean algebras. Recall our assumption that Boolean algebras are countable. We add that the Stone theorem holds for uncountable Boolean algebras as well.

Let $\mathcal{B}$ be a Boolean algebra. We can consider the set of all maximal ideals of the Boolean algebra $\mathcal{B}$. Let us denote this set by $I(\mathcal{B})$. Our goal will be to show that the Boolean algebra $\mathcal{B}$ can be viewed as a family of subsets of $I(\mathcal{B})$ closed under the set-theoretic operations of union, intersection and complementation. In order to do this we need to associate with each element b of the Boolean algebra a subset of $I(\mathcal{B})$. So let us take any element $b \in B$. Consider the set $R(b)$ of all ideals that do not contain b. Thus,

$$R(b) = \{I \mid I \text{ is a maximal ideal of } \mathcal{B} \text{ and } b \notin I\}.$$

Clearly, $R(b) \subset I(\mathcal{B})$. Thus we have a mapping R from the Boolean algebra $\mathcal{B}$ into the set of all subsets of $I(\mathcal{B})$. Now we will study several properties of the mapping $R : \mathcal{B} \to P(I(\mathcal{B}))$, where we recall that $P(A)$ is the power set of the set A. The following lemma follows immediately from the definition of the mapping R.

Lemma 6.10.4 *For R, we have $R(\mathbf{1}) = I(\mathcal{B})$ and $R(\mathbf{0}) = \emptyset$.* □

Lemma 6.10.5 *For all $a, b \in B$, if $a \neq b$, then $R(a) \neq R(b)$.*

Proof. Note that either $a \not\leq b$ or $b \not\leq a$ since $a \neq b$. We can suppose that $a \not\leq b$ (otherwise we would change the roles of a and b). Consider $a \wedge \tilde{b}$. If $a \wedge \tilde{b} = \mathbf{0}$, then

$$a = a \wedge \mathbf{1} = a \wedge (b \vee \tilde{b}) = (a \wedge b) \vee (a \wedge \tilde{b}) = a \wedge b.$$

Hence $a \leq b$. This is a contradiction to the assumption that $a \not\leq b$. Hence $a \wedge \tilde{b} \neq \mathbf{0}$. By Corollary 6.10.3, we can take a maximal ideal I that does not contain $a \wedge \tilde{b}$. Hence $a \notin I$ and $\tilde{b} \notin I$. Therefore, $b \in I$. We conclude that $I \in R(a)$ and $I \notin R(b)$. Therefore, $R(a) \neq R(b)$. The lemma is proved.

Lemma 6.10.6 *For all $a, b \in B$ we have the equalities*

$$R(a \vee b) = R(a) \cup R(b) \quad \text{and} \quad R(a \wedge b) = R(a) \cap R(b).$$

Proof. We prove the equality $R(a \vee b) = R(a) \cup R(b)$. The other equality can be proved in a similar manner. Thus, assume that $I \in R(a \vee b)$. We need to show that either $I \in R(a)$ or $I \in R(b)$. If neither $I \in R(a)$ nor $I \in R(b)$, then $a \in I$ and $b \in I$. Hence $a \vee b \in I$. This is a contradiction. Therefore, either $I \in R(a)$ or $I \in R(b)$. Assume that $I \in R(a)$. We need to show that $I \in R(a \vee b)$. We can suppose that $I \in R(a)$. Then $a \notin I$. Consider $a \vee b$. If $a \vee b \in I$, then $a \in I$ by the definition of ideal. Hence $a \vee b \notin I$. Therefore, $I \in R(a \vee b)$. The lemma is proved. □

Exercise 6.10.10 *Prove the equality $R(a \wedge b) = R(a) \cap R(b)$.*

Lemma 6.10.7 *For all $a \in B$, the equality $I(\mathcal{B}) \setminus R(a) = R(\tilde{a})$ holds.*

Proof. In order to prove the equality assume that $I \notin R(a)$. Then $a \in I$. Since I is maximal, $\tilde{a} \notin I$. Hence $I \in R(\tilde{a})$. Now assume that $I \in R(\tilde{a})$. Then $\tilde{a} \notin I$. Therefore, $a \in I$ since I is maximal. Hence $I \notin R(a)$. The lemma is proved.

Thus, the last four lemmas show that the set $\{R(a) \mid a \in B\}$ is closed under the set-theoretic operations of union, intersection, and complementation. Moreover, $I(\mathcal{B}), \emptyset \in \{R(a) \mid a \in B\}$. Hence, we conclude that the structure

$$(\{R(a) \mid a \in B\}, \cup, \cap, \setminus, \emptyset, I(\mathcal{B}))$$

is a Boolean algebra. The lemmas also guarantee that the mapping R is an isomorphism from the Boolean algebra $\mathcal{B}$ onto the Boolean algebra $(\{R(a) \mid a \in B\}, \bigcup, \bigcap, \setminus, \emptyset, I(\mathcal{B}))$. Note that $\{R(a) \mid a \in B\}$ is a family of subsets of $I(\mathcal{B})$. Here now is the theorem called Stone's representation theorem.

Theorem 6.10.3 *Any countable Boolean algebra is isomorphic to a Boolean algebra of subsets.*

Proof. Take a Boolean algebra $\mathcal{B}$. Then the mapping $a \to R(a)$ is an isomorphism from $\mathcal{B}$ onto $(\{R(a) \mid a \in B\}, \bigcup, \bigcap, \setminus, \emptyset, I(\mathcal{B}))$, which follows from the lemmas above. The theorem is proved.

This theorem allows us to use some set-theoretic terminology about elements of Boolean algebras. For example, for elements a, b of a Boolean algebra one can say that a is a subset of b to mean $a \leq b$. Similarly, we can say that a and b are pairwise disjoint to mean that $a \wedge b = \mathbf{0}$.

Exercise 6.10.11 *Let A be a subset of a Boolean algebra $\mathcal{B}$. Show that the minimal Boolean subalgebra of $\mathcal{B}$ containing A is finite if A is finite.*

Exercise 6.10.12 *Prove that any finite algebra $\mathcal{B}$ is generated by its atoms. Moreover show that any element $b \in B$ can be presented as a finite union of atoms of $\mathcal{B}$.*

Exercise 6.10.13 *A Boolean algebra $\mathcal{B}$ is* **atomic** *if for every $b \in B$ there exists an atom a such that $a \leq b$. Let A be the set of all atoms of $\mathcal{B}$. Show that any atomic Boolean algebra $\mathcal{B}$ is isomorphic to the Boolean algebra $P(A)$ of all subsets of A.*

6.10.5 Homomorphisms of Boolean Algebras. Throughout this section, all Boolean algebras are assumed to be countable unless otherwise stated. Let $\mathcal{A}$ and $\mathcal{B}$ be Boolean algebras. We say that the mapping $h : A \to B$ is a **homomorphism** if $h(\mathbf{0}) = \mathbf{0}$, $h(\mathbf{1}) = \mathbf{1}$, and for all $a, b \in A$ we have $h(a \vee b) = h(a) \vee h(b)$,

$h(a \wedge b) = h(a) \wedge h(b)$, and $h(\tilde{a}) = \widetilde{h(a)}$. Clearly, if a homomorphism h is onto and a one-to-one mapping then h is an isomorphism. A homomorphism h is called an **embedding** if $h(x) \neq h(y)$ for $x \neq y$.

Example 6.10.7 *Let I be an ideal of a Boolean algebra $\mathcal{B}$. Then the mapping $h : b \to b_I$ that maps every $b \in B$ to the $\sim_I$-equivalence class b_I containing b is a homomorphism from $\mathcal{B}$ onto the factor algebra $\mathcal{B}_I$.*

The next theorem shows that the example above is, in a certain sense, a canonical way of constructing homomorphisms of Boolean algebras.

Theorem 6.10.4 *Let h be a homomorphism from a Boolean algebra $\mathcal{B}$ onto a Boolean algebra $\mathcal{A}$. Consider the set $I = \{b \in B \mid h(a) = \mathbf{0}\}$. Then I is an ideal and the factor algebra $\mathcal{B}_I$ is isomorphic to $\mathcal{A}$.*

Proof. We prove that I is an ideal. Clearly, $\mathbf{0} \in I$. Let x be in I and $y \leq x$. Then $y \wedge x = x$. Therefore, $h(x) = h(y \wedge x) = h(y) \wedge h(x) = \mathbf{0} \wedge h(x) = \mathbf{0}$. Hence $y \in I$. Take now two elements x, y from I. Then $h(x \vee y) = h(x) \vee h(y) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$. Hence $x \vee y \in I$. We conclude that I is an ideal.

Let us consider the factor Boolean algebra $\mathcal{B}_I$. We define the mapping g from $\mathcal{B}_I$ into $\mathcal{A}$ with the goal of showing that $\mathcal{B}_I$ is isomorphic to $\mathcal{A}$. Take any element $b_I \in \mathcal{B}_I$. Define $g(b_I) = h(b)$. The function g that maps each b_I into $h(b)$ is well defined because it does not depend on the representatives of the $\sim_I$-equivalence class containing b. Using the fact that h is a homomorphism from $\mathcal{B}$ onto $\mathcal{A}$, we see that g is also a homomorphism from $\mathcal{B}_I$ into $\mathcal{A}$. We need to show that g is a one-to-one mapping. Let $b_I \neq a_I$. Assume that $g(b_I) = g(a_I)$. Then $h(a) = h(b)$. Hence $h(a \setminus b) = h(b \setminus a) = \mathbf{0}$. Therefore, $a \setminus b, b \setminus a \in I$. Hence $a_I = b_I$. This is a contradiction to the assumption that $a_I \neq b_I$. Therefore, h is an isomorphism. The theorem is proved.

We now give some conditions that allow us to build homomorphisms and isomorphisms between Boolean algebras. The following definition gives a useful condition for constructing homomorphisms.

Definition 6.10.8 *Let $\mathcal{A}$ and $\mathcal{B}$ be Boolean algebras. A set $H \subset A \times B$ is a* **homomorphism condition** *from $\mathcal{A}$ into $\mathcal{B}$ if H has the following properties:*

1. $(\mathbf{0}, \mathbf{0}), (\mathbf{1}, \mathbf{1}) \in H$.
2. *If $(x, y) \in H$ and $x = \mathbf{0}$, then $y = \mathbf{0}$.*
3. *If $(x, y) \in H$ and $x_1 \leq x$, then there exists y_1 such that $y_1 \leq y$, $(x_1, y_1) \in H$ and $(x \setminus x_1, y \setminus y_1) \in H$.*

We now prove that any homomorphism condition from $\mathcal{A}$ into $\mathcal{B}$ allows one to construct a homomorphism from $\mathcal{A}$ into $\mathcal{B}$.

Theorem 6.10.5 *Let H be a homomorphism condition from a Boolean algebra $\mathcal{A}$ into a Boolean algebra $\mathcal{B}$. Then there exists a homomorphism h from $\mathcal{A}$ into $\mathcal{B}$ with the following property: for all $a \in A$, if there exist pairwise disjoint elements $a_1, \ldots, a_n$ such that $\vee_i a_i = a$, then $(a_i, h(a_i)) \in H$.*

Proof. Since $\mathcal{A}$ is countable we can list all elements of $\mathcal{A}$ into a sequence $a_0, a_1, a_2, \ldots$ without repetition. We construct a homomorphism h by stages. The construction uses the homomorphism condition H. At stage $s+1$ of the construction we will have a finite Boolean subalgebra $\mathcal{A}_{s+1}$ of $\mathcal{A}$ and a homomorphism $h_{s+1} : \mathcal{A}_{s+1} \to \mathcal{B}$ constructed. These will satisfy the following conditions:

1. For all s, $A_s \subset A_{s+1}$.
2. For all s, $h_s \subset h_{s+1}$, hence the homomorphism h_{s+1} extends h_s.
3. For all s, the element a_s belongs to A_{s+1}.
4. For all s and $a \in A_s$ the pair $(a, h_s(a))$ belongs to H.

Note that condition (3) guarantees that $h = \bigcup_s h_s$ is a map from A into B. Conditions (2) and (3) guarantee that h is a homomorphism from $\mathcal{A}$ into $\mathcal{B}$. Here now is the construction.

Stage 0. We set $A_0 = \{\mathbf{0}, \mathbf{1}\}$, $h_0(\mathbf{0}) = \mathbf{0}$, and $h_0(\mathbf{1}) = \mathbf{1}$. Clearly, h_0 is a homomorphism from $\mathcal{A}_0$ into $\mathcal{B}$.

Stage $s+1$. Consider the Boolean algebra $\mathcal{A}_s$ generated at the previous stage. Let $a_0, \ldots, a_k$ be the set of all atoms of $\mathcal{A}_s$. These atoms generate $\mathcal{A}_s$. By the induction hypothesis we have $(a_0, h_s(a_0)), \ldots, (a_k, h_s(a_k)) \in H$. We construct $\mathcal{A}_{s+1}$ as follows. Take the element a_s. For each $i \in \{0, \ldots, k\}$, form the elements $d_{2i} = a_i \wedge a_s$ and $d_{2i+1} = a_i \wedge \bar{a}_s$. Since $(a_i, h_s(a_i)) \in H$ and $d_{2i} \leq a_i$, there must exist a b_{2i} such that $b_{2i} \leq h_s(a_i)$, $(d_{2i}, b_{2i}) \in H$ and $(d_{2i+1}, h_s(a_i) \setminus b_{2i}) \in H$. We set $b_{2i+1} = h_s(a_i) \setminus b_{2i}$. Now set $\mathcal{A}_{s+1}$ to be the Boolean algebra generated by elements $d_0, \ldots, d_{2k+1}$. Clearly, $A_s \subset A_{s+1}$. Moreover the elements $d_0, \ldots, d_{2k+1}$ are atoms of the Boolean algebra $\mathcal{A}_{s+1}$. Thus, we have constructed the subalgebra $\mathcal{A}_{s+1}$. Note that $a_s \in A_{s+1}$ because $a_s = d_0 \vee d_2 \vee \cdots \vee d_{2k}$. Now we need to define the homomorphism h_{s+1}. Take any element $a \in A_{s+1}$. There must exist a finite set $K \subset \{0, 1, \ldots, 2k+1\}$ such that $a = \bigvee_{j \in K} d_j$. Set $h_{s+1}(a) = \bigvee_{j \in K} b_j$. It is not hard to see that $h_s \subset h_{s+1}$.

Now we set $h = \bigcup_s h_s$. As noted above h is a homomorphism from $\mathcal{A}$ into $\mathcal{B}$. The theorem is proved.

The homomorphism condition H from $\mathcal{A}$ into $\mathcal{B}$ does not guarantee that there exists a homomorphism from $\mathcal{A}$ onto $\mathcal{B}$. However, we can add an extra condition on H that will suffice to build a homomorphism from $\mathcal{A}$ onto $\mathcal{B}$. We give the following definition.

Definition 6.10.9 *A homomorphism condition H from $\mathcal{A}$ into $\mathcal{B}$ is called an* **epimorphism condition** *from $\mathcal{A}$ onto $\mathcal{B}$ if for all $(x, y) \in H$ and $b \leq y$ there exists an $a \in A$ such that $a \leq x$, $(a, b) \in H$ and $(x \setminus a, y \setminus b) \in H$.*

Now we prove the following theorem that, given epimorphism condition H from $\mathcal{A}$ into $\mathcal{B}$, builds a homomorphism from $\mathcal{A}$ onto $\mathcal{B}$.

Theorem 6.10.6 *Let H be an epimorphism condition from a Boolean algebra $\mathcal{A}$ into a Boolean algebra $\mathcal{B}$. Then there exists a homomorphism h from $\mathcal{A}$ onto $\mathcal{B}$ with the following property: for all $a \in A$ if there exist pairwise disjoint elements $a_1, \ldots, a_n$ such that $\vee_i a_i = a$, then $(a_i, h(a_i)) \in H$.*

Proof. The proof is very similar to the proof of the previous theorem. We sketch the proof and leave the details to the reader. Since $\mathcal{A}$ and $\mathcal{B}$ are countable we can list all elements of $\mathcal{A}$ and $\mathcal{B}$ into the sequences

$$a_0, a_1, a_2, \ldots \quad \text{and} \quad b_0, b_1, b_2, \ldots,$$

respectively. We construct a homomorphism h from $\mathcal{A}$ onto $\mathcal{B}$ by stages. At stage 0, we set $A_0 = \{\mathbf{0}, \mathbf{1}\}$, $h_0(\mathbf{0}) = \mathbf{0}$, and $h_0(\mathbf{1}) = \mathbf{1}$. Clearly, h_0 is a homomorphism from $\mathcal{A}_0$ into $\mathcal{B}$. At stage $s+1$, we will have a finite Boolean subalgebra $\mathcal{A}_{s+1}$ of $\mathcal{A}$ and a homomorphism $h_{s+1} : \mathcal{A}_{s+1} \to \mathcal{B}$ constructed. These will satisfy the following conditions:

1. For all s, $A_s \subset A_{s+1}$.
2. For all s, $h_s \subset h_{s+1}$, hence h_{s+1} extends h_s.
3. For all $s = 2k+1$, the element a_s belongs to A_{2s+1}.
4. For all $s = 2k+2$, the element b_s belongs to $h_s(A_{2s+s})$.
5. For all s and $a \in A_s$ the pair $(a, h_s(a))$ belongs to H.

All these conditions guarantee that the mapping $h = \bigcup_s h_s$ is a homomorphism from A onto B.

The construction of h_s at stage s is very similar to the construction of the homomorphism in the proof of the previous theorem. The only modification is that at each odd stage $s = 2k+1$, the construction makes sure that a_k is put into the domain of the function h_s; at each even stage $s = 2k+2$,the construction guarantees that b_k is put into the range of the function h_s. At odd stages the construction can be carried out successfully because H is an epimorphism condition. The rest of the proof is left to the reader. □

Exercise 6.10.14 *Finish the proof of the theorem.*

We now give an application of the theorems above. A Boolean algebra $\mathcal{B}$ is **atomless** if $\mathcal{B}$ contains no atoms. An example of an atomless Boolean algebra is the following. Consider the power set $P(\omega)$. Let F be the ideal of the Boolean algebra $P(\omega)$ that consists of all finite subsets of ω. Consider the algebra obtained by factoring $P(\omega)$ by the ideal F. Then the factor algebra is an atomless Boolean algebra. Note that this Boolean algebra is uncountable.

Exercise 6.10.15 *Show that the Boolean algebra of intervals (see Exercise* 6.10.3*) of the linearly ordered set* $[0, 1]$ *is an atomless Boolean algebra.*

Exercise 6.10.16 *Give an example of a countable atomless Boolean algebra.*

Corollary 6.10.5 *If $\mathcal{B}$ is an atomless Boolean algebra, then for any Boolean algebra $\mathcal{A}$, there exists a homomorphism from $\mathcal{B}$ onto $\mathcal{A}$.*

Proof. Define the set $E \subset A \times B$ as

$$E = \{(a, b) \mid a \in A, b \in B, \text{ if } a = \mathbf{0}, \text{then } b = \mathbf{0}\}.$$

It is not hard to see that E is an epimorphism condition. The corollary is proved.

Definition 6.10.10 *A homomorphism condition H from $\mathcal{A}$ into $\mathcal{B}$ is an* **embedding condition** *if the condition $(x, \mathbf{0}) \in H$ implies that $x = \mathbf{0}$.*

Corollary 6.10.6 *If H is an embedding condition from $\mathcal{A}$ into $\mathcal{B}$, then there exists a homomorphism from $\mathcal{A}$ into $\mathcal{B}$ such that h is a one-to-one mapping.*

Proof. Since H is a homomorphism condition by Theorem 6.10.5 we can construct a homomorphism h from $\mathcal{A}$ into $\mathcal{B}$. We need to show that the constructed h is in fact an embedding. If h is not an embedding, then there exists a stage $s + 1$ such that $h_{s+1}(a) = h_{s+1}(b)$ for some distinct $a, b \in A_{s+1}$. Hence $h_{s+1}(a \setminus b) = h_{s+1}(a) \setminus h_{s+1}(b) = \mathbf{0}$. Note that $a \setminus b \in A_{s+1}$, and we can assume that $a \setminus b \neq \mathbf{0}$. Then $h_{s+1}(a \setminus b) \neq \mathbf{0}$ by the construction of h_{s+1} and the fact that H is an embedding condition. This is a contradiction. The corollary is proved. □

Definition 6.10.11 *A homomorphism condition H from $\mathcal{A}$ into $\mathcal{B}$ is a* **isomorphism condition** *if H is an epimorphism and embedding condition.*

Corollary 6.10.7 *If I is an isomorphism condition from $\mathcal{A}$ into $\mathcal{B}$, then there exists an isomorphism from $\mathcal{A}$ onto $\mathcal{B}$.*

Proof. The proof follows from Theorem 6.10.6 and the corollary above. □

Corollary 6.10.8 *Any two atomless Boolean algebras are isomorphic.*

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be atomless Boolean algebras. Consider the set

$$H = \{(\mathbf{0}, \mathbf{0}), (\mathbf{1}, \mathbf{1})\} \bigcup \{(a, b) \mid a \in A, b \in B, a \notin \{\mathbf{0}, \mathbf{1}\}, b \notin \{\mathbf{0}, \mathbf{1}\}\}.$$

It is not hard to check that I is an isomorphism condition from $\mathcal{A}$ into $\mathcal{B}$. The corollary is proved.

Corollary 6.10.9 *Let $\mathcal{B}$ be an atomless Boolean algebra. For any algebra $\mathcal{A}$ there exists an ideal I of $\mathcal{B}$ such that the factor algebra $\mathcal{B}_I$ is isomorphic to $\mathcal{A}$.*

Proof. By Corollary 6.10.5 there exists a homomorphism h from $\mathcal{B}$ onto $\mathcal{A}$. Consider the ideal $I = \{b \mid h(b) = \mathbf{0}\}$. Then by Theorem 6.10.5, the factor algebra $\mathcal{B}_I$ is isomorphic to $\mathcal{A}$. The corollary is proved.

Corollary 6.10.10 *Let h be a homomorphism from a Boolean algebra $\mathcal{B}$ onto $\mathcal{A}$. There exists a Boolean subalgebra $\mathcal{C}$ of $\mathcal{B}$ that is isomorphic to the Boolean algebra $\mathcal{A}$.*

Proof. Consider the set

$$H = \{(b, a) \mid h(b) = a \text{ and } a = \mathbf{0} \text{ if and only if } b = \mathbf{0}\}.$$

It is not hard to see that H is an embedding condition. Hence $\mathcal{A}$ can be embedded into $\mathcal{B}$.

Corollary 6.10.11 *Let $\mathcal{B}$ be an atomless Boolean algebra. For any algebra $\mathcal{A}$ there exists a Boolean subalgebra $\mathcal{C}$ of $\mathcal{B}$ such that $\mathcal{C}$ and $\mathcal{A}$ are isomorphic.*

Proof. By Corollary 6.10.5 there exists a homomorphism h from $\mathcal{B}$ onto $\mathcal{A}$. By the previous corollary there exists a Boolean subalgebra $\mathcal{C}$ of $\mathcal{B}$ such that $\mathcal{C}$ and $\mathcal{A}$ are isomorphic. The corollary is proved.

The exercise below can be proved by finding appropriate isomorphism conditions.

Exercise 6.10.17 *Let $\mathcal{A}$ be a Boolean subalgebra of a Boolean algebra $\mathcal{B}$. Assume that the following conditions hold:*

1. *For any $a \in A$ there exists a finite set A_a of atoms of $\mathcal{B}$ such that $a = \vee_{c \in A_a} c$.*
2. *$\mathcal{A}$ has infinitely many atoms.*
3. *$\mathcal{B}$ is generated by the set A and all atoms of $\mathcal{B}$.*

Show that $\mathcal{A}$ and $\mathcal{B}$ are isomorphic.

6.10.6 Decidability Results. In this section we will show that the theory of all countable Boolean algebras with variables that run over ideals is decidable. We will give an exact definition of this theory, and prove that the theory can be reduced to $S2S$. In our proof we use our knowledge from the previous section about Cantor's discontinuum CD, structures related to CD, and decidability of theories of these structures. Our interest will be in special types of open sets on CD. Here is a definition of these sets.

Definition 6.10.12 *A set $U \subseteq CD$ is* **clopen** *if U and the complement of U are open sets.*

Thus, we see that U is a clopen set if and only if U and the complement of U are closed sets. For any $v \in \{0,1\}^\star$ the set $U_v = \{v\alpha \mid \alpha \in \{0,1\}^\omega\}$ is a clopen set. Therefore, all basic open sets of CD are clopen sets. Recall that the sets of the type U_X, where $X \subset \{0,1\}^\star$ and $U_X = \bigcup_{v \in X} U_v$, range over all open subsets of CD. Also, note that CD itself and $\emptyset$ are clopen sets.

Lemma 6.10.8 *An open set U is clopen if and only if there exists a finite set $X \subset \{0,1\}^\star$ such that $U = U_X$.*

Proof. Assume that there exists a finite set $X \subset \{0,1\}^\star$ such that $U = U_X$. Note that if $v \leq w$, where $u, v \in \{0,1\}^\star$, then $U_w \subset U_v$. Therefore, we can assume that for no pair $v, w \in X$ do we have $v \leq w$. Let $k = max\{|v| \mid v \in X\}$. Consider the set $Y \subset \{0,1\}^\star$ defined as

$$Y = \{v \mid |u| = k \text{ and no prefix of } u \text{ is in } X\}.$$

Note that $Y \neq \emptyset$. It is easy to check that the complement of U is U_Y. Hence U_Y is open. Therefore, U_X is a clopen set.

Now assume that U is a clopen set. We need to show that for some finite set X we have $U = U_X$. Take an element $\alpha \in U$. Then there exists a basic open set U_x such that $U_x \subset U$ and $\alpha \in U_x$. Let $x_1 \leq x_2 \leq \cdots \leq x_n$ be all prefixes of x. Among these prefixes take the x_i such that $U_{x_i} \subset U$ but $U_{x_{i-1}} \not\subset U$. Denote this x_i by $x(\alpha)$. Now set

$$X = \{x(\alpha) \mid \alpha \in U\}.$$

We claim that X is a finite set. Assume X is not a finite set. Consider the set $X' = \{y \mid y \leq x(\alpha) \text{ for some } x \in X\}$. Then X' is an infinite finitely branching tree. By König's lemma X' has an infinite path, say β. Clearly, no element of β belongs to X'. By the definition of β for any $x \in \beta$ there exists an $\alpha \in \{0,1\}^\omega$ such that $x\alpha \in U$. Note also that $\beta \notin U$. Now the complement of U is an open set. Hence there exists an x such that $U_x \subset CD \setminus U$ and $\beta \in U_x$. But as we noted, $x\alpha \in U$ for some $\alpha \in \{0,1\}^\omega$. Contradiction. We conclude that X is a finite set. Moreover, $U = U_X$. The lemma is proved.

Definition 6.10.13 *The set B_{CD} is the set of all clopen sets of CD.*

The next lemma shows that the set of all clopen sets is an atomless Boolean algebra.

Lemma 6.10.9 *The set B_{CD} of all clopen sets of CD forms an atomless countable Boolean algebra.*

Proof. Since every clopen set is of the form U_X for some finite $X \subset \{0,1\}^\star$, we see that the set of all clopen sets is countable. Clearly, the union, intersection and the complements of clopen sets are clopen sets. Also $\emptyset$ and CD are clopen sets. Hence all the set of all clopen sets is a Boolean algebra. We need to show that the Boolean algebra $\mathcal{B}_{CD}$ of all clopen sets is atomless. Let U be a clopen set. Then $U = U_X$ for some finite X. We can assume that for no pair $v, w \in X$ do we have $v \leq w$. Let $y \in \{0,1\}^\star$ be such that some proper prefix x of y is in X. Then U_y is a proper subset of U_X, and U_y is clopen. Hence $\mathcal{B}_{CD}$ is an atomless Boolean algebra. The lemma is proved.

Lemma 6.10.10 *For any ideal I of $\mathcal{B}_{CD}$ the set $V = \bigcup_{U \in I} U$ is an open set. Moreover, for any open set U in CD the set $\{V \in \mathcal{B}_{CD} \mid V \subset U\}$ is an ideal.*

Proof. For any ideal I, the set $V = \cup_{U \in I} U$ is clearly an open set. The second part of the lemma can be easily checked using the definition of ideal. The lemma is proved.

Now we define the language L_{BA} of all Boolean algebras. The language L_B contains individual variables $x, y, z, \ldots$, that are intended to run over elements of Boolean algebras, the operation symbols $\vee, \wedge, \tilde{}$ for representing the Boolean operations, constant symbols **0** and **1**, logical connectives $\&, \bigvee, \neg, \rightarrow$, and set variables $I_1, I_2, I_3, \ldots$ that are intended to run over ideals of Boolean algebras. The language contains quantifiers $\exists, \forall$ that can be applied to the individual as well as to the set variables. The language also has the symbol $\in$ for representing membership. Formulas and sentences of this language are defined in a natural way. Now we give the following definition.

Definition 6.10.14 *The theory of Boolean algebras Th(BA) in the language L_{BA} is the set of all sentences of the language that are true in all countable Boolean algebras.*

Our goal is to show that the theory *Th*(*BA*) is decidable. In order to show that *Th*(*BA*) is decidable we need to recall the structure $(CD, \preceq)$. In this structure, for all $\alpha, \beta \in CD$, we have $\alpha \preceq \beta$ if and only if there exists a w that is a finite prefix of both α and β such that $w0 \in \alpha$ and $w1 \in \beta$. The language L corresponding to the structure $(CD, \preceq)$ contains **individual variables** $x, y, z, \ldots$, that are intended to run over elements of CD, the symbol $\preceq$ representing the order on CD, logical connectives $\&, \bigvee, \neg, \rightarrow$, and set variables of two types. The first type of set variables are $C_1, C_2, C_3, \ldots$ and range over closed subsets of CD; the second type of set variables are $D_1, D_2, D_3, \ldots$ and range over F_σ-subsets of CD. The language contains quantifiers $\exists, \forall$ that can be applied to the individual as well as to the set variables of both types. The language also has symbols $\in$ for representing membership. Theorem 6.9.6 states that the theory *Th*(*CD*) of Cantor's discontinuum in this language L is decidable.

Here now is our last theorem of this chapter.

Theorem 6.10.7 *The theory Th(BA) of all Boolean algebras is decidable.*

Proof. The proof is basically a corollary of Theorem 6.9.6. Indeed, consider the language L of the structure $(CD, \preceq)$. Consider the formula $clopen(C)$ of the language L which is

$$\exists C_1 \exists C_2 (\forall x (x \in C_1 \leftrightarrow x \in C) \& \forall y (y \in C_2 \leftrightarrow y \notin C_1)),$$

where $(\Phi \leftrightarrow \Psi)$ stands for $(\Phi \rightarrow \Psi) \& (\Psi \rightarrow \Phi)$. Note that C_1 and C_2 are variables for closed sets. Hence a set $C \subseteq CD$ makes the formula true if and only if C is a clopen set. Note that the operations of union $\cup$, intersection $\cap$, and complementation $\tilde{}$ for clopen sets are all definable in the language L. Consider the formula $open(D)$ defined as follows:

$$\forall x (x \in D \rightarrow \exists C (C \subset D \;\&\; clopen(C) \;\&\; x \in C).$$

Note that the variable D is a variable that runs over F_σ-subsets of CD. A subset D of CD satisfies the formula if and only if D is an open set of CD. Thus, the Boolean algebra $\mathcal{B}_{CD}$ of clopen subsets of CD (see Lemma 6.10.9) is definable in the language L. Moreover, by Lemma 6.10.10, the open sets of CD can be associated with the ideals of the Boolean algebra $\mathcal{B}_{CD}$. Now consider the Boolean algebra $\mathcal{B}_{CD}$ of clopen subsets of CD. There exists a formula $\sim (I, C_i, C_j)$ in the language L such that for all subsets $X, Y, Z \subset CD$, formula $\sim (X, Y, Z)$ is true in CD if and only if X is open, Y and Z are clopen subsets of CD and $Y \sim_X Z$. Recall that $\sim_X$ is the equivalence relation in the Boolean algebra $\mathcal{B}_{CD}$ defined by the ideal X.

Now by induction on the complexity of formulas we transform every formula Φ of the language L_{BA} into the formula $\Phi^{(t)}$. The transformation will be such that for all sentences Φ, the sentence Φ is true in all Boolean algebras if and only if $\Phi^{(t)}$ is true in $(CD, \preceq)$. Take an atomic formula $t = q$, where t, q are terms. Replace all variables x_i occurring in $t = q$ with variables C_i, the operation symbols $\vee, \wedge$, and $\tilde{}$ with $\cup, \cap$, and $\tilde{}$, respectively. Note that $\tilde{C} = CD \setminus C$ for all clopen sets C of CD. Let t' and q' be the resulting expressions. Then the transformed formula is $\forall D(open(D) \rightarrow \sim (D, t', q'))$.

Take an atomic formula $t \in I$. In the term t replace variables x_i with variables C_i, replace the symbols $\vee$, $\wedge$ and $\tilde{}$, with $\cup, \cap$, and $\tilde{}$, respectively. Let t' be the resulting expression. Now replace $t \in I$ with the formula $(open(D) \;\&\; t' \subseteq D)$.

If Φ is of the form $\Phi_1 \tau \Phi_2$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1$, then we set $\Phi^{(t)}$ to be $\Phi_1^{(t)} \tau \Phi_2^{(t)}$, where $\tau \in \{\vee, \&, \rightarrow\}$ or $\Phi = \neg\Phi_1^{(t)}$, respectively.

If Φ is any of the formulas $\forall x_i \Phi_1(x_i), \forall I_j \Phi_1(I_j)$, then $\Phi^{(t)}$ is

$$\forall C_i \forall D(open(D) \;\&\; clopen(C_i) \rightarrow \exists C_i (\sim (D, C_i, C_j) \;\&\; \Phi_1^{(t)}(C_j))$$

and

$$\forall D_j(open(D_j) \rightarrow \Phi_1^{(t)}(D_j)),$$

respectively. Similarly, if Φ is any of the formulas $\exists x_i \Phi_1(x_i), \exists I_j \Phi_1(I_j)$, then we replace Φ with

$$\forall D(open(D) \rightarrow \exists C_i \exists C_j \sim (D, C_i, C_j) \;\&\; \Phi_1^{(t)}(C_j)),$$

and

$$\exists D_j(open(D_j) \;\&\; \Phi_1^{(t)}(D_j)),$$

respectively. Now the reader can check that for all sentences Φ, we have $\Phi \in Th(BA)$ if and only if $\Phi^t \in S2S$. The theorem is proved.