Topics in Logic and Foundations: Spring 2004

Stephen G. Simpson

First Draft: April 30, 2004

This Draft: November 1, 2005

The latest version is available at

http://www.math.psu.edu/simpson/notes/.

Please send corrections to <simpson@math.psu.edu>.

This is a set of lecture notes from a 15-week graduate course at the Pennsylvania State University taught as Math 574 by Stephen G. Simpson in Spring 2004. The course was intended for students already familiar with the basics of mathematical logic. The course covered some topics which are important in contemporary mathematical logic and foundations but usually omitted from introductory courses at Penn State.

These notes were typeset by the students in the course: Robert Dohner, Esteban Gomez-Riviere, Christopher Griffin, David King, Carl Mummert, Heiko Todt. In addition, the notes were revised and polished by Stephen Simpson.

Contents

Chapter 1

Computability in core mathematics

1.1 Review of computable functions

For the sake of completeness, we will review the basic definitions from elementary recursion theory that will be necessary for our study of computability in core mathematics. We write $\omega = \{0, 1, 2, \ldots\}$ for the set of nonnegative integers. For $k \geq 1$, ω^k denotes the set of sequences of elements of ω of length k.

1.1.1 Register machines

Recall that a register machine is composed of an infinite number of registers, usually denoted by bins as shown in Figure 1.1. Each register holds a natural number. Register machines execute register machine programs. Register machine programs are flow-charts of four types of instructions shown in Figure 1.2. The *increment* instruction adds 1 to the value of the register specified in the instruction. Program flow then continues along the out arrow. The *decrement* instruction checks to see if the value in the specified register is greater than zero, if not the program continues execution along the arrow labeled e. Otherwise, the value in the specified register is decremented and the program continues execution along the unlabeled arrow. For every program there is one and only one *start* instruction. The *stop* instruction halts program execution. There may be many stop instructions in a program flow chart. A simple program is shown in Figure 1.2.

Let $\mathcal{P}$ denote a register machine program. When we run $\mathcal{P}$ with inputs $x_1, \ldots, x_k$, we assume that these inputs are initially placed into the registers $R_1, \ldots, R_k$ and that all other registers are empty. If and when $\mathcal{P}$ halts (i.e., completes its execution), the output is stored in register R_{k+1}. We denote a run of a register machine with program $\mathcal{P}$ on inputs $x_1, \ldots, x_k$ by $\mathcal{P}(x_1, \ldots, x_k)$. The k-place number-theoretic function computed by $\mathcal{P}$ is denoted $f_{\mathcal{P}}^{(k)}$. Thus

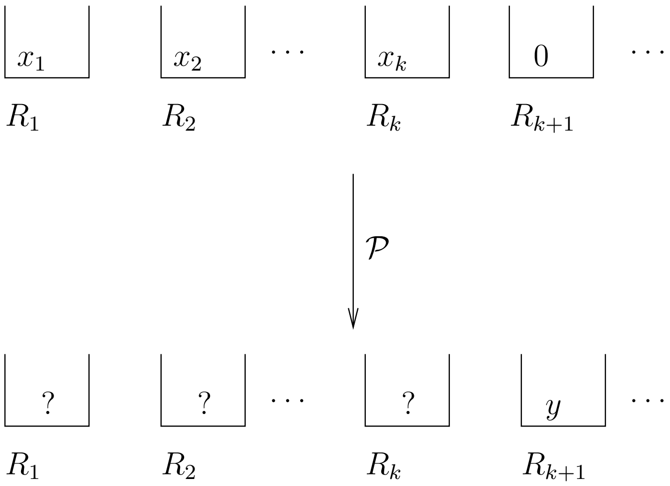

Figure 1.1: A register machine computing $y = f_{\mathcal{P}}^{(k)}(x_1, \ldots, x_k)$. Here y is the result stored in register R_{k+1} after running $\mathcal{P}(x_1, \ldots, x_k)$.

$f_{\mathcal{P}}^{(k)}(x_1, \ldots, x_k) = y$ means that y is the output after running $\mathcal{P}$ with inputs $x_1, \ldots, x_k$. For a more detailed review of register machines and register machine programs, see [18].

Each register machine program $\mathcal{P}$ can be assigned a natural number $\#(\mathcal{P})$, in a recursive one-to-one way. This number is called the *Gödel number* of $\mathcal{P}$, or an *index* of $f_{\mathcal{P}}^{(k)}$. We write $y = \varphi_e^{(k)}(x_1, \ldots, x_k)$ to indicate that the program with Gödel number e with inputs $x_1, \ldots, x_k$ eventually halts with output y.

1.1.2 Recursive and partial recursive functions

Definition 1.1.1 (recursive function). A k-place function $f : \omega^k \to \omega$ is *computable* (equivalently, *recursive*) if there exists a register machine program $\mathcal{P}$ that computes it, i.e., for all $x_1, \ldots, x_k \in \omega$, $\mathcal{P}(x_1, \ldots, x_k)$ eventually halts with $y = f(x_1, \ldots, x_k) = f_{\mathcal{P}}^{(k)}(x_1, \ldots, x_k)$ as the output.

A *k-place partial function* is a function from a subset of ω^k to ω. We write $\psi : \omega^k \xrightarrow{P} \omega$ to indicate that ψ is a k-place partial function. The fact that a partial function ψ may not be defined for some arguments $x_1, \ldots, x_k \in \omega$ leads us to consider expressions that may or may not have a numerical value. Let E be such an expression. We say that E *is defined* if E has a numerical value, and in this case, we write $E\downarrow$. Otherwise, we say that E *is undefined* and we write $E\uparrow$. Furthermore, we write $E_1 \simeq E_2$ to mean that E_1 and E_2 are either both defined and equal or both undefined. The symbol $\simeq$ is called *strong equality*.

Definition 1.1.2 (partial recursive function). A partial function $\psi : \omega^k \xrightarrow{P}$

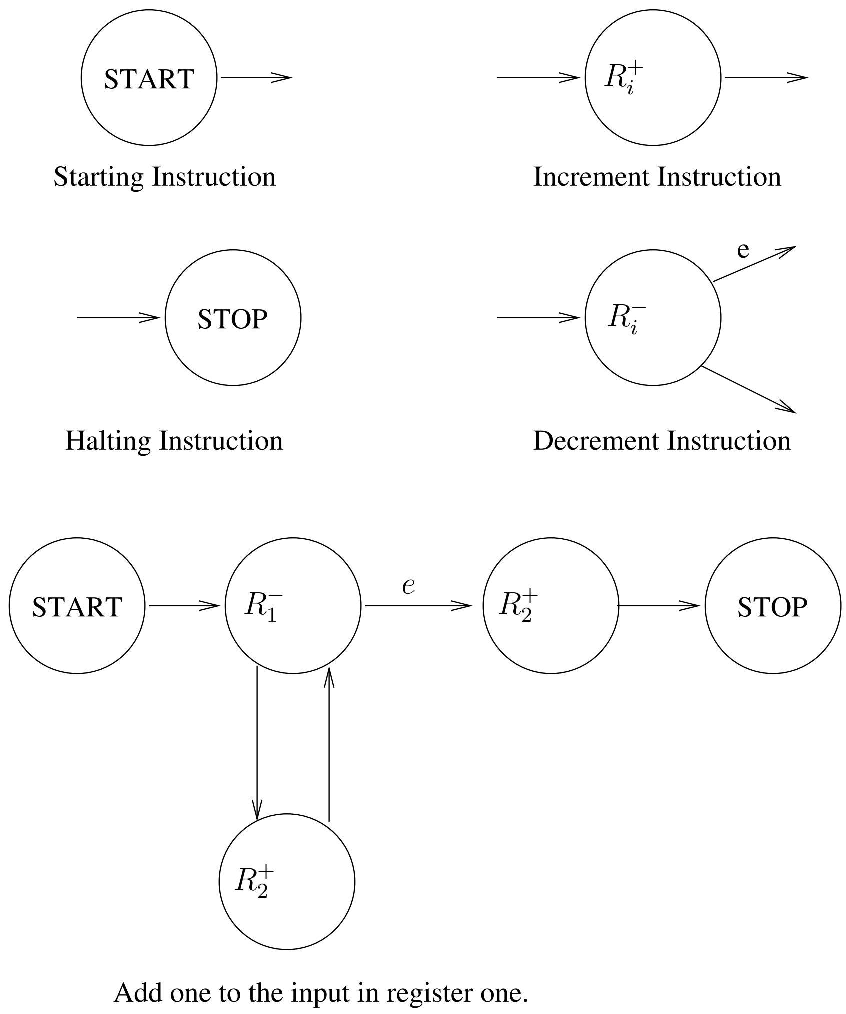

Figure 1.2: The four register machine instructions and a sample program.

ω is *partial recursive* if and only if there is a register machine program $\mathcal{P}$ such that $\forall x_1, \ldots, x_k\, \psi(x_1, \ldots, x_k) \simeq f_{\mathcal{P}}^{(k)}(x_1, \ldots, x_k)$.

Definition 1.1.3. A set (or relation) $R \subseteq \omega^k$ is said to be *computable* (or equivalently *recursive*) if the characteristic function $\chi_R : \omega^k \to \{0, 1\}$ of R is a computable function.

Definition 1.1.4. A set $A \subseteq \omega$ is said to be *recursively enumerable* (abbreviated r.e.) if it is the range of a partial recursive function.

By a *problem* we mean a set $A \subseteq \omega$. We often can use Gödel numberings to express problems in other areas of mathematics in this more formal sense. We will see an example of this when we discuss the *word problem* for groups and semigroups. A problem is said to be *solvable* if and only if it is a recursive set, otherwise *unsolvable*. The classification of unsolvable problems is an important theme in recursion theory.

1.1.3 The μ-operator

Let $R \subseteq \omega^{k+1}$ be a computable relation. Suppose we wish to search for the least $y \in \omega$ such that $R(x_1, \ldots, x_k, y)$ holds. We write this as

$$\psi(x_1, \ldots, x_k) \simeq \mu y\, R(x_1, \ldots, x_k, y).$$

The operator μ is called the *minimization operator* or the *least number operator* and can be used to create partial recursive functions from recursive sets. Since our search for a y satisfying $R(x_1, \ldots, x_k, y)$ may not halt, $\psi(x_1, \ldots, x_k)$ may be undefined.

For example, if R is a recursive subset of $\omega \times \omega$ and for each m there is an n such that $\langle m, n\rangle \in R$, then the function $m \mapsto \mu n\, \langle m, n\rangle \in R$ is recursive.

1.2 Introduction to computable algebra

1.2.1 Computable groups

Definition 1.2.1. A *computable group* is a group $\langle G, \cdot\rangle$ whose elements form a recursive subset of ω and whose multiplication is a recursive function.

Proposition 1.2.2. Let $\langle G, \cdot\rangle$ be a computable group. Then the function $a \mapsto a^{-1}$ is computable.

Proof. To compute a^{-1} for an element $a \in G$, we first find 1_G, then search for the unique element b such that $a \cdot b = 1_G$. That is, $a^{-1} = \mu b\, (a \cdot b = 1_G)$. □

Remark 1.2.3. If $\langle G, \cdot_G\rangle$ is a computable group, the identity element 1_G can be defined as the unique $a \in G$ such that $a \cdot a = a$. Therefore the function $a \mapsto a^{-1}$ from Proposition 1.2.2 is uniformly computable given indices for G and $\cdot_G$.

Remark 1.2.4. One could study the notion of a "primitive recursive group." The corresponding version of Proposition 1.2.2 would not automatically hold for primitive recursive groups, because $a \mapsto a^{-1}$ might not be primitive recursive. Therefore, we would have to assume this separately, if desired.

Remark 1.2.5. Many groups which arise in practice can be identified with computable groups. This can be done by means of Gödel numbering.

Examples 1.2.6.

1. The additive group $\mathbb{Q}$ of rational numbers is (canonically isomorphic to) a computable group. Each $r \in \mathbb{Q}$ can be identified with a unique pair of integers $\langle a, b \rangle$, with a, b relatively prime, $b > 0$, $r = a/b$. Assuming a suitable Gödel numbering for $\mathbb{Z}$, we can code $\mathbb{Q}$ as the set

$$\{2^{\#(a)} 3^{\#(b)} \mid a, b \in \mathbb{Z}, (a, b) = 1, b > 0\}.$$

   There is a computable multiplication function on this set which gives it the group structure of the additive group of rationals.

2. The multiplicative group of nonzero rational numbers is (canonically isomorphic to) a computable group.

3. The group $\mathrm{GL}_2(\mathbb{Q})$, consisting of invertible 2×2 matrices of rationals under matrix multiplication, is (canonically isomorphic to) a computable group. We choose a simple Gödel numbering scheme for matrices:

$$\# \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2^{\#(a)} 3^{\#(b)} 5^{\#(c)} 7^{\#(d)}$$

   where $a, b, c, d \in \mathbb{Q}$. There is a computable multiplication function which gives the computable set of such Gödel numbers with $ad - bc \neq 0$ the structure of $\mathrm{GL}_2(\mathbb{Q})$.

Remark 1.2.7. Clearly, every computable group is countable. Because there are $2^{\aleph_0}$ countable groups but only $\aleph_0$ indices of computable groups, there must be a noncomputable countable group. While there are concrete examples of noncomputable countable groups, none of the known examples is mathematically natural.

We note that many familiar algebraic constructions preserve computability. For example, the direct product of two computable groups is computable.

For another example, let us review the definition of a *quotient group*. Let $\langle G, \cdot \rangle$ be a group, and let N be a subgroup of G. Define an equivalence relation $\equiv_N$ on G by letting $a \equiv b$ iff $a \cdot b^{-1} \in N$. For $a \in G$, we let $[a]$ denote the equivalence class of a in $G/\equiv_N$. When N is a normal subgroup, the equivalence classes form a group under the operation $[a] \cdot [b] = [a \cdot b]$. This is the quotient group G/N.

Theorem 1.2.8. If $\langle G, \cdot \rangle$ is a computable group and $N \subseteq G$ is a computable normal subgroup of G, then the quotient group G/N is (canonically isomorphic to) a computable group.

Proof. Let $\langle G, \cdot \rangle$ and N be as above. Note that the characteristic function of $\equiv_N$ is computable. Let $h : G \to G$ be the function such that for $a \in G$, $h(a)$ is the least $b \in G$ such that $b \equiv_N a$. This computable function selects an element from each equivalence class of $G/\equiv_N$ (see Proposition 1.2.9).

We can use h to create a computable group isomorphic to G/N. Let $H = h(G)$; this set is recursive, because $b \in H \iff b \in G \wedge h(b) = b$. Define a multiplication function $\cdot_H$ on H by letting $c_1 \cdot_H c_2 = h(c_1 \cdot c_2)$. This multiplication function is also computable. It can be verified that $\langle H, \cdot_H \rangle$ is a computable group isomorphic to G/N. □

The previous construction is a special case of:

Proposition 1.2.9. Let X be a computable set and let $\equiv$ be a computable equivalence relation on X. Then there is computable selector for $X/\equiv$ whose range is a computable subset of X. That is, there is a computable function h such that for all $a, b \in X$, $a \equiv h(a)$ and $a \equiv b \iff h(a) = h(b)$.

Proof. Define $h(a)$ to be the least element of X which is $\equiv$-equivalent to a. It can be seen that $n \in h(X) \iff n \in X \wedge h(n) = n$. □

Remark 1.2.10. Let G_1 and G_2 be two computable groups, and let ϕ be a computable homomorphism from G_1 to G_2. Then the kernel of ϕ is a computable normal subgroup of G_1. This group has as its domain the set $N = \{a \in G_1 \mid \phi(a) = 1_{G_2}\}$ and inherits the multiplication operation from G_1. The image of ϕ is clearly an r.e. subgroup of G_2. This image may not, however, be computable. See Exercise 1.2.11.

Exercise 1.2.11. Construct computable groups G_1, G_2 and a computable monomorphism $\phi : G_1 \to G_2$ such that the image $\phi(G_1)$ is not computable.

Exercise 1.2.12. Let $\langle G, \cdot \rangle$ be an r.e. group. That is, let G be an r.e. subset of ω and let $\cdot : G \times G \to G$ be a partial recursive function whose domain is $G \times G$ and which makes G a group. Show that there is a computable group H which is isomorphic to G via a computable isomorphism $\phi : H \to G$ with range G.

1.2.2 Computable fields

Definition 1.2.13. A *computable field* (*computable ring*) is a field (ring) whose elements form a recursive subset of ω and whose addition and multiplication functions are computable.

Remark 1.2.14. For any computable ring, the additive inverse function $a \mapsto -a$ is computable. For any computable field, the multiplicative inverse function $a \mapsto 1/a$ is computable.

Proposition 1.2.15. If F is a computable field, then the polynomial ring $F[x]$ is (canonically isomorphic to) a computable ring.

Again, many field constructions preserve computability.

For example, suppose that F is a field and $p(x)$ is a polynomial in $F[x]$. There is an equivalence relation $\equiv_{p(x)}$ on $F[x]$ such that $q(x) \equiv_{p(x)} r(x)$ iff $p(x)$ divides $q(x) - r(x)$. The equivalence classes form a commutative ring with operations $[q(x)] + [r(x)] = [q(x) + r(x)]$ and $[q(x)] \cdot [r(x)] = [q(x)r(x)]$. If $p(x)$ is irreducible in $F[x]$, then the equivalence classes form a field.

Lemma 1.2.16. Let F be a computable field. The set

$$\{\langle p(x), q(x)\rangle \in F[x] \times F[x] \mid p(x) \text{ divides } q(x)\}$$

is computable.

Proof. To decide whether a pair $\langle p(x), q(x)\rangle$ is in the set, apply the standard long division algorithm for polynomials, and test whether the remainder is zero. $\square$

Theorem 1.2.17. Let $\langle F, +, \cdot\rangle$ be a computable field, and let $p(x)$ be a polynomial in $F[x]$. Then the quotient ring $F[x]/(p(x))$ is (isomorphic to) a computable ring. If $p(x)$ is irreducible, we have a computable field.

Proof. By Lemma 1.2.16, the equivalence relation $\equiv_{p(x)}$ is computable. Therefore, it has a computable selector function h whose range R is a recursive set. For $a, b \in R$, define two computable function from $H \times H$ to H: $a +_R b = h(a+b)$ and $a \cdot_R b = h(a \cdot b)$. It can be shown that $\langle R, +_R, \cdot_R\rangle$ is a computable ring isomorphic to $F[x]/(p(x))$. $\square$

1.3 Finitely presented groups and semigroups

1.3.1 Free groups

Let $A = \{a_1, \ldots, a_n\}$ be a finite set of symbols, and let $A^{-1} = \{a_1^{-1}, \ldots, a_n^{-1}\}$ be a second set of symbols, disjoint from A.

Definition 1.3.1. A *word* is a finite sequence $w = x_1 x_2 \cdots x_k$, where $x_i \in A \cup A^{-1}$ for all $i \leq k$. The empty sequence is a word, denoted 1.

Let V_n be the set of all words on $A \cup A^{-1}$. We can define a multiplication on words by *concatenation*, i.e., juxtaposition. That is, if u and v are two words on A, then the uv is a word on A when we simply concatenate the symbols of u followed by the symbols of v.

A word w on A is said to be *reduced* if a_i and a_i^{-1} are never adjacent within w. By canceling adjacent inverses, every word u can be transformed to a unique reduced word $w = r(u)$. We call this reduced word the *canonical form* of u. Clearly the function r is recursive, since we can easily compute the unique canonical form of any word. Using r, we may define a multiplication on reduced words. If w and w' are reduced words, we define $w \cdot w' = r(ww')$. Let $\equiv$ be the equivalence relation on W_n with $u \equiv v$ if and only if $r(u) = r(v)$. Then we have the following easy theorem, whose proof can be found in [12, Theorem 11.1]:

Theorem 1.3.2. The set $V_n/\equiv$ with the operation $\cdot$ is a group.

Definition 1.3.3. The *free group on n generators* (also called the *free group of rank n*) is the group $F_n = (V_n/\equiv, \cdot)$.

Proposition 1.3.4. The free group F_n is computable.

Proof. It is easy to see that F_n is a computable group, by coding the generators of F_n and using these codes to form codes for words. It is then trivial to check whether a given code for a word is reduced. We simply check whether or not two inverses are adjacent in the word. □

1.3.2 Group presentations and word problems

A group G is said to be *finitely generated* if it contains a finite set $X = \{g_1, \ldots, g_n\}$ of generators. Then it is easy to see that there is a homomorphism ϕ from F_n to G via $\phi(a_i) = g_i$, since G is generated by the g_i. If $K = \ker(\phi)$, then we have an isomorphism from F_n/K onto G. The normal subgroup K is called the set of *relations* on the generators $g_1, \ldots, g_n$.

Suppose R is a subset of F_n. Then the *normal subgroup generated by* R is the smallest normal subgroup of F_n containing R. If K is the normal subgroup generated by R, then we say that G is *defined by the relations* in R, since we have $G \cong F_n/K$. If R is finite, we say that G is a *finitely presented group.*

Remark 1.3.5. Note that though K may be the normal subgroup generated by a finite set R, it does not follow that K is a finitely generated group. Instead, K is generated by the set of conjugates of elements of R, which may be infinite.

In general, finitely presented groups are written as a pair $\langle A; R\rangle$, where A is the set of generators of the group and R is a finite set of words generating the kernel of the homomorphism ϕ (as a normal subgroup); i.e., the words that can be canceled to 1.

Example 1.3.6. We will show that the group of isometries of a square, D_4, is a finitely presented group. Let ρ be a 90° counter-clockwise rotation of the points of the square and let ϕ be a flip of a square along one of its lines of symmetry as shown in Figure 1.3. Then the group of symmetries of the square is the finitely presented group:

$$\langle \rho, \phi; \rho^4 = \phi^2 = \phi\rho\phi\rho = 1\rangle.$$

We can see that four ninety degree rotations will return a square to its starting position. Likewise, two flips will return a square to its starting position. Finally, a rotation followed by a flip followed by another rotation and another flip will also return a square to its original position.

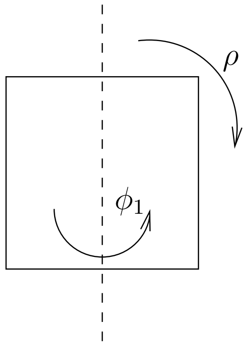

Figure 1.3: The symmetries of a square.

Definition 1.3.7. A finitely presented group G is said to have a *solvable word problem* if there exists a computable normal group N of F_n such that $G \cong F_n/N$. In general, the *word problem* for $G \cong F_n/N$ is the problem of deciding whether a given word in F_n belongs to N or not.

Remark 1.3.8. Let G be finitely presented group. An equivalent problem to the word problem for G is the set $\{(w_1, w_2) \in F_n \times F_n \mid \phi(w_1) = \phi(w_2)\}$. Thus G has a solvable word problem if and only if we can decide, given two words w_1 and w_2 over the generators of G and their inverses, whether or not $w_1 = w_2$ in G.

Example 1.3.9. The finitely presented group

$$G = \langle a, b; a^2 = b^3 = aba^{-1}b^{-1} = 1 \rangle$$

has solvable word problem. To see this, note that any word consisting of a's and b's can be transformed into a word having a's raised only to the power 1, since we have the relation $a^2 = 1$. Along the same line, we can transform any word into an equivalent word having only b's raised to powers 1 and 2. Finally, the relation $aba^{-1}b^{-1} = 1$ shows us that a's and b's commute. Therefore, we may transform all our words into words of the form $a^{e_1}b^{e_2}$, where $e_1 = 0, 1$ and $e_2 = 0, 1, 2$. The form $a^{e_1}b^{e_2}$ is called the *normal form* of the group elements. For example, consider the word: a^3babba^4. This word can be written as $abab^2$, since $a^3 = a^2a = a$ and $bb = b^2$ and $a^4 = a^2a^2 = 1$. Commuting the a's and b's we have $aabb^2$, which is $a^2b^3 = 1$, so this word is in the image of the kernel of the homomorphism taking the free group F_2 to G.

Proposition 1.3.10. The solvability of the word problem for a finitely presented group G does not depend on the choice of generators.

Proof. Suppose that a group G is generated by the set $A = \{a_1, \ldots, a_n\}$ and also by the set $B = \{b_1, \ldots, b_m\}$. Then we can express each element of A as a product of elements of B; i.e., let $a_i = w_i$ where w_i is a product of elements of

B. Then a word $v = \prod_{j=1}^{k} a_{i_j}^{e_j}$ is 1 if and only if $\prod_{j=1}^{k} w_{i_j}^{e_j} = 1$. Thus it follows that the word problem for G generated by A is reducible to the word problem of G generated by B. A similar argument shows the the word problem for G when generated by B can be reduced to the word problem for G when generated by A. Therefore, the two problems are equivalent and hence the choice of generators does not matter. □

Exercise 1.3.11. Show that a finitely generated group G has a solvable word problem if and only if G is isomorphic to a recursive group.

Theorem 1.3.12 (Boone/Novikov). There is a finitely presented group with an unsolvable word problem.

Proof. The proof of this theorem is complex and involves group theory beyond the scope of these notes. Rotman [12] gives a complete proof in his book, using Turing machines as the system of computation. □

Corollary 1.3.13. There is a countable group which is not isomorphic to any computable group.

Proof. Apply Exercise 1.3.11 to a countable group G with an unsolvable word problem. If G were isomorphic to a recursive group, then G would have a solvable word problem. □

Exercise 1.3.14. Show that the group

$$\langle a, b, c; a^2 = aba^{-1}b^{-1} = b^5 = c^7 \rangle$$

has a solvable word problem.

1.3.3 Finitely presented semigroups

Definition 1.3.15. A *semigroup* consists of a set S with an associative binary operation. A semigroup $\langle S, \cdot_S \rangle$ is a *computable semigroup* if $S \subseteq \omega$ is a recursive set and $\cdot_S : S \times S \to S$ is a partial recursive function.

Definition 1.3.16. The *free semigroup* on n generators $a_1, \ldots, a_n$ consists of the set W_n of all words (finite sequences) on $a_1, \ldots, a_n$ with the operation of concatenation.

Definition 1.3.17. Let R be a subset of $W_n \times W_n$. We define an equivalence relation $\equiv_R$ on W_n. For $w, w' \in W_n$, let $w \equiv_R w'$ if and only if there exists a finite sequence $\langle w_i \mid i \leq n \rangle$ such that $w = w_0$, $w_n = w'$, and for each $i < n$ we have $w_i = urv$ and $w_{i+1} = ur'v$ for some (r, r') or $(r', r) \in R$. The semigroup W_n/R is the set of equivalence classes $W_n/{\equiv_R}$ with the operation $\cdot$ given by $[u]_R \cdot [v]_R = [uv]_R$.

Definition 1.3.18. A *finitely presented semigroup* is a semigroup of the form W_n/R, where W_n is a free semigroup on a finite number of generators, and R is a finite subset of $W_n \times W_n$.

1.3.4 Unsolvability of the word problem for semigroups

The *word problem* for a finitely generated semigroup $S = W_n/R$ is the set

$$\{(w, w') \in W_n \times W_n \mid w \equiv_R w'\}.$$

Just as for finitely generated groups, we can show that the degree of unsolvability of a finitely generated semigroup does not depend on the choice of generators.

Theorem 1.3.19. There is a finitely presented semigroup with unsolvable word problem.

Proof. We follow the exposition of the first few sections of Chapter 12 of Rotman's group theory textbook [12], with the difference that Rotman uses Turing machines while we use register machines.

Our construction is based on the following fact. There is a register machine program $\mathcal{P}$ which computes the partial recursive function $2^x \mapsto 0 \cdot \varphi_x^{(1)}(x)$, and such that $\mathcal{P}$ uses only two registers, R_1 and R_2. This follows easily from Exercise 5.9 in Simpson's lecture notes [18].

Note that $\{x \mid \mathcal{P}(x) \text{ halts}\}$ is nonrecursive. In other words, given x, the problem of deciding whether $\mathcal{P}$ halts if started with x in R_1 and with R_2 empty, is unsolvable. Furthermore, we may safely assume that if $\mathcal{P}(x)$ halts then it halts with both registers empty.

The idea of our construction is to encode the action of $\mathcal{P}$ into the word problem of a semigroup S.

Let $I_1, \ldots, I_l$ be the instructions of $\mathcal{P}$. As usual, I_1 is the first instruction executed, and I_0 is the halt instruction. Our semigroup S will have $l + 3$ generators $a, b, q_0, q_1, \ldots, q_l$. If R_1 and R_2 contain x and y respectively, and if I_m is about to be executed, then we represent this state as a word $ba^x q_m a^y b$. Thus a serves as a counting token, and b serves as an end-of-count marker. For each $m = 1, \ldots, l$, if I_m says "increment R_1 and go to I_{n_0}", we represent this as a production $q_m \to aq_{n_0}$ or as a relation $q_m = aq_{n_0}$. If I_m says "increment R_2 and go to I_{n_0}", we represent this as a production $q_m \to q_{n_0}a$ or as a relation $q_m = q_{n_0}a$. If I_m says "if R_1 is empty go to I_{n_0} otherwise decrement R_1 and go to I_{n_1}", we represent this as a pair of productions $bq_m \to bq_{n_0}$, $aq_m \to q_{n_1}$, or as a pair of relations $bq_m = bq_{n_0}$, $aq_m = q_{n_1}$. If I_m says "if R_2 is empty go to I_{n_0} otherwise decrement R_2 and go to I_{n_1}", we represent this as a pair of productions $q_m b \to q_{n_0} b$, $q_m a \to q_{n_1}$, or as a pair of relations $q_m b = q_{n_0} b$, $q_m a = q_{n_1}$. Thus the total number of productions or relations is $l^+ + 2l^-$, where $l = l^+ + l^-$ and l^+ is the number of increment instructions and l^- is the number of decrement instructions. Let S be the semigroup described by these generators and relations.

We claim that for all x, $ba^x q_1 b = bq_0 b$ in S if and only if $\mathcal{P}(x)$ halts. The "if" part is clear. For the "only if" part, assume that $ba^x q_1 b = bq_0 b$ in S. This implies that there is a sequence of words $ba^x q_1 b = w_0 = \cdots = w_n = bq_0 b$ where each w_{i+1} is obtained from w_i by a forward or backward production. We claim that the backward productions can be eliminated. In other words, if there are any backward productions, we can replace the sequence $w_0, \cdots, w_n$ by a shorter sequence. This is actually obvious, because if there is a backward production then there must be one which is immediately followed by a forward production, and these two must be inverses of each other, because $\mathcal{P}$ is deterministic. Thus we see that $ba^x q_1 b = bq_0 b$ via a sequence of forward productions. This implies that $\mathcal{P}(x)$ halts. Our claim is proved.

This completes the proof of the theorem. □

1.4 More on computable algebra

1.4.1 Splitting algorithms

We continue our discussion of computable fields. We give an example of a recursive embedding of a computable field into its algebraic closure whose range is not computable.

Corollary 1.4.1. If F is a computable field, then all simple extensions of F are computable.

Proof. If $F(\alpha)$ is a simple extension of F, then $F(\alpha)$ is either an algebraic or transcendental extension. If it is algebraic, then Theorem 1.2.17 applies. If it is transcendental, then $F(\alpha) \cong F(x)$, the field of 1-place rational functions over F, with $\alpha \mapsto x$. Thus the field operations of $F(\alpha)$ are computable in terms of those on F. □

Recall that an algebraic closure of a field F is an algebraic extension of F, denoted $\widetilde{F}$, such that every polynomial in $F[x]$ splits into a product of linear factors in $\widetilde{F}[x]$.

Theorem 1.4.2 (Rabin [10]). If F is a computable field, then $\widetilde{F}$, the algebraic closure of F, is computable and there is a computable embedding, $\iota : F \to \widetilde{F}$, of F into its algebraic closure.

Remark 1.4.3. A non-trivial problem in algebra is to determine whether a given polynomial is irreducible or not (cf. Eisenstein's irreducibility criterion). If the set of irreducible polynomials over a computable field is recursive, then the field is said to have a *splitting algorithm*. The following theorem characterizes those fields with splitting algorithms.

Theorem 1.4.4. A computable field has a splitting algorithm if and only if it is recursively isomorphic to a computable subfield of its algebraic closure.

Proof. Let F be a computable field and let $\iota : F \to \widetilde{F}$ be a recursive isomorphism of F into its algebraic closure and $p(x) \in F[x]$ nonconstant. By Rabin's theorem, $\widetilde{F}$, the algebraic closure of F, is computable. Thus the finite set of linear factors of $\iota(p)$ is recursive. Test whether any product of a proper subset of these linear factors is in $F[x]$. If so, p is reducible, otherwise p is irreducible. Thus F has a splitting algorithm.

For the converse, assume F has a splitting algorithm and let $\iota : F \to \widetilde{F}$ be a recursive isomorphism of F into its algebraic closure. Let $y \in \widetilde{F}$. To determine whether $y \in \iota(F)$, find the least polynomial $p \in \{f \in F[x] \mid f \text{ irreducible}\}$ such that y is a root of $\iota(p)$. If $\iota(p)$ is linear, then $y \in \iota(F)$, otherwise not. Thus the image of F under ι is computable. □

Remark 1.4.5. Many common computable fields have splitting algorithms: $\mathbb{Q}, \mathbb{Q}(\alpha), \ldots, \widetilde{\mathbb{Q}}$. The splitting algorithm for $\mathbb{Q}$ is given in van der Wearden's book [20]. However, not all fields have splitting algorithms as the next example illustrates.

Example 1.4.6. We construct a computable field which does not have a splitting algorithm. Let $A \subseteq \omega$ which is recursively enumerable but not recursive. Let p_n, for $n = 0, 1, 2, \ldots$, be the enumeration of prime numbers in increasing order. The field $\mathbb{Q}(\sqrt{p_n} \mid n \in A)$ is recursively enumerable, and therefore recursively isomorphic to a computable field by a previous exercise. But

$$\{f(x) = x^2 - p_n \mid f(x) \text{ irreducible in } F[x]\}$$

is not recursive, otherwise A would be recursive. Hence, $\mathbb{Q}(\sqrt{p_n} \mid n \in A)$ does not have a splitting algorithm, and by the previous theorem this field is not computable.

1.4.2 Computable vector spaces

Definition 1.4.7. If V is a vector space over F where V is a computable abelian group, F is a computable field, and scalar multiplication is recursive, then V is a *computable vector space* over F.

Remark 1.4.8. There is an infinite dimensional computable vector space over $\mathbb{Q}$ with neither a recursive basis nor even a recursive infinite linearly independent subset.

1.5 Computable analysis and geometry

1.5.1 Computable real numbers

The class of computable reals consists of those real numbers for which there exists an algorithm for approximating them to any degree of accuracy. So not only must there be a recursive way of generating these approximations, but also the degree of accuracy must be a recursive function of the approximation as well. Thus the computable reals are those numbers such that the function giving the n^{th} digit of the decimal expansion is recursive. The following definition makes these statements precise.

Definition 1.5.1. A real number $x \in \mathbb{R}$ is computable is there exists a recursive sequence $\langle q_n \mid n \in \omega \rangle$ of rational numbers such that $x = \lim q_n$ and there exists a total recursive function f such that $\forall n \, \forall m \, (m > f(n) \Rightarrow |x - q_m| < 1/2^n)$.

Remark 1.5.2. Equivalently, $x \in \mathbb{R}$ is computable if and only if there is a recursive sequence of rationals $\langle q'_n \mid n \in \omega \rangle$ such that $\forall n \, |x - q'_n| < 1/2^n$. We can see this by taking $q'_n = q_{f(n)+1}$.

Remark 1.5.3. If x and y are computable real numbers, then so are $x + y, xy, x/y, x^y, e^x, \log x, \sin x, \sqrt{x}$, etc. In particular, the class of computable real numbers forms a real closed subfield of $\mathbb{R}$. Clearly, the class of computable reals is a proper subset of the reals numbers, since there are only countably many recursive functions and so there are only countably many computable reals. The next example gives a specific non-computable real number.

Example 1.5.4. There is a recursive bounded increasing sequence of rationals whose limit is a non-recursive real. Let $A \subseteq \omega$ which is recursively enumerable but not recursive. Let $f : \omega \to \omega$ be a one-to-one recursive function whose range is A. Consider the sequence $\langle q_n \mid n \in \omega \rangle$ where

$$q_n = \sum_{i=0}^{n} \frac{1}{2^{f(i)}} < 2.$$

This is a bounded increasing sequence of real numbers so it converges. But the limit $x = \lim q_n = \sum_{n \in A} 1/2^n$ is a real number which is not computable, otherwise χ_A would be recursive.

Recall that under the usual metric an open ball in $\mathbb{R}^n$ with center $a = \langle a_1, \ldots, a_n \rangle$ and radius r is the set

$$B(a, r) = \{x \in \mathbb{R}^n \mid \sqrt{(x_1 - a_1)^2 + \cdots + (x_n - a_n)^2} < r\}.$$

Definition 1.5.5. A set $U \subseteq \mathbb{R}^n$ is *effectively open* if

$$U = \bigcup_{i=0}^{\infty} B(a_i, r_i)$$

where $\langle a_i \mid i \in \omega \rangle$ is a recursive sequence of points in $\mathbb{Q}^n$ and $\langle r_i \mid i \in \omega \rangle$ is a recursive sequence of rational numbers.

Remark 1.5.6. The rational open balls (i.e., open balls with center in $\mathbb{Q}^n$ and rational radius) form a countable basis for the usual topology on $\mathbb{R}^n$. That is, every open set in $\mathbb{R}^n$ is a union of rational open balls.

Definition 1.5.7. A set $C \subseteq \mathbb{R}^n$ is *effectively closed* if its complement $\mathbb{R}^n \setminus C$ is effectively open.

1.5.2 Computable sequences of real numbers

Definition 1.5.8 (computable sequences). A sequence of real numbers $\langle x_n \rangle_{n \in \omega}$ is said to be *computable* if there exists a computable double sequence of rational numbers $\langle q_{nk} \rangle_{n,k \in \omega}$ such that $\forall n \, \forall k \, |x_n - q_{nk}| \le 1/2^k$.

Remark 1.5.9. If $\langle x_n \rangle_{n\in\omega}$ and $\langle y_n \rangle_{n\in\omega}$ are computable sequences of reals, then so is $\langle x_n + y_n \rangle$, etc.

Exercises 1.5.10. The following may help to explain why we do not choose to represent computable reals as recursive Dedekind cuts in $\mathbb{Q}$.

1. Show that $x \in \mathbb{R}$ is computable if and only if $\{q \in \mathbb{Q} \mid q < x\}$ is computable.

2. Give an example of a sequence of reals $\langle x_n \rangle_{n\in\omega}$ such that $\{(q,n) \mid q < x_n\}$ is computable but $\{(q,n) \mid q < x_n + \sqrt{2}\}$ is not computable.

1.5.3 Effective Polish spaces

Definition 1.5.11 (pseudometric and metric spaces). A *pseudometric space* is a pair (X, d), where $d : X \times X \to \mathbb{R}$ such that $d(x,y) = d(y,x) \geq 0$ and $d(x,y) + d(y,z) \geq d(x,z)$. A *metric space* is a pseudometric space with the added property that $d(x,y) = 0 \iff x = y$.

Remark 1.5.12. If (X, d) is a pseudometric space, then we can convert X to a metric space $(\overline{X}, \overline{d})$, where $\overline{X} = \{[x] \mid x \in X\}$, $[x] = \{y \mid d(x,y) = 0\}$, and $\overline{d}([x],[y]) = d(x,y)$.

Definition 1.5.13 (completeness). A metric space (X, d) is *complete* if, whenever $\langle x_n \rangle_{n\in\omega}$, $x_n \in X$, is a *Cauchy sequence*, i.e.,

$$\forall \epsilon > 0 \, \exists m \, \forall n > m \, d(x_m, x_n) < \epsilon,$$

then $\langle x_n \rangle_{n\in\omega}$ is *convergent*, i.e., $\exists x \in X \, \forall \epsilon > 0 \, \exists m \, \forall n > m \, d(x_n, x) < \epsilon$.

Definition 1.5.14 (completion of a pseudometric space). If (X, d) is a pseudometric space, its *completion* is defined as follows. Let $C = \{$Cauchy sequences in $X\}$. For $\langle x_n \rangle_n$, $\langle y_n \rangle_n$ in C, we say $\langle x_n \rangle_n \approx \langle y_n \rangle_n$ if

$$\forall \epsilon > 0 \, \exists m \, \forall n > m \, d(x_n, y_n) < \epsilon.$$

We define $\widehat{X} = C/{\approx}$ and $\widehat{d}([\langle x_n \rangle_n], [\langle y_n \rangle_n]) = \lim_n d(x_n, y_n)$ which gives us the complete metric space $(\widehat{X}, \widehat{d})$.

Note that there is a natural isometry of X onto a dense subset of $\widehat{X}$. If X is a metric space, then this isometry is an isometric embedding.

Definition 1.5.15 (Polish spaces). A metric space is said to be *separable* if it has a countable dense subset. A *Polish space* is a complete separable metric space, i.e., a metric space which is isometric to $(\widehat{A}, \widehat{d})$ where (A, d) is a countable metric space, or more generally a countable pseudometric space.

Definition 1.5.16 (effective Polish spaces). A *computable pseudometric space* is a countable pseudometric space of the form (A, d) where $A \subseteq \omega$ and $d : A \times A \to \mathbb{R}$ are computable. An *effective Polish space*, or equivalently a *effectively given complete separable metric space*, is a Polish space of the form $(\widehat{A}, \widehat{d})$ where (A, d) is a computable pseudometric space.

Examples 1.5.17. The following are examples of effective Polish spaces.

1. $\mathbb{R}^n$ with the Euclidean metric.

2. $C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$ with the metric $d(f,g) = \sup_{0\le x\le 1} |f(x) - g(x)|$. In this case $C[0,1] = \widehat{A}$ where $A = \mathbb{Q}[x]$, the set of all polynomials in one variable with rational coefficients.

3. $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ with the metric $d((x_1,y_1),(x_2,y_2)) = \sqrt{(x_1-x_2)^2 + (y_1-y_2)^2}$. In this case $\mathbb{R}^2 = \widehat{\mathbb{Q}^2}$.

Definition 1.5.18. Let $X = \widehat{A}$ be an effective Polish space. A point $x \in X$ is said to be *computable* or *recursive* if there exists a recursive sequence $a_n \in A$, $n \in \omega$, such that $x = \lim_{n\to\infty} a_n$ and for all n, $d(x, a_n) \le 1/2^n$.

For example, a function $f \in C[0,1]$ is computable if and only if it is uniformly effectively approximable by a sequence of polynomials with rational coefficients.

1.5.4 Examples of effective Polish spaces

Many of the basic examples and constructions in geometry and analysis can be recast in terms of effective Polish spaces.

Example 1.5.19. The set of real numbers $\mathbb{R}$ is an effective Polish space under the Euclidean distance metric, as $\widehat{\mathbb{Q}} = \mathbb{R}$. Similarly, $\mathbb{R}^n = \widehat{\mathbb{Q}^n}$ and so $\mathbb{R}^n$ is also an effective Polish space.

Example 1.5.20. For each $p \in [1,\infty]$ there is a metric on R^n known as the l_p *metric*. The l_p distance between two elements of $\mathbb{R}^n$ is

$$d(\langle a_1,\ldots,a_n\rangle, \langle b_1,\ldots,b_n\rangle) = \left(\sum_{i=1}^n |a_i - b_i|^p\right)^{1/p}.$$

For $p = \infty$ this becomes $\max_{1\le i\le n} |a_i - b_i|$. In particular the l_2-metric is the ordinary the Euclidean metric on $\mathbb{R}^n$. Then $\mathbb{R}^n$ is an effective Polish space under the l_p-metric.

Theorem 1.5.21 (Weierstrass Polynomial Approximation Theorem). For any $f(x) \in C[0,1]$ and any $\epsilon > 0$, there exists a polynomial $p(x) \in \mathbb{Q}[x]$ such that $\sup_{0\le x\le 1} |f(x) - p(x)| < \epsilon$.

Example 1.5.22. The continuous real-valued functions on $[0,1]$ can be made into an effective Polish space with the appropriate metric. By Weierstrass, $C[0,1] = \widehat{\mathbb{Q}[x]}$. The metric that we use is the sup norm:

$$d(f,g) = \sup_{0\le x\le 1} |f(x) - g(x)|.$$

Example 1.5.23. For $1 \le p < \infty$, $L_p[0,1]$ is an effective Polish space $L_p[0,1] = \widehat{\mathbb{Q}[x]}$, where $d(f,g) = \left(\int_0^1 |f(x) - g(x)|^p dx\right)^{1/p}$. This is because $\mathbb{Q}[x]$ is dense in $L_p[0,1]$ and the L_p metric is computable on $\mathbb{Q}[x]$.

Example 1.5.24. For $1 \le p < \infty$, $l_p = \widehat{\mathbb{Q}^\infty} = \widehat{V_\infty(\mathbb{Q})}$, where $\mathbb{Q}^\infty$ is the countable infinite dimensional vector space over $\mathbb{Q}$. Since a countably infinite vector space need not be computable, we let

$$V_\infty(\mathbb{Q}) = \{\langle a_n\rangle_{n\in\omega} \mid a_n \in \mathbb{Q} \wedge \exists m\, \forall n > m\, (a_n = 0)\}.$$

The metric on V_∞ is the l_p metric:

$$d(\langle a_n\rangle_{n\in\omega}, \langle b_n\rangle_{n\in\omega}) = \left(\sum_{n=0}^{\infty} |a_n - b_n|^p\right)^{1/p}.$$

Example 1.5.25. The previous three examples are actually effective separable Banach spaces. For every effective separable Banach space, the unit ball of the dual space with the weak star topology can also be made into an effectively compact effective Polish space.

Example 1.5.26. All the familiar topological constructions such as manifolds, simplicial complexes, CW-complexes, etc., can be made into effective Polish spaces with appropriate natural metrics.

Example 1.5.27. If X is a Polish space, let $\mathcal{K}(X) = \{C \subseteq X \mid C \text{ is nonempty and compact}\}$. Then $\mathcal{K}(X)$ is a Polish space with the Hausdorff metric. If X is an effective Polish space, then so is $\mathcal{K}(X)$.

Example 1.5.28. The space of all isometry types of compact metric spaces with the Gromov-Hausdorff metric is an effective Polish space. The Gromov-Hausdorff metric gives a "distance" between any two compact Hausdorff spaces.

Remark 1.5.29. As the above examples suggest, almost all Polish spaces which arise in practice are effective Polish spaces.

1.5.5 Effective topology and effective continuity

Definition 1.5.30. Let $X = \widehat{A}$ be an effective Polish space. A set $U \subseteq X$ is said to be *effectively open* if there exists a recursive sequence $(a_n, r_n) \in A \times \mathbb{Q}^+$, $n \in \omega$, such that

$$U = \bigcup_{n=0}^{\infty} B(a_n, r_n).$$

Here $B(a, r) = \{x \in X \mid d(a, x) < r\}$, the open ball of radius r centered at a. A set $C \subseteq X$ is *effectively closed* if $X \setminus C$ is effectively open.

Definition 1.5.31. $S \subseteq X$ is an *effective* G_δ if there exists a recursive double sequence $(a_{mn}, r_{mn})_{m,n\in\omega} \subset A \times \mathbb{Q}^+$ such that

$$S = \bigcap_{m\in\omega} \bigcup_{n\in\omega} B(a_{mn}, r_{mn}).$$

S is an *effective* F_σ if its complement $X \setminus S$ is an effective G_δ. Etc.

Definition 1.5.32. A point $x \in X$ is said to be *computable* or *recursive* if there exists a recursive sequence $a_n \in A$, $n \in \omega$, such that $x = \lim_{n\to\infty} a_n$ and for all n, $d(x, a_n) \leq 1/2^n$.

Exercise 1.5.33. Prove this computable analogue of the Baire Category Theorem: If X is an effective Polish space and $S \subseteq X$ is an effective G_δ which is dense in X, then $\{x \in S \mid x \text{ is recursive}\}$ is dense in X.

Definition 1.5.34 (good Cauchy sequences). Let $X = \widehat{A}$ be an effective Polish space. A *good Cauchy sequence* is a sequence $\langle a_n \rangle_{n\in\omega}$, $a_n \in A$, such that

$$\forall m \, \forall n \ (m > n \Rightarrow d(a_m, a_n) \leq 1/2^n) .$$

The set of all good Cauchy sequences is denoted $\mathrm{GC}(X)$. Note that $\mathrm{GC}(X) \subseteq A^\omega \subseteq \omega^\omega$.

Remark 1.5.35. Every point $x \in X$ is of the form $x = \lim_n a_n$ where $\langle a_n \rangle_n \in \mathrm{GC}(X)$. Note that this good Cauchy sequence representing x is not necessarily unique.

We now define the computable analogue of continuous functions between two metric spaces X and Y. The definition uses the notion of partial recursive functional, defined below in Section 2.1 in terms of oracle computations.

Definition 1.5.36 (effective continuity). Let X and Y be effective Polish spaces. A function $f : X \to Y$ is said to be *computable* or *effectively continuous* if there exists a partial recursive functional $F : \mathrm{GC}(X) \to \mathrm{GC}(Y)$ such that for all $\langle a_n \rangle_{n\in\omega} \in \mathrm{GC}(X)$, $f(\lim_n a_n) = \lim_n b_n$ where $F(\langle a_n \rangle_n) = \langle b_n \rangle_n$.

Remark 1.5.37. The continuous functions that arise in practice are almost always computable. Some examples are $\sin x, e^x$, and so on.

In the following exercises, we refer to the arithmetical hierarchy for subsets of ω^ω. This will be defined formally in Section 2.3 below.

Exercise 1.5.38. For $S \subseteq \omega^\omega$ prove the following:

1. S is effectively open if and only if S is Σ^0_1.
2. S is effectively closed if and only if S is Π^0_1.
3. S is an effective G_δ if and only if S is Π^0_2.
4. S is an effective F_σ if and only if S is Σ^0_2.

Exercise 1.5.39. Let $X = \widehat{A}$ be an effective Polish space. For $S \subseteq X$ put $\mathrm{GC}(S) = \{\langle a_n \rangle_n \in \mathrm{GC}(X) \mid \lim_n a_n \in S\}$. Prove the following:

1. S is effectively open if and only if $\mathrm{GC}(S)$ is Σ^0_1 *on* $\mathrm{GC}(X)$, i.e., $\mathrm{GC}(S)$ is the intersection with $\mathrm{GC}(X)$ of a Σ^0_1 subset of ω^ω.
2. S is effectively closed if and only if $\mathrm{GC}(S)$ is Π^0_1 on $\mathrm{GC}(X)$.
3. S is an effective G_δ if and only if $\mathrm{GC}(S)$ is Π^0_2 on $\mathrm{GC}(X)$.
4. S is an effective F_σ if and only if $\mathrm{GC}(S)$ is Σ^0_2 on $\mathrm{GC}(X)$.

Chapter 2

Degrees of unsolvability

2.1 Oracle computations

Intuitively, a Turing oracle is a "black box" which, given a natural number as input, immediately produces a natural number as output. Thus an oracle may be viewed as a function $f : \omega \to \omega$. Recall that $\omega^\omega = \{f : \omega \to \omega\}$ is the space of total functions from ω to ω. Equivalently, this space consists of all infinite sequences of natural numbers.

We want to allow our register machines to perform oracle queries. Recall that the definition of a register machine had four types of instructions: start, stop, increment, and decrement. We add a new type of instruction R_i^0 signifying an oracle query. A fixed function $f \in \omega^\omega$ serves as the oracle. If n is in R_i, then after the execution of the instruction R_i^0, $f(n)$ will be in R_i. In general, f is not a recursive function. If f is recursive, then R_i^0 can be replaced by a register machine program for f, so we obtain nothing new. In general, the oracle f is nonrecursive. See Figure 2.1 for an example of a register machine program which uses an oracle.

If $\mathcal{P}$ is an oracle program, $\mathcal{P}^f(x_1, \ldots, x_k)$ denotes the run of $\mathcal{P}$ with oracle f starting with $x_1, \ldots, x_k$ in $R_1, \ldots, R_k$ and all other registers empty. If e is the Gödel number of $\mathcal{P}$, we write $\varphi_e^{(k),f}(x_1, \ldots, x_k) \simeq$ the content of R_{k+1} if and when $\mathcal{P}^f(x_1, \ldots, x_k)$ halts.

Definition 2.1.1 (partial recursive functionals).

1. A partial functional $\Psi : \omega^\omega \times \omega^k \xrightarrow{P} \omega$ is said to be *partial recursive* if there exists $e \in \omega$ such that for all $f \in \omega^\omega$ and all $x_1, \ldots, x_k \in \omega$, $\Psi(f, x_1, \ldots, x_k) \simeq \varphi_e^{(k),f}(x_1, \ldots, x_k)$.

2. A partial functional $F : \omega^\omega \xrightarrow{P} \omega^\omega$ is said to be *partial recursive* if there exists e such that $\mathrm{dom}(F) = \{f \in \omega^\omega \mid \forall x\, \varphi_e^{(1),f}(x)\downarrow\}$ and, for all $f \in \mathrm{dom}(F)$ and $x \in \omega$, $F(f)(x) = \varphi_e^{(1),f}(x)$.

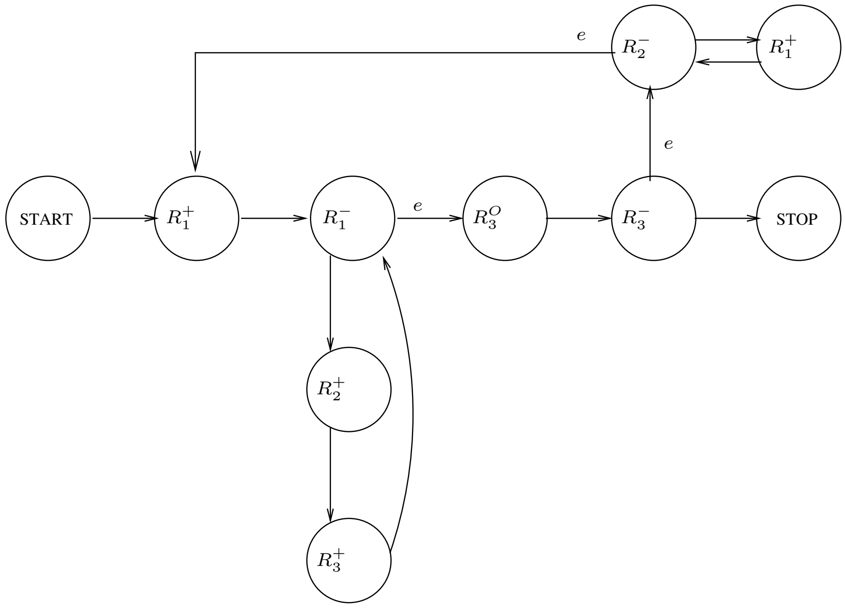

Figure 2.1: This program computes the partial recursive functional $\Psi(f, x) \simeq$ least y such that $y \geq x$ and $f(y) > 0$.

2.2 Relativization

Many of the basic theorems of recursion theory can be generalized to allow oracle computations. For example, the Parametrization Theorem or S-m-n Theorem can be relativized to an arbitrary oracle $f \in \omega^\omega$.

Theorem 2.2.1 (S-m-n Theorem). For each $m, n \geq 1$ there is a fixed $(m+1)$-ary primitive recursive function S^m_n such that

$$\varphi_e^{(m+n),f}(x_1, \ldots, x_m, y_1, \ldots, y_n) \simeq \varphi^{(n),f}_{S^m_n(x_1,\ldots,x_m)}(y_1, \ldots, y_n)$$

for all indices $e \in \omega$, inputs $x_1, \ldots, x_m, y_1, \ldots, y_n \in \omega$, and oracles $f \in \omega^\omega$.

The proof of this theorem is a straightforward adaptation of the proof of usual proof of the S-m-n Theorem or the Parametrization Theorem.

We can also relativize the arithmetical hierarchy. A predicate $P \subseteq \omega$ is said to be $\Sigma^{0,f}_1$ if there is a predicate R^f that is primitive recursive relative to f and $\forall x\, (x \in P \iff \exists y\, R^f(x, y))$. A predicate R^f is said to be primitive recursive relative to f if it can be built up from the initial functions and f. The classes $\Pi^{0,f}_n$ and $\Sigma^{0,f}_n$ are defined inductively in the way we would expect from the $\Sigma^{0,f}_1$ class of predicates. For details, see Section 2.3 below.

2.3 The arithmetical hierarchy

The arithemetical hierarchy is a method of classifying sets by the complexity of their descriptions. The complexity of a set is determined by the number of quantifiers that are required to describe it. Here we briefly review the arithmetical hierarchy. See also Rogers [11, Chapters 14 and 15].

Definition 2.3.1 (the arithmetical hierarchy). Let $R \subseteq \omega^k$ be a k-ary relation on ω. We will define classes Σ^0_n, Π^0_n, Δ^0_n which R may or may not belong to.

1. R is in the class Σ^0_0 if and only if R a primitive recursive relation. For histroical reasons, a primitive recursive R is also said to be in the classes Π^0_0 and Δ^0_0.

2. For $n > 0$, R is in the class Σ^0_n if and only if there exists a primitive recursive $(k+n)$-place predicate P such that

$$R(x_1, \ldots, x_k) \equiv \exists y_1 \, \forall y_2 \, \cdots \, Q_n y_n \, P(x_1, \ldots, x_k, y_1, y_2, \ldots, y_n)$$

   where there are n alternating quantifiers beginning with an existential quantifier. Here $Q_n = \forall$ if n is even, otherwise $Q_n = \exists$.

3. For $n > 0$, R is in the class Π^0_n if and only if there exists a recursive $(k+n)$-place predicate P such that

$$R(x_1, \ldots, x_k) \equiv \forall y_1 \, \exists y_2 \, \cdots \, Q_n y_n \, P(x_1, \ldots, x_k, y_1, \ldots y_n)$$

   where there are n alternating quantifiers beginning with an universal quantifier. Here $Q_n = \exists$ if n is even, otherwise $Q_n = \forall$.

4. R is in the class Δ^0_n if and only if R is in both Σ^0_n and Π^0_n.

5. R is said to be *arithmetical* if R is in Σ^0_n for some $n \in \omega$. (This is equivalent to R being in Π^0_n or Δ^0_n for some n).

A number of basic facts quickly follow from the definition of the arithmetical hierarchy.

Theorem 2.3.2. The following hold for all $n \geq 1$.

1. Σ^0_n is closed under $\wedge$, $\vee$, $\exists x$, $\exists x < y$, $\forall x < y$, and substitution of recursive functions.

2. Π^0_n is closed under $\wedge$, $\vee$, $\forall x$, $\exists x < y$, $\forall x < y$, and substitution of recursive functions.

3. $\Pi^0_n = \neg \, \Sigma^0_n$

4. $A \subseteq \omega$ is Σ^0_1 if and only if A is recursively enumerable.

5. $R \subseteq \omega^k$ is Δ^0_1 if and only if R is recursive.

Theorem 2.3.3. For every $n \geq 1$ there exists an $A \subseteq \omega$ such that $A \in \Sigma^0_n \setminus \Pi^0_n$. Furthermore, $\neg A \in \Pi^0_n \setminus \Sigma^0_n$, and $A \oplus \neg A$ is in $\Delta^0_{n+1} \setminus (\Sigma^0_n \cup \Pi^0_n)$.

Example 2.3.4. The halting problem $H = \{e \mid \varphi^{(1)}_e(0) \downarrow\}$ is an example of a Σ^0_1 set that is not Π^0_1. In fact, every set in Σ^0_1 is many-one reducible to H.

Example 2.3.5. Define $T = \{e \mid \forall n\, \varphi^1_e(n) \downarrow\}$, the set of indices of all total functions. T is then a Π^0_2 set that is not Σ^0_2.

Using the idea of oracle computation, we can extend the arithmetical hierarchy from ω to the Baire space ω^ω.

Definition 2.3.6. A set $R \subseteq \omega^\omega \times \omega^k$ is defined to be *recursive* if and only if $\chi_R : \omega^\omega \times \omega^k \to \{0,1\}$ is a recursive functional. For $n \geq 1$, we say that $P \subseteq \omega^\omega \times \omega^k$ is Σ^0_n if there is a recursive predicate $R \subseteq \omega^\omega \times \omega^{k+n}$ such that for all f and all $x_1, \ldots, x_k$,

$$P(f, x_1, \ldots, x_k) \iff \exists y_1\, \forall y_2 \cdots y_n\, R(f, x_1, \ldots, x_k, y_1, y_2, \ldots, y_n)$$

where there are n alternating quantifiers beginning with an existential quantifier. The last quantifier is $\forall y_n$ if n is even, $\exists y_n$ if n is odd. P is Π^0_n if and only if its complement $\neg P$ is Σ^0_n.

Remark 2.3.7 (topological analogies). The arithmetical hierarchy of subsets of ω^ω provides computable analogs of familiar topological notions. For $S \subseteq \omega^\omega$ we have that S is Σ^0_1 if and only if S is *effectively open*, i.e., the union of a recursive sequence of basic open sets. S is Π^0_1 if and only if S is *effectively closed*, i.e., the complement of an effectively open set. S is Σ^0_2 if and only if S is effectively F_σ. S is Π^0_2 if and only if S is effectively G_δ. Et cetera. Furthermore, all of this generalizes to effective Polish spaces. See Exercises 1.5.38 and 1.5.39.

Exercise 2.3.8. Prove the following *reduction principle* for Σ^0_n subsets of the Baire space. (It also holds for Σ^0_n predicates on ω.) If $P, Q \subseteq \omega^\omega$ are Σ^0_n, then there exist P^*, Q^* such that $P^* \cup Q^* = P \cup Q$, $P^* \cap Q^* = \emptyset$, and P^*, Q^* are Σ^0_n.

Definition 2.3.9. Everything relativizes to an arbitrary oracle, as follows. Recall that for $f, g \in \omega^\omega$ we have $f \oplus g \in \omega^\omega$ given by

$$\begin{aligned} (f \oplus g)(2n) &= f(n), \\ (f \oplus g)(2n+1) &= g(n). \end{aligned}$$

Given f, a partial functional $\Psi : \omega^\omega \times \omega^k \xrightarrow{P} \omega$ is said to be *partial f-recursive*, or *partial recursive relative to f*, if

$$\exists e\, \forall g\, \forall x_1 \cdots \forall x_k \left(\Psi(g, x_1, \ldots, x_k) \simeq \varphi^{(k), f \oplus g}_e(x_1, \ldots, x_k) \right).$$

Morover, for all $n \geq 1$ and all f, we say that $P \subseteq \omega^\omega \times \omega^k$ is $\Sigma^{0,f}_n$ if there is a recursive predicate R such that for all g and all $x_1, \ldots, x_k$, $P(g, x_1, \ldots, x_k)$ if and only if $\exists y_1\, \forall y_2 \cdots y_n\, R(f \oplus g, x_1, \ldots, x_k, y_1, y_2, \ldots, y_n)$.

Remark 2.3.10 (topological equivalences). When we relativize to arbitrary oracles, the topological analogies of Remark 2.3.7 become topological equivalences. For $S \subseteq \omega^\omega$ we have that S is open if and only if S is $\Sigma_1^{0,f}$ for some f. S is closed if and only if S is $\Pi_1^{0,f}$ for some f. S is F_σ (i.e., the union of countably many closed sets) if and only if S is $\Sigma_2^{0,f}$ for some f. S is G_δ (i.e., the intersection of countably many open sets) if and only if S is $\Pi_2^{0,f}$ for some f. Also, $F : \omega^\omega \to \omega^\omega$ is continuous if and only if F is f-recursive for some f. More generally, $F : \omega^\omega \xrightarrow{P} \omega^\omega$ is continuous with G_δ domain if and only if F is partial f-recursive for some f. Furthermore, all of this generalizes to effective Polish spaces, using good Cauchy sequences, in the style of Exercise 1.5.39.

2.4 Turing degrees

Notation 2.4.1. We write $\{e\}^f(x_1, \ldots, x_k) \simeq \varphi_e^{(k),f}(x_1, \ldots, x_k)$.

Definition 2.4.2 (Turing reducibility). Let f and g be two functions in ω^ω. Then $f \leq_T g$ if there exists an oracle program with Gödel number e such that $\{e\}^g(x) \simeq f(x)$ for all $x \in \omega$. In other words, f can be computed using an oracle for g. In this case, f is said to be *Turing reducible* to g.

The following proposition follows easily from the definition of Turing reducibility.

Proposition 2.4.3. The relation $\leq_T$ is reflexive and transitive.

Proof. Let f, g and h be elements of ω^ω. Clearly, f can be computed using an oracle for f, so $f \leq_T f$. Now, suppose that $f \leq_T g$ and $g \leq_T h$. Then $f(n) = \{e_1\}^g(n)$ for all n, and $g(n) = \{e_2\}^h(n)$ for all n, for some fixed $e_1, e_2 \in \omega$. Whenever g is called in computing f, substitute the program calling h to compute g. Thus we see that there is an $e_3 \in \omega$ such that $f(n) = \{e_3\}^h(n)$ for all n, hence $f \leq_T h$. □

Definition 2.4.4. Two functions f and g in ω^ω are said to be *Turing equivalent* if $f \leq_T g$ and $g \leq_T f$. In this case we write $f \equiv_T g$.

Proposition 2.4.5. Turing equivalence is an equivalence relation.

Proof. This is clear from Proposition 2.4.3 and the definition of Turing equivalence. □

Definition 2.4.6 (degrees of unsolvability). The *Turing degrees* are the set of equivalence classes of $\equiv_T$:

$$\mathcal{D}_T = \omega^\omega / {\equiv_T}.$$

If $f \in \omega^\omega$, then we have $\deg_T(f) = \{g \in \omega^\omega \mid f \equiv_T g\}$. This is the Turing degree of f. The Turing degrees are partially ordered by Turing reducibility:

$$\deg_T(f) \leq \deg_T(g) \iff f \leq_T g.$$

Turing degrees are also known as *degrees of unsolvability*.

There is a least Turing degree $\mathbf{0} = \deg_T(\lambda n.0)$. Note that $\deg_T(f) = \mathbf{0}$ if and only if f is recursive.

Proposition 2.4.7. Any two Turing degrees have a least upper bound.

Proof. The least upper bound of $\mathbf{a} = \deg_T(f)$ and $\mathbf{b} = \deg_T(g)$ is $\mathbf{a} \vee \mathbf{b} = \deg_T(h)$, where $h = f \oplus g$ is given by $h(2n) = f(n)$, $h(2n+1) = g(n)$ for all n. $\square$

Remark 2.4.8. It can be shown that there exist two Turing degrees which do not have a greatest lower bound.

If $A \subseteq \omega$ we write $\deg_T(A)$ to mean $\deg_T(\chi_A)$, where χ_A is the characteristic function of A. In some textbooks the Turing degrees are defined in terms of sets, not functions. This does not matter, because as we shall now show, all Turing degrees are Turing degrees of sets.

Proposition 2.4.9. For each $f \in \omega^\omega$ there is a set $A \subseteq \omega$ such that $\deg_T(A) = \deg_T(f)$.

Proof. Let $A = G_f = \{2^x 3^{f(x)} \mid x \in \omega\}$, the "graph" of f. It suffices to show that $\deg_T(f) = \deg_T(A)$. We have $f(x) = \mu y\,(2^x 3^y \in G_f)$, so f can be computed using an oracle for A. Conversely, $n \in A$ if and only if $n = 2^{(n)_0} 3^{(n)_1}$ and $f((n)_0) = (n)_1$. Thus, χ_A can be computed using an oracle for f. $\square$

2.5 The jump operator

Given $f \in \omega^\omega$, suppose we wish to find a Turing degree which is strictly greater than $\deg_T(f)$. The most obvious way to do so is to relativize Turing's result on the Halting Problem to oracle programs using f as the oracle. Let $H^f = \{e \mid \{e\}^f(0)\downarrow\}$, the Halting Problem relativized to f. By relativizing Turing's argument, we shall show that $H^f \not\leq_T f$. Furthermore, using the S-m-n Theorem, we shall show that $f \leq_T H^f$. Thus we will have $\deg_T(H^f) > \deg_T(f)$.

Definition 2.5.1. For $\Gamma \subseteq \mathcal{P}(\omega)$, a set $C \subseteq \omega$ is said to be Γ *complete* if

1. $C \in \Gamma$, and
2. for all $A \in \Gamma$, $A \leq_m C$.

Theorem 2.5.2. The set H^f is $\Sigma_1^{0,f}$ complete. In fact, for all $A \subseteq \omega$, $A \in \Sigma_1^{0,f}$ if and only if $A \leq_m H^f$.

Proof. This is just the relativization to f of the fact that the Halting Problem, H, is Σ_1^0 complete.

Note first that H^f is $\Sigma_1^{0,f}$ since

$$e \in H^f \iff \exists n\,((\mathrm{State}^f(e,0,n))_0 = 0).$$

Here, n is the stopping time of the program e started with inputs 0 and oracle f.

Now suppose $A \in \Sigma_1^{0,f}$, say $A = \{x \mid \exists y\, R^f(x,y)\}$, where R^f is primitive recursive relative to f. Consider the function $\psi^f(x) \simeq \mu y\, R^f(x,y)$. This is a partial recursive function relative to f. Hence there is a Gödel number e such that

$$\psi^f(x) \simeq \varphi_e^{(2),f}(x,z),$$

where z is a dummy variable. By the S-m-n Theorem we have

$$\varphi_{S_1^1(e,x)}^{(1),f}(z) \simeq \varphi_e^{(2),f}(x,z)$$

where S_1^1 is primitive recursive. Setting $z = 0$ we see that $x \in A$ if and only if $S_1^1(e,x) \in H^f$. Thus $A \leq_m H_f$ via $\lambda x.S_1^1(e,x)$. $\square$

Corollary 2.5.3. Suppose f and g are elements of the Baire space. Then:

1. if $f \leq_T g$, then $H^f \leq_m H^g$;
2. $f \leq_T H^f$; and
3. $H^f \not\leq_T f$.

Proof. If $f \leq_T g$, then $\Sigma_1^{0,f} \subset \Sigma_1^{0,g}$, so $H^f \leq_m H^g$. We showed above that $G_f \equiv_T f$ and hence G_f is in $\Sigma_1^{0,f}$. It follows that $G_f \leq_m H^f$, so $G_f \leq_T H^f$. Thus, it follows that $f \leq_T H^f$. Finally, let $K^f = \{e \mid \varphi_e^{(1),f}(e)\downarrow\}$ (the diagonal halting problem). Then $K^f \not\leq_T f$ by the usual diagonalization argument. We can show that K^f is $\Sigma_1^{0,f}$ so $K^f \leq_m H^f$ and therefore $H^f \not\leq_T f$. $\square$

Exercise 2.5.4. Show that $f \leq_T g$ if and only if $H^f \leq_m H^g$.

Definition 2.5.5. The function

$$J : \mathcal{D}_T \to \mathcal{D}_T$$

defined by $J(\deg_T(f)) = \deg_T(H^f)$ is called the *Turing jump operator*.

Note that if $f \equiv_T g$, then $H^f \equiv_T H^g$, so the Turing jump does not depend on the choice of Turing degree representative.

Notation 2.5.6. If $\mathbf{a}$ is any Turing degree, we often denote $J(\mathbf{a})$ by $\mathbf{a}'$. We denote the nth Turing jump of $\mathbf{a}$ as $\mathbf{a}^{(n)}$. Thus $\mathbf{a}^{(0)} = \mathbf{a}$, and $\mathbf{a}^{(n+1)} = (\mathbf{a}^{(n)})'$ for all n. Thus we have

$$\mathbf{a} < \mathbf{a}' < \mathbf{a}'' < \cdots < \mathbf{a}^{(n)} < \mathbf{a}^{(n+1)} < \cdots .$$

Proposition 2.5.7. If $\mathbf{a}$ and $\mathbf{b}$ are Turing degrees, we have:

1. $\mathbf{a} < \mathbf{a}'$.
2. $\mathbf{a} \leq \mathbf{b}$ implies $\mathbf{a}' \leq \mathbf{b}'$.

3. In particular $\mathbf{a}' \geq \mathbf{0}'$ for all $\mathbf{a}$.

Note also that $\mathbf{0}'$ is the Turing degree of the Halting Problem, $\mathbf{0}' = \deg_T(H)$.

The following two theorems express nice properties of the jump operator. We state them now without proof. We shall prove them later, after developing some machinery.

Theorem 2.5.8 (Friedberg's Jump Theorem). For all Turing degrees $\mathbf{c} \geq \mathbf{0}'$ there exists a Turing degree $\mathbf{a}$ such that $\mathbf{a}' = \mathbf{c}$. In other words, the range of the Turing jump operator $J : \mathcal{D}_T \to \mathcal{D}_T$ is $\{\mathbf{c} \in \mathcal{D}_T \mid \mathbf{c} \geq \mathbf{0}'\}$.

Theorem 2.5.9 (Post's Theorem). The Turing degree $\mathbf{0}^{(n)}$ is $\deg_T(C_n)$, where C_n is a complete Σ^0_n set.

2.6 Finite approximations

Intuitively, if an oracle computation $\{e\}^f(x)$ halts, it can only use a finite amount of information from f, because it only performs a finite number of steps before halting. In this section, we formalize this intuition into Proposition 2.6.3. Then we use this idea to prove that incomparable Turing degrees exist (Theorem 2.6.4) and to prove Friedberg's theorem characterizing the range of the Turing jump operator (Theorem 2.6.7).

Definition 2.6.1 (finite sequences). We define $\mathrm{Seq} = \omega^{<\omega}$ to be the set of finite sequences of elements of ω. Also, $\mathrm{Seq}_2 = 2^{<\omega}$ consists of the finite sequences from the set $\{0, 1\}$. We sometimes identify sequences $\sigma \in \mathrm{Seq}$ with their Gödel numbers. The length of σ is denoted $\mathrm{lh}(\sigma)$. For $n < \mathrm{lh}(\sigma)$, $\sigma(n)$ is the nth element of σ. The first element of σ is $\sigma(0)$. Let $f \in \omega^\omega$ and $\sigma, \tau \in \mathrm{Seq}$. We write $\sigma \subseteq \tau$ if and only if $\mathrm{lh}(\sigma) \leq \mathrm{lh}(\tau)$ and $\forall n < \mathrm{lh}(\sigma)[\sigma(n) = \tau(n)]$. We write $\sigma \subset f$ if and only if $\forall n < \mathrm{lh}(\sigma)\,[\sigma(n) = f(n)]$. For $n \in \omega$, $f[n]$ denotes the sequence consisting of the first n elements of f:

$$f[n] = \langle f(0), f(1), \ldots, f(n-1)\rangle.$$

Definition 2.6.2. For $e, s, x, y \in \omega$ and $\sigma \in \mathrm{Seq}$, we write $\{e\}^\sigma_s(x) \simeq y$ if and only if the following conditions hold:

1. x, y, and e are all less than s.
2. For some (equivalently, all) $f \in \omega^\omega$ extending σ, $\{e\}^f(x)$ halts in fewer than s steps with output y, and during this computation, no oracle information from f is used except the part of f which is in σ.

We write $\{e\}^\sigma(x) \simeq y$ if and only if $\{e\}^\sigma_{\mathrm{lh}(\sigma)}(x) \simeq y$.

A basic tool in the study of Turing degrees is the following proposition.

Proposition 2.6.3. We have:

1. $\{e\}^f(x) \simeq y$ if and only if $\exists n\, \exists s\, \{e\}_s^{f[n]}(x) \simeq y$.

2. $\{e\}^f(x) \simeq y$ if and only if $\exists n\, \{e\}^{f[n]}(x) \simeq y$.

3. If $s \leq t$ and $\sigma \subseteq \tau$, then $\{e\}_s^\sigma(x) \simeq y$ implies $\{e\}_t^\tau(x) \simeq y$.

4. The 5-place relation $\{e\}_s^\sigma(x) \simeq y$ is primitive recursive.

5. The 4-place relation $\{e\}_s^\sigma(x) \downarrow$ is primitive recursive.

6. The 4-place relation $\{e\}^\sigma(x) \simeq y$ is primitive recursive.

7. The 3-place relation $\{e\}^\sigma(x) \downarrow$ is primitive recursive.

We now use this technique to prove the existence of incomparable Turing degrees.

Theorem 2.6.4 (Kleene/Post). There are incomparable Turing degrees below $\mathbf{0}'$. That is, there are $\mathbf{a}, \mathbf{b} \leq \mathbf{0}'$ such that $\mathbf{a} \not\leq \mathbf{b}$ and $\mathbf{b} \not\leq \mathbf{a}$.

Proof. We shall have $\mathbf{a} = \deg_T(A)$, $\mathbf{b} = \deg_T(B)$ where $A, B \subseteq \omega$. We will build $f = \chi_A$ and $g = \chi_B$ by finite approximation. That is, we will construct two sequences $\langle \sigma_n \rangle_{n=0}^\infty$ and $\langle \tau_n \rangle_{n=0}^\infty$ of elements of Seq_2 such that, for all $n \in \omega$, $\sigma_n \subseteq \sigma_{n+1}$ and $\tau_n \subseteq \tau_{n+1}$. Then we will let $f = \bigcup_{n=0}^\infty \sigma_n$ and $g = \bigcup_{n=0}^\infty \tau_n$. Thus $f, g \in 2^\omega$. In the end, the Turing degrees of f and g will satisfy the conclusions of the theorem. The construction will proceed by stages. At stage n, we will create σ_n and τ_n.

Informally, the construction proceeds as follows. At stage $2e$, we ensure that once f and g are constructed, $f \neq \{e\}^g$. At stage $2e+1$, we ensure that $g \neq \{e\}^f$. After f and g are constructed, we will see that they are recursive in the Halting Problem, $H = 0'$.

We begin the construction at stage 0 by letting $\sigma_0 = \tau_0 = \langle\rangle$, the empty sequence.

At stage $2e+1$, if there exists $\sigma \in \mathrm{Seq}_2$ extending σ_{2e} such that $\{e\}^\sigma(\mathrm{lh}(\tau_{2e})) \simeq 1$, we let $\sigma_{2e+1} = \sigma$ and $\tau_{2e+1} = \tau_{2e}{}^\frown\langle 0 \rangle$. Otherwise, we let $\sigma_{2e+1} = \sigma_{2e}$ and $\tau_{2e+1} = \tau_{2e}{}^\frown\langle 1 \rangle$.

At stage $2e+2$, if there exists τ extending τ_{2e+1} such that $\{e\}^\tau(\mathrm{lh}(\sigma_{2e+1})) \simeq 1$, then we let $\tau_{2e+2} = \tau$ and $\sigma_{2e+2} = \sigma_{2e+1}{}^\frown\langle 0 \rangle$. Otherwise, we let $\tau_{2e+2} = \tau_{2e+1}$ and $\sigma_{2e+2} = \sigma_{2e+1}{}^\frown\langle 1 \rangle$.

Define $f = \bigcup_n \sigma_n$ and $g = \bigcup_n \tau_n$. We claim that f and g have incomparable Turing degrees. Suppose that $f = \{e\}^g$. This is impossible, because $f(\mathrm{lh}(\sigma_{2e+1})) = 1$ if and only if $\{e\}^{\tau_{2e+1}}(\mathrm{lh}(\sigma_{2e+1})) \not\simeq 1$, if and only if $\{e\}^g(\mathrm{lh}(\sigma_{2e+1})) \not\simeq 1$. Similarly, it can be shown that $g \neq \{e\}^f$.

We next claim that the functions $n \mapsto \sigma_n$ and $n \mapsto \tau_n$ are recursive in $\mathbf{0}'$. We prove this by induction on n. Suppose we know how to compute σ_n and τ_n and we want to compute σ_{n+1} and τ_{n+1}. We mimic the construction above. The only nonrecursive decision which must be made during this construction is whether a certain unbounded search will terminate. We can decide whether this search will terminate by using an oracle for the Halting Problem. Hence

σ_{n+1} and τ_{n+1} are recursive in $\mathbf{0}'$ as claimed. Hence f and g are recursive in $\mathbf{0}'$ as well. $\square$

The Kleene/Post method yields many other properties of the Turing degrees, as illustrated by the following exercises.

Exercise 2.6.5. Show that in Theorem 2.6.4 we can also require that $\mathbf{a}$ and $\mathbf{b}$ form a *minimal pair*, i.e., for all $\mathbf{c}$, if $\mathbf{c} \leq \mathbf{a}$ and $\mathbf{c} \leq \mathbf{b}$ then $\mathbf{c} = \mathbf{0}$.

Exercise 2.6.6. An *ideal* in the Turing degrees is a set $I \subseteq \mathcal{D}_T$ such that $\mathbf{0} \in I$, and $\mathbf{c}_1 \vee \mathbf{c}_2 \in I$ if and only if $\mathbf{c}_1, \mathbf{c}_2 \in I$. Show that for any countable ideal I there exist $\mathbf{a}, \mathbf{b}$ such that $I = \{\mathbf{c} \mid \mathbf{c} \leq \mathbf{a} \wedge \mathbf{c} \leq \mathbf{b}\}$. Conclude from this that no strictly ascending sequence of Turing degrees has a least upper bound. Conclude also that $\mathcal{D}_T$ is not a lattice.

Next we prove the Freidberg Jump Theorem.

Theorem 2.6.7 (Friedberg). Given a Turing degree $\mathbf{c} \geq \mathbf{0}'$, we can find a Turing degree $\mathbf{a}$ such that $\mathbf{a}' = \mathbf{a} \vee \mathbf{0}' = \mathbf{c}$.

Proof. Fix $C \subseteq \omega$ such that $\mathbf{c} = \deg_T(C)$. As before we construct $\mathbf{a} = \deg_T(A)$ where $\chi_A \in 2^\omega$ is the limit of an increasing sequence $\sigma_n \in \mathrm{Seq}_2$ of finite approximations. Then we will show that A has the desired properties. The construction will proceed by stages. At stages of the form $2e+1$, we will exert some control over the Turing jump of A. At stages of the form $2e+2$ we will ensure that $C \leq_T A \oplus 0'$.

At stage 0, let $\sigma_0 = \langle\rangle$.

At stage $2e+1$, we ask whether there exists $\sigma \in \mathrm{Seq}_2$ extending σ_{2e} such that $\{e\}^\sigma(0)\downarrow$. If so, we choose the unique σ of least Gödel number among all elements of Seq_2 with this property, and let $\sigma_{2e+1} = \sigma$. Otherwise, we let $\sigma_{2e+1} = \sigma_{2e}$.

At stage $2e+2$, we let $\sigma_{2e+2} = \sigma_{2e+1}{}^\frown\langle\chi_C(e)\rangle$.

To end the construction, let $\chi_A = \bigcup_n \sigma_n$. It is clear that the length of σ_n becomes arbitrarily large as n goes to infinity, so A is well defined.

First, we claim that the function $n \mapsto \sigma_n$ is recursive in C. The construction at stages of the form $2e+2$ is clearly recursive in C. The construction at stages of the form $2e+1$ is recursive in $0'$, which in turn is recursive in C by hypothesis. This proves the claim.

Next, we claim that C is recursive in $A \oplus 0'$. It is enough to show that the function $n \mapsto \sigma_n$ is recursive in $A \oplus 0'$, because C is clearly recursive in this sequence. The construction of σ_{n+1} given σ_n at a stage of the form $2e+2$ is recursive in A; at a stage of the form $2e+1$ the construction is recursive in $0'$. This implies that $C \leq_T A \oplus 0'$.

Combining this with the previous claim, we see that $\mathbf{c} = \mathbf{a} \vee \mathbf{0}'$.

Finally, we claim that $\mathbf{a}' = \mathbf{a} \vee \mathbf{0}'$. A straightforward argument shows that $\mathbf{a} \vee \mathbf{0}' \leq \mathbf{a}'$. We will show that the converse inequality holds. We showed above that the sequence $\langle\sigma_n\rangle$ is recursive in $\mathbf{a} \vee \mathbf{0}'$. By construction, $\{e\}^A(0)\downarrow$ if and only if $\{e\}^{\sigma_{2e+1}}(0)\downarrow$. Since the latter computation must halt in no more than

$\mathrm{lh}(\sigma_{2e+1})$ steps, we can recusively decide whether $\{e\}^A(0)$ halts by running it for $\mathrm{lh}(\sigma_{2e+1})$ steps. As $\mathrm{lh}(\sigma_{2e+1})$ can be computed from $\mathbf{a} \vee \mathbf{0}'$, this shows that $\mathbf{a}' \leq \mathbf{a} \vee \mathbf{0}'$. $\square$

Remark 2.6.8. A Turing degree $\mathbf{a}$ is said to be *low* if $\mathbf{a}' \leq \mathbf{0}'$, and *generalized low* if $\mathbf{a}' \leq \mathbf{a} \vee \mathbf{0}'$. (The opposite inequalities hold automatically for all $\mathbf{a}$.) Using this language, we can say that the Turing degree $\mathbf{a}$ constructed in Theorem 2.6.7 is generalized low.

Exercise 2.6.9. Show that for all $\mathbf{c} \geq \mathbf{0}'$ there exist $\mathbf{a}, \mathbf{b}$ such that $\mathbf{a}' = \mathbf{a} \vee \mathbf{0}' = \mathbf{b}' = \mathbf{b} \vee \mathbf{0}' = \mathbf{a} \vee \mathbf{b} = \mathbf{c}$ and $\mathbf{a} \not\leq \mathbf{b}$ and $\mathbf{b} \not\leq \mathbf{a}$. In addition we can require that $\mathbf{a}$ and $\mathbf{b}$ form a minimal pair.

2.7 Post's Theorem and its corollaries

Theorem 2.7.1 (Post). Let $R \subseteq \omega^k$ be a k-place predicate on ω. Then R is $\Sigma^{0,B}_{n+1}$ if and only if R is $\Sigma^{0,B^{(n)}}_1$. Here $B^{(n)}$ denotes the nth Turing jump of B.

Proof. The proof is by induction on n. The base case when $n = 0$ is trivial, since $B^{(0)} = B$. Let $n \geq 1$ and suppose R is $\Sigma^{0,B}_{n+1}$. Then we have

$$R(x_1, \ldots, x_n) \equiv \exists y\, S(x_1, \ldots, x_n, y)$$

for a $\Pi^{0,B}_n$ predicate S. It follows that the complement of S is $\Sigma^{0,B}_n$ and hence by the induction hypothesis, the complement of S is $\Sigma^{0,B^{(n-1)}}_1$. From this we deduce that S is $\Pi^{0,B^{(n-1)}}_1$. Then S is recursive in $B^{(n)}$, hence R is $\Sigma^{0,B^{(n)}}_1$.

To prove the converse, assume that R is $\Sigma^{0,B^{(n)}}_1$. Letting e be an index of R, we can write

$$R(x_1, \ldots, x_n) \;\equiv\; \{e\}^{\chi_{B^{(n)}}}(x_1, \ldots, x_k)\downarrow \equiv\; \exists s\, \{e\}^{\chi_{B^{(n)}}[s]}_s(x_1, \ldots, x_k)\downarrow.$$

This is equivalent to

$$\exists \sigma\, (\chi_{B^{(n)}}[\mathrm{lh}(\sigma)] = \sigma \wedge \{e\}^\sigma(x_1, \ldots, x_k)\downarrow).$$

To show that this is $\Sigma^{0,B}_{n+1}$, it suffices to show that the predicate $\chi_{B^{(n)}}[\mathrm{lh}(\sigma)] = \sigma$ is $\Delta^{0,B}_{n+1}$, since the predicate

$$\{e\}^\sigma(x_1, \ldots, x_k)\downarrow$$

is primitive recursive.

Note that the predicate $x \in B^{(n)}$ is $\Sigma^{0,B}_n$. To see this we first note that $B^{(n)}$ is $\Sigma^{0,B^{(n-1)}}_1$ by definition. Applying the induction hypothesis, we see that $B^{(n)}$ is $\Sigma^{0,B}_n$.

Now, observe that $\chi_{B^{(n)}}[\mathrm{lh}(\sigma)] = \sigma$ if and only if

$$\forall i < \mathrm{lh}(\sigma)\, [i \in B^{(n)} \iff \sigma(i) = 1].$$

Because $i \in B^{(n)}$ is $\Sigma_n^{0,B}$, we see that $i \in B^{(n)} \iff \sigma(i) = 1$ is $\Delta_{n+1}^{0,B}$, being the conjunction of a $\Sigma_n^{0,B}$ statement and a $\Pi_n^{0,B}$ statement. Since the quantifier $\forall i < \mathrm{lh}(\sigma)$ is bounded, it follows that the whole formula is $\Delta_{n+1}^{0,B}$. Hence, as noted above, R is $\Sigma_{n+1}^{0,B}$. This completes the proof. $\square$

Corollary 2.7.2. Let $A, B \subseteq \omega$. Then A is $\Sigma_{n+1}^{0,B}$ if and only if A is r.e. in $B^{(n)}$.

Proof. This follows from Post's Theorem plus the relativization to $B^{(n)}$ of the fact that A is Σ_1^0 if and only if A is r.e. $\square$

Corollary 2.7.3. A is $\Sigma_{n+1}^{0,B}$ if and only if $A \leq_m B^{(n+1)}$. In particular, $B^{(n+1)}$ is a complete $\Sigma_{n+1}^{0,B}$ set.

Proof. This follows from Corollary 2.7.2 plus the relativization to $B^{(n)}$ of the fact that A is Σ_1^0 if and only if $A \leq_m H$. $\square$

Corollary 2.7.4. A is $\Delta_{n+1}^{0,B}$ if and only if $A \leq_T B^{(n)}$.

Proof. This follows from Corollary 2.7.2 plus the relativization to $B^{(n)}$ of the fact that A is r.e. and co-r.e. if and only if A is recursive. $\square$

Corollary 2.7.5. $\deg_T(B^{(n)}) = \max\{\deg_T(A) \mid A \in \Delta_{n+1}^{0,B}\}$.

Proof. This is immediate from the previous corollary. $\square$

Combining these corollaries and setting $B = 0$, we have the following unrelativized results.

Corollary 2.7.6. Let A be a subset of ω.

1. A is Σ_{n+1}^0 if and only if A is r.e. in $0^{(n)}$.

2. A is Σ_{n+1}^0 if and only if $A \leq_m 0^{(n+1)}$.

3. A is Δ_{n+1}^0 if and only if $A \leq_T 0^{(n)}$.

4. $A \in \Sigma_\infty^0 = \bigcup_{n=0}^\infty \Sigma_n^0$ if and only if $A \leq_T 0^{(n)}$ for some n.

Remark 2.7.7. Note that, according to Post's Theorem, Σ_n^0 predicates on ω behave very much like Σ_1^0 predicates, for all $n \geq 1$. Thus, to understand the structure of Σ_n^0 subsets of ω, $n \geq 1$, it suffices to understand the structure of r.e. sets.

To illustrate, we briefly explore a well known property of Σ_1^0 predicates which easily generalizes to $\Sigma_n^{0,B}$, $n \geq 1$, using Post's Theorem.

Consider the following statement:

> If $S \subseteq \omega^{k+1}$ is Σ_1^0 and $\forall x_1 \cdots \forall x_k \, \exists y \, S(x_1, \ldots, x_k, y)$ holds, then we can find a recursive Skolem function $f : \omega^k \to \omega$ such that $\forall x_1 \cdots \forall x_k \, S(x_1, \ldots, x_k, f(x_1, \ldots, x_k))$.

This is well known as a special case of the so-called *uniformization principle* for Σ^0_1 predicates. Relativizing to an arbitrary oracle B, we obtain:

> If $S \subseteq \omega^{k+1}$ is $\Sigma^{0,B}_1$ and $\forall x_1 \cdots \forall x_k \, \exists y \, S(x_1, \ldots, x_k, y)$ holds, then we can find $f : \omega^k \to \omega$ such that $f \leq_T B$ and $\forall x_1 \cdots \forall x_k \, S(x_1, \ldots, x_k, f(x_1, \ldots, x_k))$.

In particular, if we let $B = 0^{(n)}$, then by Post's Theorem we obtain:

> If $S \subseteq \omega^{k+1}$ is Σ^0_{n+1} and $\forall x_1 \cdots \forall x_k \, \exists y \, S(x_1, \ldots, x_k, y)$ holds, then we can find a Δ^0_{n+1} function $f : \omega^k \to \omega$ such that $\forall x_1 \cdots \forall x_k \, S(x_1, \ldots, x_k, f(x_1, \ldots, x_k))$.

This is an interesting property of Σ^0_{n+1} predicates which is not obvious from the definitions.

Remark 2.7.8. It is worth noting that Post's Theorem applies to predicates on ω, but does not apply to predicates on the Baire space, ω^ω. For example, consider the set of constant functions, $C = \{f \mid \forall n \, f(n) = f(0)\} \subseteq \omega^\omega$. Clearly C is Π^0_1, hence Σ^0_2, but C is not $\Sigma^{0,0'}_1$. In fact, C is not $\Sigma^{0,f}_1$ for any oracle f. One way to see this is to note that a set $S \subseteq \omega^\omega$ is $\Sigma^{0,f}_1$ for some f if and only if S is open (with respect to the usual topology on ω^ω). See Remark 2.3.10. Our set C is certainly not open.

2.8 A minimal Turing degree

In this section, we prove the existence of a minimal Turing degree. We follow the method, due to Sacks [13], of forcing with recursive perfect trees.

We begin with a discussion of trees in general.

Definition 2.8.1 (trees). A *tree* is a nonempty subset of Seq which is closed under initial segments. Thus if T is a tree, $\sigma \in T$, and $\tau \subseteq \sigma$, then $\tau \in T$. A tree is said to be *recursive* if the characterstic function of the tree as a subset of Seq is recursive.

Definition 2.8.2. A *path* through a tree T is a function $f \in \omega^\omega$ such that every initial segment of f is in T. The set of paths through T is denoted $[T]$. Thus we have

$$[T] = \{f \in \omega^\omega \mid \forall n \, (f[n] \in T)\}.$$

Proposition 2.8.3. A nonempty set $C \subseteq \omega^\omega$ is closed if and only if there exists a tree $T \subseteq \text{Seq}$ such that $C = [T]$.

Proof. Suppose that $T \subseteq \text{Seq}$ is a tree. Let f be a function in ω^ω such that $f \notin [T]$. Then there is an $n \in \omega$ such that $f[n] \notin T$. Hence f has an open neighborhood $U_\sigma = \{g \mid \sigma \subset g\}$ disjoint from $[T]$, where $\sigma = f[n]$. Therefore $[T]$ is closed.

Conversely, let C be a closed set. Then the set

$$T_C = \{\sigma \in \text{Seq} \mid \sigma \subset f \text{ for some } f \in C\}$$

is a tree. Suppose $f \in [T_C]$, that is, $f[n] \in T_C$ for all $n \in \omega$. This implies that for each n there is a $g \in C$ such that $g[n] = f[n]$ Since C is closed, it follows that $f \in C$. Therefore $C = [T_C]$. $\square$

Definition 2.8.4 (tidy trees). A tree T is *tidy* if for all $\sigma \in T$ there is a τ in T such that $\sigma \subsetneqq \tau$. Note that a tidy tree has no "dead ends."

Definition 2.8.5 (perfect trees). A tree T is *perfect* if for any $\sigma \in T$ there exist $\tau_1, \tau_2 \in T$ such that $\tau_1 \mid \tau_2$, $\sigma \subset \tau_1$, and $\sigma \subset \tau_2$. A node $\sigma \in T$ is called a *branching node* if $\sigma^\frown\langle i\rangle \in T$ and $\sigma^\frown\langle j\rangle \in T$ for some $i, j \in \omega$, $i \neq j$.

Remark 2.8.6. Every perfect tree is tidy, but not every tidy tree is perfect. Every recursive tidy tree $T \subseteq \omega^\omega$ has a recursive path, e.g., the *leftmost path*, defined by $f(n) =$ the least i such that $f[n]^\frown\langle i\rangle \in T$, for all $n \in \omega$.

Remark 2.8.7. The construction in the proof of Proposition 2.8.3 gives a one-to-one correspondence $C \mapsto T_C$ between nonempty closed sets in ω^ω and tidy trees in Seq. Under this correspondence, nonempty perfect closed subsets of ω^ω correspond to perfect trees in Seq.

We now return to degrees of unsolvability.

Definition 2.8.8. A Turing degree $\mathbf{a}$ is said to be *minimal* if $\mathbf{a} > \mathbf{0}$ and for all $\mathbf{b} \leq \mathbf{a}$ either $\mathbf{b} = \mathbf{0}$ or $\mathbf{b} = \mathbf{a}$.

Definition 2.8.9. A Turing degree $\mathbf{a}$ is said to be *almost recursive* if every total function recursive in $\mathbf{a}$ is bounded pointwise by a total recursive function. For historical reasons such Turing degrees are also known as *hyperimmune-free*, but we will not use this terminology.

Theorem 2.8.10. There is a Turing degree $\mathbf{a}$ such that $\mathbf{a}$ is minimal. In addition, $\mathbf{a}$ is almost recursive.

Proof. The proof uses Sacks trees, which are defined as follows.

Definition 2.8.11 (Sacks trees). A *Sacks tree* is a recursive, perfect subtree of Seq_2.

Remark 2.8.12. Clearly Seq_2 is itself a Sacks tree. Moreover, every Sacks tree "looks like" Seq_2, i.e., if $T \subseteq \text{Seq}_2$ is a Sacks tree then $[T]$ is recursively homeomorphic to $2^\omega = [\text{Seq}_2]$.

Definition 2.8.13. If T is a Sacks tree and $\sigma \in T$, put

$$T^\sigma = \{\tau \in T \mid \sigma \subseteq \tau \vee \tau \subseteq \sigma\}.$$

Note that T^σ is again a Sacks tree.

We will construct a sequence of Sacks trees $T_n \subseteq \mathrm{Seq}_2$, $n \in \omega$, which is *descending*, i.e., for all n, $T_{n+1} \subseteq T_n$. The intersection $\bigcap_n [T_n]$ will consist of a single function $f \in 2^\omega$. The set A for which $f = \chi_A$ will have the desired Turing degree. The construction will proceed by stages.

Stage 0. Let $T_0 = \mathrm{Seq}_2$.

Stage 3e+1. At this stage, we will ensure that $\{e\} \neq \chi^A$. Let σ be a branching node in T_{3e} and let $n = \mathrm{lh}(\sigma)$. If $\{e\}(n)\uparrow$, let $T_{3e+1} = T_{3e}$. Otherwise, let τ be an immediate extension of σ such that $\tau(n) \neq \{e\}(n)$ and let $T_{3e+1} = T_{3e}^\tau$. For any $f \in [T_{3e+1}]$, it is clear that $f \neq \{e\}$.

Stage 3e+2. At this stage, we ensure that for any path f through T_{3e+1}, if $\{e\}^f$ is a total function then $\{e\}^f$ is bounded by a recursive function. We split this stage of the construction into two complementary cases.

Case 1: There is some $n \in \omega$ and some $\tau \in T_{3e+1}$ such that for all $\sigma \in T_{3e+1}$ extending τ, $\{e\}^\sigma(n)\downarrow$. In this case, let $T_{2e+2} = T_{3e+1}^\sigma$.

Case 2: Case 1 is false. In this case, for all n and for all $\tau \in T_{3e+1}$, there is some $\sigma \in T_{3e+1}$ for which $\{e\}^\sigma(n)\downarrow$. We next construct a monotone function $\psi : \mathrm{Seq}_2 \to T_{3e+1}$; we will define $\psi(\sigma)$ by induction on the length of σ. Let $\psi(\emptyset)$ be the element $\tau \in T_{3e+1}$ with least Gödel number such that $\{e\}^\tau(0)\downarrow$ and τ is a branching node. Let $\psi(\sigma^\frown\langle 0\rangle)$ be the element $\tau \in T_{3e+1}$ with least Gödel number such that τ is a branching node, $\psi(\sigma)^\frown\langle 0\rangle \subseteq \tau$, and $\{e\}^\tau(n)\downarrow$. Let $\psi(\sigma^\frown\langle 1\rangle)$ be the element $\tau \in T_{3e+1}$ with least Gödel number such that τ is a branching node, $\psi(\sigma)^\frown\langle 1\rangle \subseteq \tau$, and $\{e\}^\tau(n)\downarrow$. It is clear that $\psi(\sigma)$ is a recursive function defined for all $\sigma \in \mathrm{Seq}_2$.

Let T_{3e+2} be the downward closure of the range of ψ, that is, $T_{3e+2} = \{\tau \in T_{3e+1} \mid \exists\sigma \in \mathrm{Seq}_2\,(\tau \subseteq \psi(\sigma))\}$. This is a recursive set, because if there is any σ such that $\tau \subseteq \psi(\sigma)$ then there some such σ of length less than or equal to $\mathrm{lh}(\tau)$ with this property, so the quantifier is bounded. Hence T_{3e+2} is a Sacks tree.

This completes the construction at stage $3e+2$. Now suppose that $f \in [T_{3e+2}]$ and $\{e\}^f$ is a total function recursive in f. If this occurs, the construction must have followed case 2. Let $g(n) = \max\{\{e\}^{\psi(\sigma)}(n) \mid \sigma \in 2^n$. Then $f(n) \leq_T g(n)$, because $\{e\}^f(n) = \{e\}^{f[\mathrm{lh}(\psi(f[n]))]}$.

Stage 3e+3. At this stage, we will ensure that if $f \in [T_{3e+3}]$ and $g = \{e\}^f$ is a total recursive function then either g is recursive or $f \leq_T g$.

Case 1: For some $\sigma \in T_{3e+2}$ and for some n, $\{e\}^\sigma(n)\uparrow$. In this case, let $T_{3e+3} = T_{3e+2}^\sigma$.

In the remaining two cases, we assume case 1 was false. This implies that for every $\sigma \in T_{3e+2}$ and for every n, $\{e\}^\sigma(n)\downarrow$.

Case 2: Case 1 fails, and the following condition holds: For every $\sigma \in T_{3e+2}$ there is some n and a pair of incompatible elements $\tau_1, \tau_2 \in (T_{3e+2})_\sigma$ such that $\{e\}^{\tau_1}(n) \neq \{e\}^{\tau_2}(n)$.

We construct a monotone function $\psi : \mathrm{Seq}_2 \to T_{3e+2}$, defining $\psi(\sigma)$ by induction on the length of σ. Let $\psi(\langle\rangle) = \langle\rangle$. Let $\psi(\sigma^\frown\langle 0\rangle)$ and $\psi(\sigma^\frown\langle 1\rangle)$ be the least pair of elements of Seq_2 witnessing that the defining condition of Case 2 holds for σ. For any σ, these elements of T_{3e+2} can be found by searching, so ψ is recursive and defined for all $\sigma \in \mathrm{Seq}_2$.

To finish the construction, let $T_{3e+2} = \{\tau \mid \exists\sigma\,(\tau \subseteq \psi(\sigma))\}$. It can be seen that this is a Sacks tree.

Case 3: Neither case 1 nor case 2 holds. Hence there is some $\sigma \in T_{3e+2}$ such that for all n and for all $\tau_1, \tau_2 \in (T_{3e+2})_\sigma$, $\{e\}^{\tau_1}(n) \downarrow\simeq \{e\}^{\tau_2}(n)$. In this case, let $T_{3e+3} = T^\sigma_{3e+2}$.

This completes the construction for stage $3e+3$. Choose $f \in [T_{3e+3}]$ such that $\{e\}^f$ is a total function. Since $\{e\}^f$ is a total function, the construction above followed case 2 or 3. These constructions were chosen to control the functional $\Psi : [T_{3e+3}] \ni f \mapsto \{e\}^f \in 2^\omega$. If the construction followed case 2, then Ψ is injective. This implies that we can compute $f(n)$ from $\{e\}^f$, by computing $\{e\}^\sigma \in \mathrm{Seq}_2$ for longer and longer σ until we have found a σ of some length $m \geq n$ such that $\{e\}^\sigma \subseteq \{e\}^f$. If the construction followed case 3, then Ψ is constant. This implies $\{e\}^f$ is recursive; for any recursive $g \in T_{3e+3}$, $\{e\}^f = \{e\}^g$.

We have completed the description of the three stages of the construction. It is clear that $\cap[T_n]$ contains a single path f. Let $A \subseteq \omega$ be the set such that $f = \chi_A$. We claim that A satisfies the conclusions of the theorem. The set A cannot be recursive; for any e, $\chi_A \neq \{e\}$ because of the construction at stage $3e$. Suppose that $g = \{e\}^A$ is a total recursive function. By the construction at stage $3e+1$, g is bounded by a total recursive function. Therefore A is almost recursive. Finally, because of the construction at stage $3e+3$, either g is recursive, or $f \leq_T g$. Therefore $\deg_T(A)$ is minimal. $\square$

2.9 Sacks forcing

In this section, we will introduce the idea of forcing by using Sacks trees. We begin by defining the relevant structures.

Definition 2.9.1. Let $\mathcal{P}$ denote the partial order of Sacks trees ordered by inclusion.

Remark 2.9.2. It is common for a partial order to be referred to as a *notion of forcing*, and its elements to be referred to as *conditions*.

Definition 2.9.3 (dense sets). A set $\mathcal{D} \subseteq \mathcal{P}$ is said to be *dense* if for all $P \in \mathcal{P}$ there exists $Q \in \mathcal{D}$ such that $Q \subseteq P$. We say $f \in \omega^\omega$ *meets* $\mathcal{D}$ if and only if there exists $P \in \mathcal{D}$ such that $f \in [P]$.

Definition 2.9.4 (genericity). $\mathcal{D} \subseteq \mathcal{P}$ is said to be *arithmetical* if $\{e \mid \{e\} = \chi_P$ for some $P \in \mathcal{D}\}$ is arithmetical. We say $g \in 2^\omega$ is *Sacks generic* if g meets every dense arithmetical set $\mathcal{D} \subseteq \mathcal{P}$.

Lemma 2.9.5. For every $P \in \mathcal{P}$, there exists a Sacks generic $g \in [P]$.

Proof. Let $\langle \mathcal{D}_n \rangle_{n\in\omega}$ be an enumeration of the arithmetical dense subsets of $\mathcal{P}$. We define a sequence $\langle P_n \rangle_n$ of Sacks trees by letting $P_0 = P$ and letting P_{n+1} be a tree such that $P_{n+1} \subseteq P_n$ and $P_{n+1} \in \mathcal{D}_n$. Finally, let g be the unique element of $\bigcap_{n\in\omega}[P_n]$. $\square$

Theorem 2.9.6. For every Sacks generic $g \in 2^\omega$, we have

1. $\deg_T(g)$ is minimal, and
2. $\deg_T(g)$ is almost recursive.

Proof. We will only prove that $\deg_T(g)$ is almost recursive. To do this, we will show how the proof of Theorem 2.8.10 can be recast in terms of forcing. The proof that $\deg_T(g)$ is minimal follows similarly.

For $P \in \mathcal{P}$, Let $\mathrm{Br}(P)$ denote the set of *branching nodes* of P,

$$\mathrm{Br}(P) = \{\sigma \in P \mid \sigma^\frown\langle 0\rangle \in P \wedge \sigma^\frown\langle 1\rangle \in P\}.$$

Let $\mathrm{Br}_n(P)$ be the set of nth-level branching nodes of P. That is, $\sigma \in \mathrm{Br}_n(P)$ if and only if $\sigma \in \mathrm{Br}(P)$ and there are exactly n proper initial segments of σ in $\mathrm{Br}(P)$.

For each $e \in \omega$ we define $\mathcal{D}_e \subseteq \mathcal{P}$ by

$$\mathcal{D}_e = \{P \in \mathcal{P} \mid \exists n\, \forall \sigma \in P\, \{e\}^\sigma(n) \uparrow\, \vee \forall n\, \forall \sigma \in \mathrm{Br}_n(P)\, \{e\}^\sigma(n) \downarrow\}.$$

We first show that for each e, $\mathcal{D}_e$ is dense. Given $Q \in \mathcal{P}$ we have the following two cases:

Case 1: There is an n and a $\sigma \in Q$ such that for every $\tau \in Q$ extending σ, $\{e\}^\tau(n) \uparrow$. In this case we let $P = Q^\sigma$. It follows by construction that $P \in \mathcal{D}_e$ and $P \subseteq Q$.

Case 2: Case 1 fails. Then for all n and all $\sigma \in Q$, there exists $\tau \in Q$ extending σ such that $\{e\}^\tau(n) \downarrow$. In this case we define a recursive $h : 2^{<\omega} \to Q$, where $\{e\}^{h(\sigma)}(n) \downarrow$ for all $\sigma \in 2^{<\omega}$ and $\mathrm{lh}(\sigma) = n$. It follows from this definition that $\sigma_1 \subseteq \sigma_2 \iff h(\sigma_1) \subseteq h(\sigma_2)$. So we can define

$$P = \{\tau \in Q \mid \exists \sigma \in 2^{<\omega}\, \tau \subseteq h(\sigma)\}.$$

Then $P \in \mathcal{D}_e$ and $P \subseteq Q$. This proves our claim. Therefore $\mathcal{D}_e$ is dense.

Let g be Sacks generic. We will show that g is almost recursive. Let f be a total function recursive in g, so $f = \{e\}^g$ for some e. Since $\mathcal{D}_e$ is dense, g meets $\mathcal{D}_e$. The construction of $\mathcal{D}_e$ allows us to compute a total recursive function h which bounds every such f, so g is almost recursive. Let P be a Sacks tree in $\mathcal{D}_e$ such that g is a path through P. To compute $h(n)$ we do the following: First, find the finite set $\mathrm{Br}_n(P)$ of nth level branching nodes. This can be done recursively since P is a recursive tree in Seq_2. Call this set $\mathrm{Br}_n(P) = \{\sigma_j \mid 1 \leq j \leq 2^n\}$. Let $h(n) = \max_j \{e\}^{\sigma_j}(n)$. It follows from the constriction of $\mathcal{D}_e$ that all the computations involved in computing $h(n)$ will halt. So h is a total recursive function. Moreover, $h(n)$ bounds $f(n)$ because $f(n) = \{e\}^g(n) = \{e\}^\sigma(n)$ where σ is the nth level branching node in P which g extends. $\square$

We now introduce forcing and state its key properties.

Definition 2.9.7 (the forcing language). The *forcing language* is $L = \{+, \cdot, 0, 1, <, =, \underline{g}\}$, i.e., the language of arithmetic with an added 1-place function symbol $\underline{g}$. If $g \in 2^\omega$ and if φ is an L-sentence, we say that g *satisfies* φ, written $g \models \varphi$, if φ is true in the L-structure $(\omega, +, 0, 1, \cdot, =, <, g)$.

Definition 2.9.8 (forcing). Let $P \in \mathcal{P}$. Let φ be a sentence of the forcing language. We say P *forces* φ, written $P \Vdash \varphi$, if every generic g in $[P]$ satisfies φ.

Theorem 2.9.9 (definability of forcing). For each formula $\varphi(x_1, \ldots, x_k)$ the set $\{\langle P, n_1, \ldots, n_k\rangle \mid P \Vdash \varphi(n_1, \ldots, n_k)\}$ is arithmetical.

Theorem 2.9.10 (forcing equals truth). If g is generic, then $\langle \omega, +, \cdot, 0, 1, <, =, g\rangle \models \varphi$ if and only if there is some $P \in \mathcal{P}$ such that $g \in [P]$ and $P \Vdash \varphi$.

To prove Theorems 2.9.9 and 2.9.10, we introduce a relation $\Vdash_s$ known as the *strong forcing* relation. We will restate the theorems replacing forcing by strong forcing, and prove these new theorems. Then we will show that the forcing relation is definable in terms of the strong forcing relation, which will allow us to prove Theorems 2.9.9 and 2.9.10.

Remark 2.9.11. Forcing is preserved under logical equivalence. I.e., if $\varphi_1 \equiv \varphi_2$ then $P \Vdash \varphi_1 \iff P \Vdash \varphi_2$. We shall see that strong forcing is not preserved under logical equivalence.

Definition 2.9.12 (strong forcing). Let $P \in \mathcal{P}$ and let φ be an L-sentence. We define the relation $P \Vdash_s \varphi$ by induction on formulas as follows:

$$\begin{aligned}
P \Vdash_s (m_1 + m_2 = m_3) \quad &\equiv \quad m_1 + m_2 = m_3\\
P \Vdash_s (m_1 \cdot m_2 = m_3) \quad &\equiv \quad m_1 \cdot m_2 = m_3\\
P \Vdash_s f(m) = n \quad &\equiv \quad f(m) = n \text{ for all } f \in [P]\\
P \Vdash_s m < n \quad &\equiv \quad m < n\\
P \Vdash_s m = n \quad &\equiv \quad m = n\\
P \Vdash_s \varphi_1 \vee \varphi_2 \quad &\equiv \quad P \Vdash_s \varphi_1 \text{ or } P \Vdash_s \varphi_2\\
P \Vdash_s \neg\varphi \quad &\equiv \quad \neg\,\exists Q \subseteq P\,(Q \Vdash_s \varphi)\\
P \Vdash_s \exists n\,\varphi(n) \quad &\equiv \quad P \Vdash_s \varphi(n) \text{ for some } n.
\end{aligned}$$

Lemma 2.9.13. If $P \Vdash_s \varphi$ and $Q \subseteq P$ then $Q \Vdash_s \varphi$

Proof. The proof follows from a straightforward induction on φ. ☐

Lemma 2.9.14 (definability of strong forcing). Let $\varphi(n_1, \ldots, n_k)$ be an L-formula. The set of all tuples $\langle P, n_1, \ldots, n_k\rangle$ such that $P \Vdash_s \varphi(n_1, \ldots, n_k)$ is arithmetical.

Proof. The proof follows from a straightforward induction on φ. ☐

Lemma 2.9.15. If $P, Q \in \mathcal{P}$ and g is a generic element of $[P] \cap [Q]$ then there exists $R \in \mathcal{P}$ such that $R \subseteq P \cap Q$ and $g \in [R]$.

Proof. Let P, Q, g be as in the hypotheses of the lemma. Define $\mathcal{D}_P$ and $\mathcal{D}_Q$ as follows:

$$\begin{aligned}\mathcal{D}_P &= \{R \in \mathcal{P} \mid R \subseteq P \text{ or } Br_0(R) \cap P = \emptyset\},\\ \mathcal{D}_Q &= \{R \in \mathcal{P} \mid R \subseteq Q \vee R_P(R) \cap Q = \emptyset\}.\end{aligned}$$

It can be seen that $\mathcal{D}_P \cap \mathcal{D}_Q$ is dense and arithmetical. Therefore g meets $\mathcal{D}_P \cap \mathcal{D}_Q$, which establishes the result. □

Lemma 2.9.16 (strong forcing equals truth). Let $g \in 2^\omega$ be generic and let φ be a sentence of the forcing language. Then $g \models \varphi$ if and only if there exists $P \in \mathcal{P}$ such that $g \in [P]$ and $P \Vdash_s \varphi$.

Proof. The proof proceeds by induction on sentences of the forcing language. If φ is atomic, the result follows immediately from the definition of strong forcing.

Suppose $\varphi = \psi_0 \vee \psi_1$. Since g satisfies φ, g satisfies either ψ_0 or ψ_1. Therefore, by induction, there is a P such that $g \in [P]$ and $P \Vdash_s \psi_0$ or $P \Vdash_s \psi_1$. Therefore there is a P with $g \in [P]$ such that $P \Vdash_s \varphi$.

Suppose the $\varphi = \neg\psi$. Assume that $P \Vdash_s \neg\psi$; we want to show that $g \models \neg\psi$. Towards a contradiction, suppose $g \models \psi$. By induction it follows that g is in some Sacks tree Q such that $Q \Vdash_s \psi$. By Lemma 2.9.15, there is an R extending P and Q. By Lemma 2.9.13, $R \Vdash_s \psi$. This contradicts the assumption that $P \Vdash \neg\psi$.

For the other direction, suppose $g \models \neg\psi$. We want to show that g is a path through some tree P such that $P \Vdash_s \neg\psi$. Let $\mathcal{D} = \{P \mid P \Vdash_s \psi \vee P \Vdash_s \neg\psi\}$. Since $\mathcal{D}$ is dense and arithmetical, g meets $\mathcal{D}$. This finishes the induction in the case that $\varphi = \neg\psi$.

Finally, suppose that $\varphi = \exists n\, \psi(n)$. We want to show $g \models \exists n\, \psi(n)$ iff there is some $P \in \mathcal{P}$ such that $g \in [P]$ and $P \Vdash_s \exists n\, \psi(n)$. First, assume that g satisfies $\exists n\, \psi(n)$. Fix an n such that g satisfies $\psi(n)$. Using induction on P, it follows that there is a P such that $X \in [P]$ and $P \Vdash_s \psi(n)$. Therefore $P \Vdash_s \exists n\, \psi(n)$. For the reverse implication, assume that $P \Vdash_s \exists n\, \psi(n)$ and $X \in [P]$. Then $P \Vdash_s \psi(n)$ for some fixed n. By induction by P, $g \models \psi(n)$. Therefore $g \models \exists n\, \psi(n)$. □

Lemma 2.9.17. Let P be a Sacks tree and φ be a sentence of the forcing language. Then $P \Vdash \varphi$ if and only if $\{R \subseteq P \mid R \Vdash_s \varphi\}$ is dense below P. That is, $P \Vdash \varphi$ if and only if $P \Vdash_s \neg\neg\varphi$.

Proof. First, assume that $\mathcal{D} = \{R \subseteq P \mid R \Vdash_s \varphi\}$ is dense below P. We want to show $P \Vdash \varphi$. Let $g \in [P]$ be generic. Then $g \in [R]$, $R \subseteq P$ and $R \Vdash_s \varphi$. Therefore $g \models \varphi$. Thus $P \Vdash \varphi$. Next, assume that $P \Vdash \varphi$. We want to show that $\mathcal{D}$ is dense below P. Given $Q \subseteq P$, let $g \in [Q]$ be generic. Now $g \models \varphi$ because $g \in P$ and $P \Vdash \varphi$. Therefore there is an R such that $g \in [R]$ and $R \Vdash_s \varphi$. By Lemma 2.9.15, there is an $R' \subseteq R \cap Q$ such that $X \in [R']$. It follows that $R' \subseteq Q$, $R' \Vdash_s \varphi$ and $R' \in D$. We have shown that D is dense below P. □

We have now proved the basic properties of forcing. Next we present an application of forcing to the study of definability over the standard model of arithmetic, $(\omega, +, \cdot, 0, 1, <, =)$.

Definition 2.9.18 (implicit arithmeticity). A set $A \subseteq \omega$ is said to be *implicitly arithmetical* if it is implicitly definable over $(\omega, +, \cdot, 0, 1, <, =)$. In other words, there is a sentence φ in the language $L = \{+, \cdot, 0, 1, <, =, \underline{f}\}$ such that A is the unique subset of ω such that $(\omega, +, \cdot, 0, 1, <, =, \chi_A)$ satisfies φ.

Lemma 2.9.19. No generic real is implicitly arithmetical.

Proof. Suppose g were Sacks generic and implicitly arithmetical. Let φ be an L-sentence such that g is the unique member of 2^ω satisfying φ. By the forcing-equals-truth theorem, there exists P such that $g \in [P]$ and $P \Vdash \varphi$. Let $h \in [P]$ be a generic element not equal to g. Then h satisfies φ. This contradicts the assumption that only g satisfies φ. $\square$

Remark 2.9.20. Lemma 2.9.19 can be strengthened slightly. A variant of the proof shows that no countable arithmetically definable set of reals contains a generic real. Tanaka [19] has shown that every countable arithmetical set of reals contains an implicitly arithmetical real. Harrington [4] has constructed a countable arithmetical set of reals which contains a real which is not implicitly arithmetical.

Lemma 2.9.21. The set $0^{(\omega)} = \{2^m 3^n \mid m \in 0^{(n)}\}$ is implicitly arithmetical. Note that $0^{(\omega)}$ is essentially just the truth set for first order arithmetic.

Proof. We prove this by exhibiting a sentence φ which defines $0^{(\omega)}$. For any $A \subseteq \omega$ let $(A)_n$ denote the set $\{m \mid 2^m 3^n \in A\}$. We define φ as follows:

$$\varphi \equiv \forall n \, n \notin (A)_0 \wedge \forall n \, (A)_{n+1} = (A)'_n \wedge \forall j \in A \, \exists m \, \exists n \, j = 2^m 3^n.$$

The first conjunct says that $(A)_0$ is empty, the second that $(A)_{n+1}$ is the Turing jump of $(A)_n$, and the third that $A = \{2^m 3^n \mid m \in (A)_n\}$. $\square$

Lemma 2.9.22. There is a Sacks generic real $g \leq_T 0^{(\omega)}$.

Proof. This is just a more precise version of Lemma 2.9.5 stating the existence of a Sacks generic real. The key point is that $0^{(\omega)}$ can decide if an arithmetical subset of $\mathcal{P}$ is dense. $\square$

Theorem 2.9.23. There exist $f, g \in 2^\omega$ such that $g \leq_T f$, f is implicitly arithmetical, and g is not implicitly arithmetical.

Proof. Let g be a Sacks generic real recursive in $0^{(\omega)}$. Then g is not implicitly arithmetical, but g is Turing reducible to the implicitly arithmetical set $0^{(\omega)}$. $\square$

2.10 Homogeneity of Sacks forcing

Sacks forcing has the following homogeneity property.

Lemma 2.10.1 (homogeneity). Let $P, Q \in \mathcal{P}$ be Sacks trees, i.e., recursive perfect subtrees of $2^{<\omega}$. Then there is a recursive homeomorphism $F : [P] \cong [Q]$. Moreover, for all $g \in [P]$, g is Sacks generic if and only if $F(g)$ is Sacks generic.

Proof. Note that $\mathrm{Br}(P)$ and $\mathrm{Br}(Q)$ are recursive, because $\sigma \in \mathrm{Br}(P)$ if and only if both $\sigma^\frown\langle 0\rangle$ and $\sigma^\frown\langle 1\rangle$ both belong to P. There is an obvious recursive one-to-one correspondence between $\mathrm{Br}(P)$ and $\mathrm{Br}(Q)$. Namely, let $\mathrm{Br}_n(P) = \{\sigma_1, \ldots, \sigma_{2^n}\}$ and $\mathrm{Br}_n(Q) = \{\tau_1, \ldots, \tau_{2^n}\}$, both listed in lexicographic order. Then we can map σ_i to τ_i for $1 \leq i \leq 2^n$. This induces a one-to-one correspondence between paths in $[P]$ and paths in $[Q]$. Furthermore, this induces a one-to-one correspondence between $\{P' \in \mathcal{P} \mid P' \subseteq P\}$ and $\{Q' \in \mathcal{P} \mid Q' \subseteq Q\}$. $\square$

From the above homogeneity property, we obtain the following theorem.

Theorem 2.10.2. Let $S \subseteq 2^\omega$ be arithmetical and closed under $\equiv_T$. Then the set of Sacks generic reals is either included in S or disjoint from S.

Proof. We have

$$S = \{f \in 2^\omega \mid (\omega, +, \cdot, 0, 1, =, <, f) \models \varphi\}$$

for some sentence φ. We will first prove the following claim: For all P and Q, $P \Vdash \varphi$ if and only if $Q \Vdash \varphi$. To prove this, let $F : P \cong Q$ be a recursive homeomorphism as in Lemma 2.10.1. Then $\{g \in [P] \mid g \text{ is Sacks generic}\}$ is recursively homeomorphic to $\{F(g) \in [Q] \mid g \text{ is Sacks generic}\} = \{h \in [Q] \mid h$ is Sacks generic$\}$. Moreover, $F(g) \equiv_T g$ because $F : [P] \to [Q]$ and $F^{-1} : [Q] \to [P]$ are recursive functionals. Our claim now follows from the definition of forcing.

Now suppose g and h are Sacks generic. By the forcing-equals-truth lemma, let $g \in P$ such that $P \Vdash \varphi$ or $P \Vdash \neg\varphi$, and let $h \in [Q]$ such that $Q \Vdash \varphi$ or $Q \Vdash \neg\varphi$. Since $P \Vdash \varphi \iff Q \Vdash \varphi$, g satisfies φ if and only if h satisfies φ. Thus, $g \in S$ if and only if $h \in S$. $\square$

Remark 2.10.3. The previous theorem implies that $\{S \mid S$ contains every generic real$\}$ is an ultrafilter on the Boolean algebra of arithmetical subsets of 2^ω which are closed under Turing equivalence. Furthermore, we could weaken Turing equivalence to truth-table equivalence, because $F(g)$ is actually truth-table equivalent to g.

Example 2.10.4. As a typical consequence of Theorem 2.10.2, either all or no Sacks generic Turing degrees satisfy $\mathbf{a}' = \mathbf{a} \vee \mathbf{0}'$. Which is it?

2.11 Cohen genericity

Definition 2.11.1. A *Cohen forcing condition* is an element of Seq_2. We define a partial order $\leq$ on these conditions by letting $\sigma \leq \tau$ if and only if $\tau \subseteq \sigma$. We say that $D \subseteq 2^{<\omega}$ is *dense* if for all $\sigma \in 2^{<\omega}$ there exists $\tau \in D$ such that $\tau \supseteq \sigma$. We say that f *meets* D if $f \supset \sigma$ for some $\sigma \in D$. We say that $g \in 2^\omega$ is *Cohen generic* if g meets D for all dense arithmetical $D \subseteq 2^\omega$.

Compare this to the Kleene/Post construction of f by finite approximations.

Forcing with Cohen conditions is defined exactly as for Sacks forcing; i.e., $\sigma \Vdash \varphi$ if and only if for all Cohen generic $g \in 2^\omega$ such that $g \supset \sigma$, g satisfies φ. The definability-of-forcing and the forcing-equals-truth lemmas follow for Cohen forcing just as they did for Sacks forcing.

Lemma 2.11.2 (homogeneity). For all $\sigma, \tau \in 2^{<\omega}$ there is a recursive one-to-one correspondence between $\{g \in 2^\omega \mid g \supset \sigma, g \text{ Cohen generic}\}$ and $\{h \in 2^\omega \mid h \supset \tau, h \text{ Cohen generic}\}$.

Proof. Simply map the set of all paths above σ to the set of paths above τ using the lexicographic ordering. □

Theorem 2.11.3. If $S \subseteq 2^\omega$ is arithmetical and closed under Turing equivalence, then $\{g \in 2^\omega \mid g \text{ Cohen generic}\}$ is either included in S or disjoint from S.

Proof. The proof follows as in the case of Sacks forcing, using homogeneity. □

Remark 2.11.4. Instead of assuming that S is closed under $\equiv_T$, it would suffice to assume that S is closed under the equivalence relation $f \equiv g \iff \exists m \, \forall n > m \, f(n) = g(n)$.

Remark 2.11.5. There are many kinds of forcing in recursion theory. Sacks forcing and Cohen forcing are only two examples.

Chapter 3

Models of set theory

3.1 Countable transitive models

Remark 3.1.1. We will be concerned only with pure, well founded sets. A set x is said to be *pure* if all of the elements of x, elements of elements of x, etc., are sets. A set x is said to be *well founded* if it is not the beginning of an infinite descending $\in$-sequence, i.e., there is no infinite sequence $x = x_0 \ni x_1 \ni \cdots \ni x_n \ni x_{n+1} \ni \cdots$.

Definition 3.1.2. A set M is said to be *transitive* if, for all $x \in M$, $x \subseteq M$. That is, for any element x of M, the elements of x are also elements of M. Equivalently we could say that, for all $x \in M$ and $y \in x$, $y \in M$.

Definition 3.1.3. Let $L = \{\in, =\}$ be the language of set theory. A nonempty transitive set M may be identified with the L-structure

$$(M, \in|M, =|M)$$

where $\in|M = \{\langle a, b\rangle \mid a \in b \in M\}$ and $=|M = \{\langle a, a\rangle \mid a \in M\}$. Thus, for any L-sentence φ with parameters from M, we have either $M \models \varphi$ or $M \models \neg\,\varphi$.

Definition 3.1.4. ZF is the L-theory consisting of the Zermelo/Fraenkel axioms of set theory. ZFC is the L-theory consisting of ZF plus the Axiom of Choice.

Remark 3.1.5. In what follows, we shall assume the existence of a *countable transitive model of* ZFC, i.e., a countable transitive set M such that $M \models \mathsf{ZFC}$.

3.2 Models constructed by forcing

Let M be a countable transitive model of ZFC. Let $(P, \leq) \in M$ be a partial ordering which is an element of M. The elements of P will be called *forcing conditions*, or simply *conditions*. P will be called a *notion of forcing*.

Definition 3.2.1 (generic filter). A set $D \subseteq P$ is said to be *dense* if for all $p \in P$ there exists $q \in D$ such that $q \leq p$. A *filter* is a set $G \subseteq P$ such that

1. $\forall p \in G \, \forall q \in P \, (p \leq q \Rightarrow q \in G)$.
2. $\forall p, q \in G \, \exists r \in G \, (r \leq p \wedge r \leq q)$.

A filter G is said to be *generic*, or *M-generic*, if $G \cap D \neq \emptyset$ for all dense $D \in M$.

Lemma 3.2.2. Given $p \in P$, there exists a generic filter G such that $p \in G$.

Proof. Since M is countable, let $\langle D_n \mid n \in \omega \rangle$ be an enumeration of the dense sets which belong to M. Given $p \in P$, construct a sequence

$$p = p_0 \geq p_1 \geq \cdots \geq p_n \geq p_{n+1} \geq \cdots$$

where $p_0 = p$ and p_{n+1} is chosen recursively to be any $q \leq p_n$ such that $q \in D_n$. Put $G = \{q \mid \exists n \, (p_n \leq q)\}$. Clearly $p \in G$, and it is easy to check that G is a generic filter. $\square$

Remark 3.2.3. If P is linear, then clearly $G = P$, hence $G \in M$. The typical situation will be that P is a partial ordering which is not linear, and $G \notin M$. For example, see Section 3.3 below.

Definition 3.2.4. We use a generic filter G to define a transitive model $M[G]$ as follows:

$$M[G] = \{a_G \mid a \in M\}$$

where

$$a_G = \{b_G \mid (p, b) \in a \text{ for some } p \in G\}.$$

Thus the elements of M are regarded as "terms" denoting elements of $M[G]$. Namely, $a \in M$ denotes $a_G \in M[G]$.

Remark 3.2.5. Note that the definition of a_G is carried out by transfinite recursion on the rank of a. The rank has a few basic properties that make it ideal for transfinite recursion:

1. Every set has a rank.
2. The rank of the elements of a set are lower than the rank of the set itself.

Formally, the rank of a set is defined by transfinite recursion as

$$\text{rank}(a) = \sup\{\text{rank}(b) + 1 \mid b \in a\}.$$

Theorem 3.2.6. *$M[G]$ is a countable transitive model of ZFC. Moreover, it is the smallest transitive model of ZFC containing $M \cup \{G\}$.*

We omit the proof of this theorem. For details of the proof, see Shoenfield's classic expository paper [15].

Remark 3.2.7. We refer to $M[G]$ as a model of ZFC which is *constructed by forcing* over M. We shall see that, by cleverly choosing the partial ordering P, we can control $M[G]$ and cause it to satisfy various properties such as the Continuum Hypothesis ($2^{\aleph_0} = \aleph_1$) or its negation. This is an important methodology for independence results in set theory.

Remark 3.2.8. Even though $M[G]$ is a proper extension of M, the "person living in M" has a very good understanding of $M[G]$. This is because of the definability of forcing, as we shall now explain.

Definition 3.2.9 (the forcing language). The *forcing language* is $L_M = L \cup M$, that is the language of set theory plus a constant symbol for each element of M. Thus we have $L_M = \{\in, =, a, b, \ldots\}$ as the forcing language, where $a, b, \ldots \in M$. A typical sentence of L_M is $\varphi(a_1, \ldots, a_n)$, where $\varphi(x_1, \ldots, x_n)$ is a formula in L with free variables $x_1, \ldots, x_n$, and $a_1, \ldots, a_n \in M$. Recall that $a \in M$ denotes $a_G \in M[G]$.

Definition 3.2.10 (forcing). If $p \in P$, we say that $p \Vdash \varphi(a_1, \ldots, a_n)$ if $M[G] \models \varphi((a_1)_G, \ldots, (a_n)_G)$ for all generic G such that $p \in G$.

Theorem 3.2.11 (definability of forcing). If $\varphi(x_1, \ldots, x_n)$ is an L-formula with free variables $x_1, \ldots, x_n$, then

$$\{\langle p, a_1, \ldots, a_n \rangle \mid p \Vdash \varphi(a_1, \ldots, a_n)\} \subseteq P \times M^n$$

is a definable class over M (using P as a parameter).

Theorem 3.2.12 (forcing equals truth). If φ is a sentence of the forcing language and G is a generic filter, then $M[G] \models \varphi$ if and only if there exists $p \in G$ such that $p \Vdash \varphi$.

Remark 3.2.13. The proofs of Theorems 3.2.11 and 3.2.12 are similar in outline and concept to the proofs already given for Sacks forcing in the recursion-theoretic context. New difficulties arise because we are dealing with set theory rather than arithmetic. Theorems 3.2.11 and 3.2.12 are used in proving Theorem 3.2.6, that $M[G]$ is a model of ZFC.

3.3 An example: Cohen forcing

Let M be a countable transitive model of ZFC. Let $P = \mathrm{Seq}_2 = 2^{<\omega}$, partially ordered by $\sigma \leq \tau$ if and only if $\sigma \supseteq \tau$. Note that the partial ordering $(P, \leq)$ is an element of M. Thus $(P, \leq)$ may be viewed as a notion of forcing. This particular partial ordering is known as *Cohen forcing*.

Let $G \subseteq P = \mathrm{Seq}_2$ be a generic filter. In particular, for all $\sigma, \tau \in G$ there exists $\rho \in G$ such that $\rho \supseteq \sigma$ and $\rho \supseteq \tau$. It follows that either $\sigma \subseteq \tau$ or $\tau \subseteq \sigma$. Thus G is linearly ordered under $\subseteq$.

Note that for each $n \in \omega$ the set $D_n = \{\sigma \in P \mid \mathrm{lh}(\sigma) \geq n\}$ is dense. Since G meets D_n for all n, we see that G is infinite. Since G is linearly ordered under

$\subseteq$, it follows that $g = \bigcup G$ is a path through Seq_2, i.e., a function in 2^ω. Note also that $G = \{g[n] \mid n \in \omega\}$. Thus $G \subseteq P$ and $g \in 2^\omega$ contain essentially the same information. We describe g as being *Cohen generic* over M.

We claim that $g \notin M$. To see this, suppose $g \in M$. Put $D_g = \{\sigma \in \text{Seq}_2 \mid \sigma \not\subset g\}$. Clearly D_g is dense. Moreover $D_g \in M$, since $g \in M$. Hence $G \cap D_g \neq \emptyset$, i.e., $g[n] \neq G$ for some n, a contradiction.

Since $g \notin M$, it follows that $G \notin M$, hence $M[G] \supsetneqq M$.

Thus we have the following theorem, which does not mention forcing. We do not know how to prove this theorem, except by means of forcing or some closely related technique.

Theorem 3.3.1. Let M be a countable transitive model of ZFC. Then there exists $M' \supsetneqq M$ such that M' is a sideways extension of M, and M' is a countable transitive model of ZFC.

3.4 Properties of generic extensions

Let M be a countable transitive model of ZFC, $(P, \leq)$ a partial order belonging to M, and G a generic filter on P. As discussed above we can create a new model of ZFC, $M[G]$ by adjoining G to the ground model M. We now discuss some basic, general properties of $M[G]$.

The following theorem states that $M[G]$ is a "sideways" extension of M: it includes $M \cup \{G\}$ but is of the same rank as M.

Theorem 3.4.1. Let M be a countable model of ZFC, $P \in M$ a partial ordering, and G a generic filter on P. Then $M[G]$ has the following properties:

1. $M \subseteq M[G]$.
2. $G \in M[G]$.
3. For all $a \in M$, $\text{rank}(a_G) \leq \text{rank}(a)$.

Thus $\text{rank}(M) = \text{rank}(M[G])$.

Proof.

1. For each $a \in M$ we construct a term $\check{a} \in M$ such that $\check{a}_G = a$, by transfinite recursion on the rank of a. Namely,

$$\check{a} = \{(p, \check{b}) \mid p \in P, b \in a\}$$

so that $\check{a}_G = \{\check{b}_G \mid (p, \check{b}) \in \check{a}, p \in G\} = \{b \mid b \in a\} = a$.

2. We construct a term $\dot{G} \in M$ such that $\dot{G}_G = G$. Namely,

$$\dot{G} = \{(p, \check{p}) \mid p \in P\}$$

so that $\dot{G}_G = \{\check{p}_G \mid (p, \check{p}) \in \dot{G}, p \in G\} = \{p \mid p \in G\} = G$.

3. Finally, we verify that $\text{rank}(a_G) \leq \text{rank}(a)$ for all $a \in M$. By transfinite induction on $\text{rank}(a)$, we have

$$\begin{aligned} \text{rank}(a_G) &= \sup\{\text{rank}(b_G) + 1 \mid b_G \in a_G\} \\ &\leq \sup\{\text{rank}(b) + 1 \mid (b, p) \in a \text{ for some } p \in P\} \\ &\leq \text{rank}(a). \end{aligned}$$

□

Next we note that the sideways extension $M[G]$ is usually a proper extension of M.

Definition 3.4.2. If $p_1, p_2 \in P$ and there is no $q \in P$ such that $q \leq p_1$ and $q \leq p_2$, we say p_1 and p_2 are *incompatible*, abbreviated $p_1 \perp p_2$.

Theorem 3.4.3. Suppose P is such that for all $p \in P$ there exist $p_1, p_2 \leq p$ such that $p_1 \perp p_2$. Then $G \notin M$, hence $M[G] \supsetneqq M$.

Proof. This is proved just as for the special case of Cohen forcing, in Section 3.3. If $G \in M$, then the complement $P \setminus G \in M$, and our assumption implies that $P \setminus G$ is dense in P. (Given $p \in P$, let $p_1, p_2 \leq p$ with $p_1 \perp p_2$. At most one of p_1, p_2 belongs to G, hence at least one of p_1, p_2 belongs to $P \setminus G$.) But then $G \cap (P \setminus G) \neq \emptyset$, a contradiction. □

3.5 Blowing up the continuum

The Continuum Hypothesis states that $2^{\aleph_0} = \aleph_1$. We use the symbol CH to represent this logical statement. Using the technique of forcing we can construct models of ZFC + CH and ZFC + ¬ CH, by choosing the appropriate forcing conditions.

We first construct a model of ZFC in which the Continuum Hypothesis fails.

Theorem 3.5.1. Let M be a countable transitive model of ZFC. Then there exists a countable transitive model $M' \supseteq M$ which is a sideways extension of M and satisfies $\mathsf{ZFC} + \neg\,\text{CH}$.

Proof. In M, let A be a set of cardinality κ, where $\kappa > \aleph_1$. Let P be the set of finite partial functions p from $A \times \omega$ to $\{0, 1\}$. We order P by putting $p \leq q$ if and only if $p \supseteq q$, i.e., p extends q. Let G be a generic filter on P. Clearly $g = \bigcup G$ is a function.

We claim that g is a total function from $A \times \omega$ to $\{0, 1\}$. To see this, consider the sets $D_{\alpha,n} = \{p \in P \mid (\alpha, n) \in \text{dom}(p)\}$. Each $D_{\alpha,n}$ is dense in P, and so G must meet each of them and so $(\alpha, n) \in \text{dom}(g)$ for all $(\alpha, n) \in A \times \omega$. Thus we have $g : A \times \omega \to \{0, 1\}$.

Next, for each $\alpha \in A$ define $g_\alpha(n) = g((\alpha, n))$. We have $g_\alpha : \omega \to \{0, 1\}$, i.e., $g_\alpha \in 2^\omega$, and $g_\alpha \in M[G]$. We claim that $\alpha \neq \beta \Rightarrow g_\alpha \neq g_\beta$. To see this, consider

$$D'_{\alpha,\beta} = \{p \in P \mid \exists n\, ((\alpha, n), (\beta, n) \in \text{dom}(p), p((\alpha, n)) \neq p((\beta, n)))\}.$$

Each $D'_{\alpha,\beta}$ belongs to M and is dense in P. Thus G meets $D'_{\alpha,\beta}$, and this gives our claim.

Since $g_\alpha \in 2^\omega \cap M[G]$ for all $\alpha \in A$, we see that $M[G]$ satisfies $2^{\aleph_0} = |2^\omega| \geq |A|$. It remains to show that, in $M[G]$, the cardinality of A is still greater than $\aleph_1$. In fact, we shall show that the cardinals of $M[G]$ are the same as the cardinals of M. This follows from the results in Section 3.6 below. $\square$

3.6 Preservation of cardinals and the c.c.c.

To finish the proof of Theorem 3.5.1, it suffices to prove that M and $M[G]$ have the same cardinals. This result depends on properties of the specific forcing extension used there.

Definition 3.6.1. A partial ordering $P \in M$ is said to be *cardinal preserving* if, for every M-generic filter $G \subseteq P$, the cardinals of $M[G]$ are the same as the cardinals of M.

In general, if $M[G]$ is an arbitrary forcing extension of M, then uncountable cardinals need not be preserved. This is because $M[G]$, being a sideways extension of the ground model M, may contain bijections whereby sets of differing cardinalities in M are placed into one-to-one correspondence in $M[G]$. This phenomenon is known as *cardinal collapsing*. For examples of how this can happen, see Theorem 3.7.6 and Example 3.8.3 below.

Now consider the following family of partial orderings.

Notation 3.6.2. If X and Y are sets, let $F(X,Y)$ be the set of finite partial functions from X into Y, partially ordered by putting $p \leq q$ if and only if $p \supseteq q$.

In particular, the partial ordering used in the proof of Theorem 3.5.1 is of the form $F(X, \{0,1\})$ where X is an uncountable set. (Namely, $X = A \times \omega$ where A is of cardinality $> \aleph_1$ in M.) We shall show that partial orderings of this form preserve cardinals. In more detail, we shall show that $F(X, \{0,1\})$ has a certain property called the c.c.c., and all c.c.c. partial orderings preserve cardinals.

Definition 3.6.3. Let P be a partial ordering. An *antichain* of P is a set $W \subseteq P$ such that, for all $p, q \in W$, if $p \neq q$ then $p \perp q$, i.e., p is incompatible with q. A partial ordering P is said to have the *countable chain condition*, abbreviated *c.c.c.*, if every antichain of P is countable.

Lemma 3.6.4. If P has the countable chain condition, then P preserves cardinals.

Proof. Suppose P does not preserve cardinals. Then there are $X, Y \in M$ such that $M \vDash |X| < |Y|$, but $M[G] \vDash |X| = |Y|$. Let $f : X \to Y$ be a bijection of X onto Y in $M[G]$. We have $f = (\dot{f})_G$ for some $\dot{f} \in M$. Because forcing equals truth, there is $p \in G$ such that p forces $\dot{f} : \check{X} \to \check{Y}$ to be a bijection. Fix such a p.

For $i \in X, j \in Y$, say that j is a *possible value of* $f(i)$ if there exists $q \leq p$ such that $q \Vdash \dot{f}(\check{i}) = \check{j}$. Say that j is a *possible value of* f if j is a possible value of $f(i)$ for some $i \in X$. Let Z_i be the set of possible values of $f(i)$, and let Z be the set of possible values of f. These sets belong to M, by definability of forcing. Now suppose $q_1, q_2 \leq p$ are such that $q_1 \Vdash \dot{f}(\check{i}) = \check{j}_1$ and $q_2 \Vdash \dot{f}(\check{i}) = \check{j}_2$ for some i, j_1, j_2 with $\check{j}_1 \neq \check{j}_2$. Then clearly q_1 is incompatible with q_2. Thus, since P has c.c.c., the set Z_i of possible values of $f(i)$ is countable in M. Hence $Z = \bigcup_{i \in I} Z_i$, the set of possible values of f, is of cardinality $\leq |X| \cdot \aleph_0 = |X|$ in M. Hence $Z \subsetneqq Y$, yet clearly $p \Vdash \operatorname{rng}(\dot{f}) \subseteq \check{Z}$. This contradiction completes the proof. $\square$

For example, we have:

Corollary 3.6.5. The Cohen poset $2^{<\omega}$ preserves cardinals. In other words, if $G \subseteq 2^{<\omega}$ is Cohen generic over M, then $M[G]$ has the same cardinals as M.

Proof. Being countable, the Cohen poset $2^{<\omega}$ has the c.c.c. Therefore it preserves cardinals. $\square$

More generally, we have the following result.

Definition 3.6.6. For any cardinal κ, a partial ordering $\mathcal{P}$ has the *κ-chain condition*, abbreviated *κ-c.c.*, if every antichain in $\mathcal{P}$ is of cardinality $< \kappa$. Under this definition, the countable chain condition is the $\aleph_1$-chain condition.

Lemma 3.6.7. If a partial ordering $P \in M$ has the κ-c.c., then forcing over M with P preserves all cardinals $\geq \kappa$.

Proof. Similar to the proof of Lemma 3.6.4. $\square$

We now return to the proof of Theorem 3.5.1.

Lemma 3.6.8. Let X be an uncountable set. Then $F(X, \{0,1\})$ has the c.c.c.

Proof. We assume some familiarity with basic measure theory. Consider the "fair coin" measure space $\{0,1\}^X$ with measure μ given by

$$\mu(\{f \in \{0,1\}^X \mid f(a) = i\}) = 1/2$$

for all $a \in X$ and $i \in \{0,1\}$. Given $p \in F(X, \{0,1\})$, put

$$U_p = \{f \in \{0,1\}^X \mid f \supset p\}.$$

Then $\mu(U_p) = 2^{-|\mathrm{dom}(p)|} > 0$.

Let W be an antichain in $F(X, \{0,1\})$. The elements of W are pairwise incompatible, so for all $p, q \in W$ with $p \neq q$ we have $U_p \cap U_q = \emptyset$. Hence

$$\textstyle\sum_{p \in W} \mu(U_p) = \mu\left(\bigcup_{p \in W} U_p\right) \leq \mu(U_\emptyset) = 1.$$

A basic fact about unordered summation is that a convergent unordered sum can have only countably many non-zero summands. Because $\mu(U_p)$ is non-zero for all $p \in W$, we see that W must be countable. Thus $F(X, \{0,1\})$ has c.c.c. $\square$

Theorem 3.6.9. The poset $F(X, \{0, 1\})$ of finite partial functions from X into $\{0, 1\}$ partially ordered by inclusion preserves all cardinals.

Proof. This follows by combining Lemmas 3.6.4 and 3.6.8. $\square$

Note also that this completes the proof of Theorem 3.5.1, giving a model of $\mathsf{ZFC} + \neg\,\mathrm{CH}$.

Remark 3.6.10. The proof of Lemma 3.6.8 given above may be criticized for its dependence on measure theory. There is a more elementary proof which we briefly sketch here.

The proof uses a combinatorial result known as the Δ-lemma. We define a Δ-*system* to be a set S of sets such that, for some fixed set D, $A \cap B = D$ for all $A, B \in S$, $A \neq B$. The Δ-lemma asserts that any uncountable collection of finite sets contains an uncountable Δ-system. The proof of the Δ-lemma is not difficult.

To prove Lemma 3.6.8, let W be an uncountable subset of $F(X, \{0, 1\})$. Applying the Δ-lemma to $\{\mathrm{dom}(p) \mid p \in W\}$, we obtain an uncountable set $Z \subseteq W$ and a fixed finite set D included in X such that $\mathrm{dom}(p) \cap \mathrm{dom}(q) = D$ for all $p, q \in Z$, $p \neq q$. Since $\{p{\restriction}D \mid p \in Z\}$ is finite, there exists an uncountable set $Z' \subseteq Z$ such that $p{\restriction}D = q{\restriction}D$ for all $p, q \in Z'$. It follows that, for all $p, q \in Z'$, p and q are compatible. Thus W is not an antichain. We conclude that all antichains in $F(X, \{0, 1\})$ are countable.

3.7 Forcing the Continuum Hypothesis

Recall that CH is the statement $2^{\aleph_0} = \aleph_1$. We have seen that, if M is a countable transitive model of ZFC, there is a forcing extension of M in which CH fails. In this section we shall see that there is a different forcing extension of M in which CH holds.

Let Ω denote the set of countable ordinals. A basic fact about Ω is that $|\Omega| = \aleph_1$ and every proper initial segment of Ω is countable.

Definition 3.7.1. Let P_Ω be the set of one-to-one functions from a proper initial segment of Ω into 2^ω. We partially order P_Ω by putting $p \leq q$ if and only if $p \supseteq q$.

Definition 3.7.2. A partial ordering P is said to be *countably closed* if every countable descending sequence of elements of P has a lower bound in P.

Example 3.7.3. The Cohen forcing poset 2^ω is not countably closed.

Lemma 3.7.4. P_Ω is countably closed.

Proof. If $p_0 \geq p_1 \geq \cdots \geq p_n \geq p_{n+1} \geq \cdots$ in P_Ω, then clearly $p = \bigcup_n p_n \in P_\Omega$, because the union of countably many proper initial segments of Ω is a proper initial segment of Ω. Thus p is a lower bound for the sequence $\langle p_n \mid n \in \omega \rangle$. $\square$

Lemma 3.7.5. Suppose $P \in M$ and $M \models$ "P is countably closed". Let G be an M-generic filter on P. Then $2^\omega \cap M = 2^\omega \cap M[G]$.

Proof. Clearly $2^\omega \cap M \subseteq 2^\omega \cap M[G]$. We need to prove the reverse inclusion. Given $f \in 2^\omega \cap M[G]$, let $\dot{f} \in M$ be such that $f = (\dot{f})_G$, and let $p \in G$ be such that $p \Vdash \dot{f} \in 2^\omega$. Put

$$D = \{q \leq p \mid \forall n \in \omega\,(q \Vdash \dot{f}(\check{n}) = \check{0} \vee q \Vdash \dot{f}(\check{n}) = \check{1})\}.$$

We claim that D is dense below p. To see this, given $q \leq p$, construct within M a sequence $\langle q_n \mid n \in \omega \rangle$ of elements of P with $q_0 = q$ and, for all n, $q_{n+1} =$ some $q \leq q_n$ such that either $q \Vdash \dot{f}(\check{n}) = \check{0}$ or $q \Vdash \dot{f}(\check{n}) = \check{1}$. Finally, let r be a lower bound for q_n, $n \in \omega$. Clearly $r \in D$. Thus D is dense below p.

Because D is dense below p and $p \in G$, let $q \in G$ be such that $q \in D$. Then clearly $f(n) = m$ if and only if $q \Vdash \dot{f}(\check{n}) = \check{m}$. By definability of forcing, it follows that $f \in M$. This completes the proof. □

Theorem 3.7.6. Let M be a countable transitive model of ZFC, and let G be a M-generic filter on P_Ω in M. Then $M[G] \models \mathsf{ZFC} + \mathrm{CH}$.

Proof. We know from earlier results that $M[G] \models \mathsf{ZFC}$. Let $g = \bigcup G$ be the unique function extending every condition in G. A straightforward dense set argument shows that g maps $\aleph_1^M$ one-to-one onto $(2^\omega)^M$. On the other hand, by Lemma 3.7.5, $(2^\omega)^M = (2^\omega)^{M[G]}$. It follows also that $\aleph_1^M$ is uncountable in $M[G]$, hence $\aleph_1^M = \aleph_1^{M[G]}$. Thus $M[G]$ contains a function from $\aleph_1^{M[G]}$ one-to-one onto $(2^\omega)^{M[G]}$. We conclude that $M[G] \models \mathrm{CH}$. □

Remark 3.7.7. We can generalize Lemma 3.7.5 as follows. Let κ be an infinite cardinal. A poset P is said to be *κ-closed* if every linearly ordered subset of P of cardinality $< \kappa$ has a lower bound in P. (Note that countably closed is equivalent to $\aleph_1$-closed.) We can show that κ-closed forcing over M creates no new functions $f : \lambda \to M$, $\lambda < \kappa$, hence preserves all cardinals $\leq \kappa$.

3.8 Additional models obtained by forcing

A great many different models of ZFC can be obtained by forcing. We give a few more examples. Let M be a countable transitive model of ZFC.

Example 3.8.1 (Sacks forcing). Let P be the set of perfect subtrees of $2^{<\omega}$ belonging to M, ordered by inclusion. Clearly P is a partial ordering which belongs to M. If G is an M-generic filter, we have $M[G] = M[g]$ where $g \in 2^\omega$. Namely, g is the unique member of $\bigcap_{T \in G}[T]$. We have $g \notin M$. It can be shown that g is *minimal*, in the sense that for all $f \in 2^\omega \cap M[g]$ either $f \in M$ or $g \in M[f]$. Compare this with the analogous construction of a minimal Turing degree in Theorem 2.8.10.

Example 3.8.2 (product forcing). Let P_1, P_2 be partial orderings in M. Then the product ordering $P_1 \times P_2$ is a partial ordering in M. It can be shown that G is an M-generic filter on $P_1 \times P_2$ if and only if $G = G_1 \times G_2$ where G_1 is an M-generic filter on P_1 and G_2 is an $M[G_1]$-generic filter on P_2. In this case we have $M[G] = M[G_1][G_2]$.

Example 3.8.3 (cardinal collapsing). Let κ be an uncountable cardinal of M. Let $P = F(\omega, \kappa) = \{p \mid p \text{ is a finite partial function from } \omega \text{ to } \kappa\}$, ordered by $p \leq q \iff p \supseteq q$. Then P is a partial ordering in M. If G is an M-generic filter on P, then $g = \bigcup G$ is a total function from ω onto κ. Thus κ is countable in $M[G]$. We describe this by saying that P collapses κ to $\aleph_0$. On the other hand, we have in M that $|P| = \kappa$, hence P has the κ^+-chain condition, so P preserves all cardinals $\geq \kappa^+$. It follows that $(\kappa^+)^M = \aleph_1^{M[G]}$, $(\kappa^{++})^M = \aleph_2^{M[G]}$, etc.

Example 3.8.4 (the Solovay model). Another important model of ZFC obtained by forcing is the so-called *Solovay model*. See Remark 6.4.10 below.

Example 3.8.5 (models where AC fails). Forcing may also be used to obtain models of ZF where the Axiom of Choice fails. We describe two such models.

Let DC be the *Axiom of Dependent Choice*: if $R \subseteq A \times A$ and for all $a \in A$ there exists $b \in A$ such that aRb, then for all $a \in A$ there exists an ω-sequence $\langle a_n \rangle_{n \in \omega}$ such that $a_0 = a$ and $a_n R a_{n+1}$ for all n. Let BPI be the *Boolean Prime Ideal Theorem*: every Boolean algebra carries an ultrafilter. Both DC and BPI are well known consequences or special cases of the Axiom of Choice. DC is important in analysis, while BPI is important in algebra and general topology.

Let G be an M-generic filter on P where $P = F(\omega \times \omega, \{0, 1\})$. This is essentially just Cohen forcing. Put $g = \bigcup G : \omega \times \omega \to \{0, 1\}$. For each $n \in \omega$ define $g_n : \omega \to \{0, 1\}$ by $g_n(m) = g((m, n))$. Thus $g_n \in 2^\omega$, and we have

$$M[G] = M[g] = M[\langle g_n \mid n \in \omega \rangle].$$

We consider the following submodels of $M[G]$.

1. $M_1 = M[g_n \mid n \in \omega] =$ the model of ZF generated by $M \cup \{g_n \mid n \in \omega\}$.

2. $M_2 = M[\{g_n \mid n \in \omega\}] =$ the model of ZF generated by $M \cup \{\{g_n \mid n \in \omega\}\}$.

We have $M_1 \subset M_2 \subset M[G]$. It can be shown that $M_1 \models \mathsf{ZF} + \mathrm{DC} + \neg\,\mathrm{BPI}$, and $M_2 \models \mathsf{ZF} + \mathrm{BPI} + \neg\,\mathrm{DC}$. For details see Felgner [3] and Jech [6].

Chapter 4

Absoluteness and constructibility

4.1 Absoluteness

Definition 4.1.1. Let M be a transitive model of ZFC. A *sideways extension* of M is a transitive model M' of ZFC such that $M' \supseteq M$ and $\text{rank}(M') = \text{rank}(M)$.

Example 4.1.2. Let $M' = M[G]$, where G is an M-generic filter on a poset $P \in M$. We have seen in Section 3.4 that $M[G]$ is a sideways extension of M.

Definition 4.1.3 (absoluteness). A formula $\varphi(x_1, \ldots, x_k)$ in the language of set theory is said to be *absolute* if, whenever M is a transitive model of ZFC and M' is a sideways extension of M and $a_1, \ldots, a_k \in M$, we have $M \models \varphi(a_1, \ldots, a_k)$ if and only if $M' \models \varphi(a_1, \ldots, a_k)$.

Examples 4.1.4. The formula "x is the empty set" is clearly absolute, because we are only considering transitive models.

The formula "x is countable" is not absolute, because any uncountable set $x \in M$ can be made countable in a generic extension of M by forcing with finite partial functions from ω to x.

Definition 4.1.5. A formula in the language of set theory $\{\in, =\}$ is said to be Δ_0 if it is built up from atomic formulas using propositional connectives and bounded quantifiers $\forall x \in y$ and $\exists x \in y$, defined as follows:

$$\begin{aligned} (\forall x \in y)\,\varphi &\equiv \forall x\,(x \in y \Rightarrow \varphi), \\ (\exists x \in y)\,\varphi &\equiv \exists x\,(x \in y \wedge \varphi). \end{aligned}$$

Example 4.1.6. There is a Δ_0 formula $\theta(x, y)$ defining $x = \bigcup y$, namely

$$\theta(x, y) \equiv ((\forall u \in x)\,(\exists z \in y)\,(u \in z)) \wedge ((\forall z \in y)\,(\forall u \in z)\,(u \in x)).$$

Similarly there are Δ_0 formulas equivalent to $x = y \times z$, etc. On the other hand, there is no Δ_0 formula equivalent to "$y =$ the powerset of x", etc.

Lemma 4.1.7. Any Δ_0 formula is absolute.

Proof. In fact, Δ_0 formulas are absolute to transitive sets, not only to models of ZFC containing all the ordinals. In other words, for any Δ_0 forumla $\varphi(x_1, \ldots, x_n)$ and transitive set A and $a_1, \ldots, a_n \in A$, we have that $\varphi(a_1, \ldots, a_n)$ holds if and only if $A \models \varphi(a_1, \ldots, a_n)$. The proof is straightforward by induction on the complexity of φ. $\square$

Example 4.1.8. Let ω denote the set of all finite ordinals. The formula "$x = \omega$" is absolute, because we can write it as the conjunction of the following Δ_0 formulas:

x is transitive:	$(\forall y \in x)\,(\forall z \in y)\,(z \in x)$.
x is linearly ordered by $\in$:	$(\forall y \in x)\,(\forall z \in x)\,(y = z \vee y \in z \vee z \in y)$.
x is a limit ordinal:	$\emptyset \in x \wedge (\forall y \in x)\,(y \cup \{y\} \in x)$.
x contains no limit ordinal:	$(\forall z \in x)\,(z = \emptyset \vee (\exists y \in z)\,(y \cup \{y\} = z))$.

Remark 4.1.9. From the absoluteness of ω, it follows that arithmetical sentences and predicates are absolute. In other words, if M' is a sideways extension of M, then for all arithmetical propositions θ we have $M \models \theta$ if and only if $M' \models \theta$. Thus the method of forcing cannot by itself suffice to show that an arithmetical statement (e.g., the Riemann hypothesis) is independent of ZFC set theory.

Remark 4.1.10. The property of being an uncountable cardinal is clearly not upward absolute, because of cardinal collapsing. However, it is downward absolute, as are many large cardinal properties. For example, if M' is a sideways extension of M and $M' \models \kappa$ is an inaccessible cardinal, then $M \models \kappa$ is an inaccessible cardinal. This is the content of the following theorem.

Theorem 4.1.11. The property of being an inaccessible cardinal is downward absolute.

Proof. Recall that a κ is inaccessible if $\kappa > \omega$, κ is regular, and $2^\lambda < \kappa$ for all $\lambda < \kappa$. Regularity means that for all $\lambda < \kappa$ and $f : \lambda \to \kappa$, $\operatorname{rng}(f)$ is bounded. By writing these definitions in the language of set theory, it can be seen that there is a Δ_0 formula $\varphi(\kappa, x)$ such that $\mathsf{ZFC} \vdash \kappa$ inaccessible $\iff \forall x\, \varphi(\kappa, x)$. Hence by Lemma 4.1.7 inaccessibility is downward absolute. $\square$

Remark 4.1.12. Similarly, some other large cardinal properties such as hyperinaccessibility, the Mahlo property, etc., are downward absolute. However, we shall see later that the properties of being a measurable cardinal or a Ramsey cardinal are not downward absolute.

4.2 Trees and well foundedness

We now go beyond first order arithmetical definability, by considering the lightface projective hierarchy.

Recall the arithmetical hierarchy, Section 2.3. Just as the arithmetical hierarchy was defined by counting quantifiers over ω, so the lightface projective hierarchy is now defined by counting quantifiers over ω^ω. For another introduction to the lightface projective hierarchy, see Rogers[1] [11, Chapter 17].

Definition 4.2.1 (the lightface projective hierarchy). The *language of second order arithmetic* consists of number variables $i, j, k, m, n, \ldots$ ranging over ω; function variables $f, g, h, \ldots$ ranging over ω^ω; first order functions and relations $+, \cdot, 0, 1, <, =$ (for the number variables), and a function application symbol $\mathrm{App}(f, n)$ which we abbreviate $f(n)$. Both number variables and function variables are quantified.

A formula of the language of second order arithmetic is *arithmetical* if it has no function quantifiers. Thus arithmetical predicates are those which are in the arithmetical hierarchy, i.e., Σ^0_n or Π^0_n for some $n \in \omega$.

The *lightface projective hierarchy* is a hierarchy of formulas in the language of second order arithmetic. A formula is Σ^1_1 if it is of the form $\exists f\, \varphi$ where φ is arithmetical. A formula is Π^1_n if it is the negation of a Σ^1_n formula. A formula is Σ^1_{n+1} if it is of the form $\exists f\, \varphi$, where φ is Π^1_n.

Example 4.2.2. For example, a Π^1_2 predicate is one of the form $P(f) \equiv \forall g\, \exists h\, A(f, g, h)$, where $A(f, g, h)$ is arithmetical. And, a Σ^1_2 predicate is one of the form $S(f) \equiv \exists g\, \forall h\, A(f, g, h)$, where $A(f, g, h)$ is arithmetical.

Remark 4.2.3. Our ultimate goal is to prove the Shoenfield Absoluteness Theorem: Σ^1_2 and Π^1_2 predicates are absolute. We begin by proving in this section that Σ^1_1 and Π^1_1 predicates are absolute.

Theorem 4.2.4 (Kleene Normal Form Theorem). Given a Σ^1_1 predicate $S(f)$, we can find a primitive recursive predicate R such that

$$S(f) \equiv \exists g\, \forall n\, R(f[n], g[n]).$$

Proof. Let $S(f)$ be Σ^1_1. Thus $S(f) \equiv \exists g\, A(f, g)$, where A is arithmetical. Putting $A(f, g)$ in prenex form, we obtain a quantifier-free formula Q such that

$$S(f) \equiv \exists g\, \forall m_1\, \exists n_1 \cdots \forall m_k\, \exists n_k\, Q(f, g, m_1, \ldots, m_k, n_1, \ldots, n_k).$$

We now replace the existential number quantifiers $\exists n_i$, $1 \le i \le k$, by Skolem functions h_i, $1 \le i \le k$. Thus $S(f)$ is equivalent to the formula

$$\exists g\, \exists h_1 \cdots \exists h_k\, \forall m_1 \cdots \forall m_k\, Q(f, g, m_1, \ldots, m_k, h_1(m_1), \ldots, h_k(m_1, \ldots, m_k))$$

Using a primitive recursive bijection $\omega^{k+1} \to \omega$, we can replace the sequence of functions $g, h_1, \ldots, h_k$ by a single function h. Thus we have a primitive recursive predicate P such that $S(f) \equiv \exists h\, \forall m\, P(f, h, m)$. Since primitive recursive predicates are computable, we can find an index e such that $S(f) \equiv \exists h\, \{e\}^{f \oplus h}(0)\uparrow$. Now by Proposition 2.6.3 we obtain a primitive recursive predicate R such that $S(f) \equiv \exists h\, \forall n\, R(f[n], h[n])$. $\square$

[1] Note however that Rogers [11] refers to the lightface projective hierarchy as "the analytical hierarchy." We dislike this terminology, because it conflicts with the use of the term "analytical" in classical descriptive set theory, where it means boldface Σ^1_1.

Definition 4.2.5 (well founded trees). A *tree* is a nonempty subset of $\mathrm{Seq} = \omega^{<\omega}$ which is closed under taking initial segments. A *path* through a tree T is a function $g : \omega \to \omega$ such that $g[n] \in T$ for all $n \in \omega$. A tree is said to be *well founded* if it has no path.

By the Kleene Normal Form Theorem, we have:

Proposition 4.2.6. Let $P(f) \equiv \forall g\, \exists n\, R(f[n], g[n])$ be a Π^1_1 predicate. Let

$$T_f = \{\tau \in \omega^{<\omega} \mid \neg\, \exists n \leq \mathrm{lh}(\tau)\, R(f[n], \tau[n])\}.$$

Then T_f is a tree, and $P(f)$ holds if and only if T_f is well founded.

Proof. Clearly T_f is a tree. By the construction of T_f, a path through T_f is just a function $g : \omega \to \omega$ such that $\neg\, \exists n\, R(f[n], g[n])$. Thus T_f has no path if and only if $\forall g\, \exists n\, R(f[n], g[n])$, i.e., $P(f)$. $\square$

We now show that well foundedness of trees is absolute. From this it will follow that Π^1_1 predicates are absolute.

Definition 4.2.7. Let T be a tree, and let Ord denote the ordinal numbers. A function $F : T \to \mathrm{Ord}$ is said to be *order preserving*, abbreviated *o.p.*, if $\forall \sigma, \tau \in T\, (\sigma \subset \tau \Rightarrow F(\sigma) > F(\tau))$.

Let Ω denote the set of countable ordinal numbers.

Lemma 4.2.8. Let $T \subseteq \mathrm{Seq} = \omega^{<\omega}$ be a tree. Then T is well founded if and only if there exists an order preserving map $F : T \to \mathrm{Ord}$, if and only if there exists an order preserving map $F : T \to \Omega$.

Proof. If T has a path g, then an order preserving map F from T to the ordinals would give a descending sequence of ordinals

$$F(g[0]) > F(g[1]) > \cdots > F(g[n]) > F(g[n+1]) > \cdots.$$

This is impossible. Conversely, if T is well founded, we define the map $R_T : \mathrm{Seq} \to \Omega$, where

$$R_T(\tau) = \begin{cases} 0 & \text{if } \tau \notin T, \\ \sup\{R_T(\tau^\frown\langle n\rangle) + 1 \mid n \in \omega\} & \text{otherwise.} \end{cases}$$

Then the restriction of R_T to T is an order preserving map from T to the ordinals. $\square$

Lemma 4.2.9. If $T \subseteq \omega^{<\omega}$ is a tree, then "T is well founded" is absolute.

Proof. Let M' be a sideways extension of M, and let $T \in M$ be a tree. We first show that "T is well founded" is downward absolute. Suppose that T is not well founded in M, so that $M \models \exists g \in \omega^\omega\, (g \text{ is a path through } T)$. Since "$g$ is a path through T" is arithmetical and thus absolute, $M' \models$ "g is a path through T".

Therefore"T is not well founded" is upward absolute, so "T is well founded" is downward absolute.

We next show that "T is well founded" is upward absolute. Suppose M satiesfies "T is well founded." Since Lemma 4.2.8 is provable in ZFC, it is true in M. Therefore M contains an order preserving map F from T to the ordinals. Since "x is an order preserving map from T to the ordinals" is definable by a Δ_0 formula, it is absolute. Hence M' satisfies that F is an order preserving map from T to the ordinals. By applying Lemma 4.2.8 inside M', we see that T is well founded in M'. □

Combining Proposition 4.2.6 and Lemma 4.2.9, we have:

Theorem 4.2.10. Σ^1_1 and Π^1_1 predicates are absolute.

Proof. Let $P(f)$ be a Π^1_1 predicate. Note that the construction of the tree T_f in Proposition 4.2.6 is uniformly recursive in f, hence arithmetical, hence absolute. We have $P(f) \equiv (T_f$ is well founded), and by Lemma 4.2.9 this is absolute. We have now shown that Π^1_1 predicates are absolute. It follows immediately that Σ^1_1 predicates are absolute. □

Remark 4.2.11. More generally, we can consider trees $T \subseteq A^{<\omega}$, where A is an arbitrary set. For such trees, the predicate "T is well founded" is again absolute, by essentially the same argument as for Lemma 4.2.9.

The previous remark will be used in the next section to prove Shoenfield's Absoluteness Theorem.

4.3 The Shoenfield Absoluteness Theorem

Theorem 4.3.1 (Shoenfield). Σ^1_2 and Π^1_2 predicates are absolute.

Proof. Let $S(f)$ be a Σ^1_2 predicate. Let I be an initial segment of the ordinals such that $I \supseteq \Omega$. We shall construct an uncountable tree $\mathcal{T}^I_f$ such that $S(f)$ holds if and only if $\mathcal{T}^I_f$ is not well founded.

Since $S(f)$ is Σ^1_2, we have $S(f) \equiv \exists g\, P(f,g)$ where $P(f,g)$ is Π^1_1. Apply the Kleene Normal Form Theorem to $P(f,g)$ to obtain a primitive recursive predicate R such that

$$S(f) \equiv \exists g\, \forall h\, \exists n\, R(f[n], g[n], h[n]).$$

Letting $T_{f,g} = \{\tau \in \omega^{<\omega} \mid \neg\, \exists n \leq \mathrm{lh}(\tau)\, R(f[n], g[n], \tau[n])\}$, we see as before that $S(f)$ holds if and only if there exists $g \in \omega^\omega$ such that $T_{f,g}$ is well founded. Therefore, by Lemma 4.2.8, $S(f)$ holds if and only if there exist $g \in \omega^\omega$ and $F : T_{f,g} \to I$ such that F is order preserving. Our tree $\mathcal{T}^I_f$ will be a tree of finite approximations to such a pair (g, F).

For each $\sigma \in \omega^{<\omega}$ define a finite tree $T^*_{f,\sigma} \subseteq \omega^{<\omega}$ by

$$T^*_{f,\sigma} = \{\tau \mid \mathrm{lh}(\tau) \leq \mathrm{lh}(\sigma), \#(\tau) \leq \#(\sigma), \neg\, \exists n \leq \mathrm{lh}(\tau)\, R(f[n], \sigma[n], \tau[n])\}.$$

Here $\#$ is a one-to-one Gödel numbering $\# : \omega^{<\omega} \to \omega$ which is assumed to have the property that $\tau_1 \subseteq \tau_2 \Rightarrow \#(\tau_1) \leq \#(\tau_2)$. It follows that $T^*_{f,\sigma}$ is a finite tree. Moreover $T_{f,g} = \bigcup_n T^*_{f,g[n]}$, and $T^*_{f,g[n]} \subseteq T^*_{f,g[n+1]}$ for all n. Thus $T_{f,g}$ is well founded if and only if there exists a sequence $\langle F_n \mid n \in \omega \rangle$ of finite maps such that for all n, $F_n \subseteq F_{n+1}$ and $F_n : T_{f,g[n]} \overset{o.p.}{\to} I$.

Notation 4.3.2. Recall that, for any set Z, $Z^{<\omega} = \bigcup_n Z^n$. Applying this to $Z = \omega \times A$ where A is any set, we have $(\omega \times A)^{<\omega} = \bigcup_n (\omega \times A)^n$. We identify this with $\bigcup_n \omega^n \times A^n$ in the obvious way. Thus each $s \in (\omega \times A)^{<\omega}$ is identified with an ordered pair $s = (\sigma, t) \in \omega^{<\omega} \times A^{<\omega}$.

In particular, let A be the set of finite, order preserving, partial functions from $\omega^{<\omega}$ to I. Our "supertree" $\mathcal{T}^I_f$ is defined by putting $s = (\sigma, t)$ into $\mathcal{T}^I_f$ if and only if, for all $n < \mathrm{lh}(t)$, $t(n) \subseteq t(n+1)$ and $t(n+1) \in A$ is an order preserving map from the finite tree $T^*_{f,\sigma[n+1]}$ into I. In view of the notation given in 4.3.2, we see that $\mathcal{T}^I_f$ is a subtree of $(\omega \times A)^{<\omega}$. Note also that the construction of $\mathcal{T}^I_f$ is absolute, given f and I.

Lemma 4.3.3. *$S(f)$ holds if and only if $\mathcal{T}^I_f$ is not well founded.*

Proof. $S(f)$ holds if and only if $\exists g\, P(f,g)$, if and only if $\exists g\, (T_{f,g}$ is well founded), if and only if $\exists g\, \exists F : T_{f,g} \overset{o.p.}{\to} I$, if and only if $\exists$ path through $\mathcal{T}^I_f$. $\square$

We now complete the proof of the Shoenfield Absoluteness Theorem. Let M and M' be transitive models of ZFC such that M' is a sideways extension of M. Let I be the set of countable ordinals of M'. Note that I is an initial segment of the ordinals of M and includes the countable ordinals of M. Applying Lemma 4.3.3 in both M and M', and using the absoluteness of well foundedness, we have

$$\begin{aligned} M \models S(f) &\iff M \models T^I_f \text{ is not well founded} \\ &\iff M' \models T^I_f \text{ is not well founded} \\ &\iff M' \models S(f). \end{aligned}$$

Thus $S(f)$ is absolute.

We have shown that Σ^1_2 predicates are absolute. It follows immediately that Π^1_2 predicates are absolute. This completes the proof. $\square$

Corollary 4.3.4. *Σ^1_3 predicates are upward absolute, and Π^1_3 predicates are downward absolute.*

Proof. Let $S(f)$ be the Σ^1_3 predicate $\exists g\, P(f,g)$, where $S(f,g)$ is Π^1_2. Let M' be a sideways extension of M. Suppose that M satisfies $S(f)$. Then there exists $g \in \omega^\omega \cap M$ such that M satisfies $P(f,g)$. By the Shoenfield Absoluteness Theorem, M' also satisfies $P(f,g)$. Therefore M' satisfies $S(f)$. This shows that Σ^1_3 predicates are upward absolute. It follows dually that Π^1_3 predicates are downward absolute. $\square$

4.4 Some examples

In this section we present some relatively easy examples illustrating the Shoenfield absoluteness phenomenon and its limitations. More complicated and revealing examples are in Corollary 4.6.2 and Remark 5.9.15 below.

Example 4.4.1. Consider the Σ^1_2 sentence θ which says "there exists a countable transitive model of ZFC." (For the precise construction of the sentence θ, see Remark 4.4.8 below.) Then, by the Shoenfield Absoluteness Theorem, θ is absolute. In other words, if M and M' are transitive models of ZFC and M' is a sideways extension of M, then $M \models \theta$ if and only if $M' \models \theta$.

Example 4.4.2. In the Shoenfield Absoluteness Theorem, it is required that M' be a sideways extension of M. This requirement cannot be eliminated. For example, let M be the smallest countable transitive model of ZFC, and let M' be a countable transitive model of ZFC such that $M \in M'$. Note that M' is not a sideways extension of M, because $\mathrm{rank}(M) < \mathrm{rank}(M')$. As above, let θ be the Σ^1_2 sentence asserting the existence of a countable transitive model of ZFC. Then M satisfies $\neg\,\theta$ but M' satisfies θ.

We consider stuctures for the predicate calculus with equality and one binary predicate symbol $\in$. We will always interpret equality naturally; therefore, a structure for this language consists of a nonempty set A (the universe) and a binary relation $E \subseteq A \times A$. We consider a class of structures for which there is a certain relationship between equality and the interpretation of the $\in$ relation; these are the extensional structures.

Definition 4.4.3. A structure (A, E) is *extensional* if (A, E) satisfies the Axiom of Extensionality:

$$\forall a, b \in A\,(a = b \iff \forall c \in A\,(cEa \iff cEb)).$$

Lemma 4.4.4 (Mostowski). If (A, E) is well founded and extensional, then there is a transitive set T such that $(A, E) \cong (T, \in\!|T)$. Furthermore, both T and the isomorphism $f : A \cong T$ are uniquely determined by (A, E). The transitive set T is called the *Mostowski collapse* of (A, E).

Proof. This is well known. $\square$

Corollary 4.4.5. Up to isomorphism, the countably infinite transitive sets are the same as the structures (ω, E), $E \subseteq \omega \times \omega$, which are well founded and extensional.

Remark 4.4.6. For structures of the form (ω, E) where $E \subseteq \omega \times \omega$, the satisfaction relation $\{(E, \#(\varphi)) \mid (\omega, E) \models \varphi\}$ is Δ^1_1. In fact, the satisfaction relation for (ω, E) is uniformly implicitly definable over the structure $(\omega, +, \cdot, =, E)$.

Remark 4.4.7. Well foundedness is a Π^1_1 property.

Remark 4.4.8. The sentence "there exists a countable transitive model of ZFC" is a Σ^1_2 sentence. To see this, observe that our sentence is equivalent to the Σ^1_2 sentence

$$\exists E \subseteq \omega \times \omega \, ((\omega, E) \text{ is well founded and } (\omega, E) \models \mathsf{ZFC}).$$

More generally we have:

Theorem 4.4.9. Let S be a recursively axiomatized theory in the language $\{\in, =\}$. The sentence "there exists a transitive model of S" is Σ^1_2, hence absolute.

Proof. By the Löwnheim-Skolem Theorem and the Collapsing Lemma, "there exists a transitive model of S" is equivalent to

$$\exists E \subseteq \omega \times \omega \, ((\omega, E) \text{ is well founded } \wedge (\omega, E) \models S).$$

The statement "(ω, E) is well founded" is Π^1_1, while "$(\omega, E) \models S$" is Δ^1_1. Therefore our sentence is Σ^1_2, hence absolute. $\square$

Example 4.4.10. The sentence "there exists a transitive model of $\mathsf{ZFC}+$ there exists an inaccessible cardinal" is Σ^1_2, hence absolute.

4.5 Constructible sets

In this section we review Gödel's work on the constructible sets.

Definition 4.5.1. Let T be a transitive set. We define $\mathrm{Def}(T)$, the collection of all definable subsets of T, as follows: $\mathrm{Def}(T) = \{X \subseteq T \mid X$ is definable over the structure $(T, \in\restriction T)$ allowing parameters from $T\}$.

Remark 4.5.2. Let T be a transitive set. Then $T \subseteq \mathrm{Def}(T)$, because each $a \in T$ is defined by the formula $x \in a$, using a as a parameter. Moreover $\mathrm{Def}(T)$ is transitive, and $T \in \mathrm{Def}(T) \setminus T$. Note that if T is finite then $\mathrm{Def}(T) = P(T)$ is finite, while T infinite implies $|\mathrm{Def}(T)| = |T|$.

Definition 4.5.3 (constructible sets). We define transitive sets L_α, $\alpha \in \mathrm{Ord}$, by transfinite recursion.

$$\begin{array}{lcll} L_0 & = & \emptyset, & \\ L_{\alpha+1} & = & \mathrm{Def}(L_\alpha), & \\ L_\delta & = & \bigcup_{\alpha<\delta} L_\alpha & \text{for } \delta \text{ a limit ordinal.} \end{array}$$

Remark 4.5.4. The following statements hold:

1. For all α, L_α is a transitive set.
2. $\alpha < \beta \Rightarrow L_\alpha \subsetneqq L_\beta$
3. For $n \in \omega$, L_n is finite. The set $L_\omega = \bigcup_{n\in\omega} L_n$ (also denoted HF) is the set of hereditarily finite sets.

4. For $\alpha \geq \omega$, $|L_\alpha| = |\alpha|$.
5. For all α, $\alpha = \mathrm{Ord} \cap L_\alpha$, thus $\alpha \in L_{\alpha+1}$. Therefore all ordinal numbers are constructible.

Definition 4.5.5. A set x is *constructible* if $x \in L_\alpha$ for some α. We define the class of constructible sets L by $L = \bigcup_{\alpha \in \mathrm{Ord}} L_\alpha$.

The class of constructible sets is an inner model of V, the class of all pure well founded sets. The following theorem states some properties of L.

Theorem 4.5.6 (Gödel). L is a transitive model of $\mathsf{ZFC}+\mathrm{GCH}$ which includes Ord. In fact, L is the smallest transitive model of ZFC which includes Ord.

In Theorem 4.5.8 below, we will show that $L \models \mathrm{CH}$. A key technical lemma needed for the proof is the following.

Lemma 4.5.7. There is a sentence φ of $\{\in, =\}$ such that for all transitive sets T, the structure $(T, \in|T) \models \varphi \iff T = L_\delta$ for some limit ordinal δ. We write the sentence φ as "$V{=}L$".

Proof. We omit the proof. Basically, "$V{=}L$" states that every set is constructible. It follows from Gödel's work that if $M \models \mathsf{ZFC} + V{=}L$ then $M \models$ GCH. $\square$

Theorem 4.5.8. $L \models \mathrm{CH}$, i.e., $(2^{\aleph_0})^L = (\aleph_1)^L$.

Proof. Given $X \in 2^\omega \cap L$, let λ be a limit ordinal such that $X \in L_\lambda$. By the Löwenheim-Skolem Theorem, there exists a countable set A such that $A \subseteq L_\lambda$, $X \in A$ and $(A, \in|A)$ is an elementary submodel of $(L_\lambda, \in|L_\lambda)$. Note that $(A, \in|A)$ is a countable, well founded, extensional, and satisfies $V{=}L$. Hence $(A, \in|A)$ is isomorphic to $(L_\delta, \in|L_\delta)$ for some countable limit ordinal δ. We can easily see that $X \in L_\delta$. Thus we have shown that, for any $X \in P(\omega) \cap L$, $X \in L_\delta$ for some $\delta < \omega_1$. Therefore $P(\omega) \subseteq \bigcup_{\delta<\omega_1} L_\delta = L_{\omega_1}$. Since $|L_{\omega_1}|^L = \aleph_1^L$, $|P(\omega)|^L \leq \aleph_1^L$.

Because L is a model of ZFC, Cantor's Theorem holds in L. Therefore $L \models |P(\omega)| > \aleph_0$. We conclude that $(2^{\aleph_0})^L = \aleph_1^L$. $\square$

4.6 Constructible reals

Theorem 4.6.1. The set of constructible members of the Baire space, $\omega^\omega \cap L$, is a Σ^1_2 set.

Proof. Let $f \in \omega^\omega$. By Gödel's proof of CH in L, the assertion "$f \in L$" is equivalent to "there exists a countable limit ordinal δ such that $f \in L_\delta$". And by Sections 4.4 and 4.5 this is equivalent to "there exists a countable transitive set T satisfying $V{=}L$ with $f \in T$". This in turn is equivalent to "there exists an $E \subseteq \omega \times \omega$ such that (ω, E) is well founded, $(\omega, E) \models V{=}L$, and there exists $k \in \omega$ such that $\forall m \, \forall n \, (f(m) = n \iff (\omega, E) \models k(\underline{m}) = \underline{n})$. Here $\underline{m}$ is the term representing the number m. This final assertion consists of an existential quantifier in front of a Π^1_1 formula, so the entire assertion is Σ^1_2. $\square$

Corollary 4.6.2. The sentence "every real is constructible" is Π^1_3 and not absolute.

Proof. Let φ be the sentence $\forall f \in \omega^\omega\,(f \in L)$. By the above theorem, this sentence is Π^1_3. Let M be a countable transitive model of $\mathsf{ZFC} + V{=}L$, and let G be a generic filter for some notion of forcing which adds new reals. Then $M \models \varphi$ but $M[G] \models \neg\,\varphi$. $\square$

Corollary 4.6.3. The Shoenfield Absoluteness Theorem, which states that Σ^1_2 and Π^1_2 sentences are absolute, is best possible.

For later use we note the following result.

Theorem 4.6.4. There is a Σ^1_2 well ordering of $\omega^\omega \cap L$, the set of constructible reals.

Proof. Note first that, by Gödel's work, the transitive sets L_δ for δ a limit ordinal are uniformly definably well ordered. This means that there is a formula $\psi(x,y)$ in the language $\{\in,=\}$ such that, for all limit ordinals δ,

$$\{(a,b) \in L_\delta \times L_\delta \mid L_\delta \models \psi(a,b)\}$$

is a well ordering of L_δ. (This fact is the basis of Gödel's proof that L satisfies the Axiom of Choice.)

For $a \in L$, the *constructible rank* of a is $r_L(a) =$ the least ordinal α such that $a \in L_{\alpha+1}$. Put $r'_L(a) = r_L(a) + \omega =$ the least limit ordinal δ such that $a \in L_\delta$. For $a, b \in L$ put $a \prec b$ if either $r'_L(a) < r'_L(b)$, or $r'_L(a) = r'_L(b) = \delta$ and $L_\delta \models \psi(a,b)$. Clearly $\prec$ is an L-definable well ordering of L. Furthermore, for $f, g \in \omega^\omega \cap L$, we have that $f \prec g$ if and only if there exists a well founded $E \subseteq \omega \times \omega$ such that $(\omega, E) \models V{=}L$ and there exist $i, j \in \omega$ such that $(\omega, E) \models i, j : \omega \to \omega$ and $\forall m\,\forall n\,(f(m) = n \iff (\omega, E) \models i(\underline{m}) = \underline{n})$ and $\forall m\,\forall n\,(g(m) = n \iff (\omega, E) \models j(\underline{m}) = \underline{n})$ and $(\omega, E) \models i \prec j$. Thus the restriction of $\prec$ to $\omega^\omega \cap L$ is Σ^1_2. This completes the proof. $\square$

Corollary 4.6.5. If $\forall f\,(f \in L)$ holds, then $\prec$ is a Δ^1_2 well ordering of ω^ω, and the order type of ω^ω under $\prec$ is ω_1.

4.7 Relative constructibility

Historically, forcing was developed with L as the ground model. Only later was the theory extended to work with arbitrary models of set theory. In this section, we note that models of set theory obtained by forcing may be viewed as being obtained by relative constructibility.

We can generalize the notion of constructibility either by relativizing to an extra predicate X, or by starting from an initial transitive set T, or both. The following definition encompasses both of these extensions.

Definition 4.7.1 (relative constructibility). Give a transitive set T and a class X, we define the class $L^T[X]$, read as "L relative to X over T", by transfinite recursion as follows:

$$\begin{aligned}
L_0^T[X] &= T, \\
L_{\alpha+1}^T[X] &= \mathrm{Def}(L_\alpha^T[X], X \cap L_\alpha^T[X], \in | L_\alpha^T[X]), \\
L_\delta^T[X] &= \textstyle\bigcup_{\alpha<\delta} L_\alpha^T[X], \text{ if } \delta \text{ is a limit ordinal.}
\end{aligned}$$

The notation $\mathrm{Def}(L_\alpha^T[X], X \cap L_\alpha^T[X], \in | L_\alpha^T[X])$ should be read as "the subsets of $L_\alpha^T[X]$ definable using parameters from $L_\alpha^T[X]$ and the extra predicate $X \cap L_\alpha^T[X]$." We define $L^T[X] = \bigcup\{L_\alpha^T[X] \mid \alpha \in \mathrm{Ord}\}$, the sets constructible relative to X starting with T.

Remark 4.7.2. $L^T[X]$ is a model of $\mathsf{ZF} + V{=}L^T[X]$. In fact, $L^T[X]$ is the smallest transitive model of $\mathsf{ZF}(X)$ containing all of the ordinals and $\{T\}$. Caution: $L^T[X]$ may or may not satisfy the Axiom of Choice. In fact, $L^T[X] \models \mathrm{AC}$ if and only if $L^T[X]$ contains a well ordering of T. In particular, with $T = \emptyset$, $L[X]$ satisfies the Axiom of Choice. However, $L[X]$ need not satisfy the GCH.

Remark 4.7.3. If $P \in L$ is a partial ordering and $G \subseteq P$ is L-generic, then the sideways extension $L[G]$ is given by relative constructibility, with G as the extra predicate.

Remark 4.7.4. More generally, if M is a transitive model of ZFC, P is a partial ordering in M, and G is an M-generic filter on P, then we have

$$M[G] = \bigcup\{L_\alpha^T[G] \mid T \in M, \alpha \in \mathrm{Ord} \cap M\}.$$

Contrast this with the definition of $M[G]$ already given in Section 3.2 above. However, the two definitions are equivalent.

Chapter 5

Measurable cardinals

In this chapter we introduce the study of large cardinals. We focus on measurable cardinals, this being one of the most typical large cardinal properties.

5.1 Filters

Definition 5.1.1 (filters). Let I be a nonempty set. A *filter* on I is a set $F \subseteq \mathcal{P}(I)$ such that:

1. $I \in F$ and $\emptyset \notin F$,
2. if $X \in F$ and $X \subseteq Y$, then $Y \in F$,
3. if $X, Y \in F$, then $X \cap Y \in F$.

Example 5.1.2. Let I be the closed unit interval $[0,1]$. Let

$$F = \{X \subseteq [0,1] \mid \mu(X) = 1\},$$

where μ denotes Lebesgue measure. Clearly $I \in F$ and $\emptyset \notin F$. Furthermore, it is obvious that if $\mu(X) = 1$ and $Y \supseteq X$ then $\mu(Y) = 1$. Finally, if $\mu(X) = \mu(Y) = 1$, then $\mu(X \cap Y) = 1$. Thus F is a filter.

Definition 5.1.3. A filter F is *countably additive* (a.k.a., σ-additive) if for all sequences $\langle X_n \rangle_{n \in \omega}$ with $X_n \in F$ for all $n < \omega$, we have $\bigcap_{n \in \omega} X_n \in F$.

Example 5.1.4. The filter in Example 5.1.2 is countably additive. This follows from countable additivity of Lebesgue measure.

Example 5.1.5. Let $I = \omega$. Clearly $F = \{X \subseteq \omega \mid \omega \setminus X \text{ is finite}\}$ is a filter on ω. It is called the Frechet filter. It is not countably additive.

Example 5.1.6. Let I be a topological space for which the Baire Category Theorem holds, e.g., any complete metric space, or any compact Hausdorff space. Then the comeager sets form a countably additive filter on I.

Definition 5.1.7 (κ-additivity). Let κ be an uncountable cardinal. A filter F is said to be *κ-additive* if the intersection of any $< \kappa$ sets in F is in F. I.e., for all families of sets $X_\alpha \in F$, $\alpha < \lambda$, with $\lambda < \kappa$, we have $\bigcap_{\alpha<\lambda} X_\alpha \in F$.

Remark 5.1.8. Every filter is $\aleph_0$-additive. Countable additivity is the same as $\aleph_1$-additivity.

Example 5.1.9. Let I be a set of cardinality $\geq \kappa$. The filter

$$F = \{X \subseteq I \mid |I \setminus X| < \kappa\}$$

is κ-additive. When $\kappa = \aleph_0$, this is just the Frechet filter on I.

5.2 The closed unbounded filter

In this section we present another interesting example of a filter, namely the *closed unbounded filter* (a.k.a., the *club filter*) on a regular uncountable cardinal.

Notation 5.2.1. Throughout this section, let κ be a regular uncountable cardinal. By definition this means that κ is an ordinal $> \omega$ and every unbounded subset of κ is of order type κ. Recall that, by von Neumann, every cardinal is an ordinal, and every ordinal is an initial segment of the ordinals.

Definition 5.2.2. A set $X \subseteq \kappa$ is *bounded* if $\sup X < \kappa$. A set $C \subseteq \kappa$ is *unbounded* if $\sup C = \kappa$, and *closed* if $\sup X \in C$ for all nonempty bounded sets $X \subseteq C$. A *club* is a closed unbounded set, i.e., a set $C \subseteq \kappa$ which is closed and unbounded.

Lemma 5.2.3. Let $F = \{X \subseteq \kappa \mid X \text{ includes a club}\}$. Then F is a filter on κ.

Proof. If suffices to show that the intersection of two clubs is a club. Suppose that $C_1, C_2 \subseteq \kappa$ are club. Clearly $C_1 \cap C_2$ is closed. We show that $C_1 \cap C_2$ is unbounded. Given $\alpha < \kappa$, to find $\gamma > \alpha$ such that $\gamma \in C_1 \cap C_2$. Pick $\alpha_0 \in C_1$ such that $\alpha_0 > \alpha$. Pick $\beta_0 \in C_2$ such that $\beta_0 > \alpha_0$. Pick $\alpha_1 \in C_1$ such that $\alpha_1 > \beta_0$. Pick $\beta_1 \in C_2$ such that $\beta_1 > \alpha_1$. Continuing for ω steps, we obtain two sequences $\alpha_n \in C_1$, $\beta_n \in C_2$, $n < \omega$, with

$$\alpha < \alpha_0 < \beta_0 < \cdots < \alpha_n < \beta_n < \cdots.$$

Finally put

$$\gamma = \sup_n \alpha_n = \sup_n \beta_n.$$

Since κ is regular and $> \omega$, we have $\gamma < \kappa$. Since C_1 and C_2 are closed, we have $\gamma \in C_1 \cap C_2$. Thus $C_1 \cap C_2$ is unbounded. ◻

Remark 5.2.4. The filter that we have just defined is called the *club filter* on κ. The argument used to show that $C_1 \cap C_2$ is unbounded is called a hand-over-hand argument. We can use a multiple hand-over-hand argument to show that the club filter is κ-additive, i.e., the intersection of fewer than κ clubs is a club.

More generally, we have the following.

Definition 5.2.5. The *diagonal intersection* of a κ-sequence of sets $X_\alpha \subseteq \kappa$, $\alpha < \kappa$, is defined by

$$\triangle_{\alpha<\kappa} X_\alpha = \{\alpha < \kappa \mid \alpha \in \bigcap_{\beta<\alpha} X_\beta\}.$$

Remark 5.2.6. A hand-over-hand argument shows that the diagonal intersection of clubs is a club. From this it follows that the club filter is closed under diagonal intersection.

Definition 5.2.7. A set $S \subseteq \kappa$ is said to be *stationary* if $S \cap C \neq \emptyset$ for all clubs $C \subseteq \kappa$. Clearly S is unbounded. In fact, $S \cap C$ is unbounded, for any club C.

Lemma 5.2.8 (Fodor). Let $S \subseteq \kappa$ be stationary, and let $f : S \to \kappa$ be such that $f(\alpha) < \alpha$ for all $\alpha \in S$. Then f is constant on a stationary set. I.e., there exists $\beta < \kappa$ such that $\{\alpha \in S \mid f(\alpha) = \beta\}$ is stationary.

Proof. Suppose not. Then for all $\beta < \kappa$ we can choose a club C_β such that $f(\alpha) \neq \beta$ for all $\alpha \in S \cap C_\beta$. Put $C = \triangle_{\beta<\kappa} C_\beta$, the diagonal intersection. Then C is a club, and for all $\alpha \in S \cap C$ we have that $f(\alpha) \neq \beta$ for all $\beta < \alpha$. This is a contradiction. □

Theorem 5.2.9. There exist κ pairwise disjoint stationary sets.

Proof. Let $S = \{\alpha < \kappa \mid \mathrm{cf}(\alpha) = \omega\}$, the set of limit ordinals $< \kappa$ of cofinality ω. (Or, instead of ω, we could use any regular uncountable cardinal $\lambda < \kappa$.) Clearly S is stationary. For each $\alpha \in S$ let $\alpha = \sup_n f_n(\alpha)$ where $f_n(\alpha) < \alpha$ for all $n < \omega$. We claim: there exists n such that $\{\alpha \in S \mid f_n(\alpha) \geq \gamma\}$ is stationary for all $\gamma < \kappa$. Otherwise, for each n let $\gamma_n < \kappa$ be such that $\{\alpha \in S \mid f_n(\alpha) \geq \gamma_n\}$ is not stationary, and let C_n be a club such that $f_n(\alpha) < \gamma_n$ for all $\alpha \in S \cap C_n$. Then $\gamma = \sup_n \gamma_n < \kappa$, and $C = \bigcap_n C_n$ is a club, and for all $\alpha \in S \cap C$ we have that $f_n(\alpha) \leq \gamma$ for all n, hence $\alpha \leq \gamma$. This is absurd, so our claim is proved. Fixing n as in the claim, we have by Fodor's Lemma 5.2.8 that $S_\beta = \{\alpha \in S \mid f_n(\alpha) = \beta\}$ is stationary, for unboundedly many $\beta < \kappa$. Since κ is regular, this gives us κ pairwise disjoint stationary sets. □

Remark 5.2.10. The above line of argument shows that any stationary subset of $\{\alpha < \kappa \mid \mathrm{cf}(\alpha) < \alpha\}$ is decomposable into κ pairwise disjoint stationary sets. Solovay has improved this by showing that *any* stationary set is decomposable into κ pairwise disjoint stationary sets. For a proof of this stronger result, see Jech [5, pp. 433–434].

5.3 Ultrafilters

Definition 5.3.1. An *ultrafilter* on a set I is a filter U such that for all $X \subseteq I$ either $X \in U$ or $I \setminus X \in U$. Alternatively, we can say that U is a maximal filter on I, in the sense of Zorn's Lemma.

Remark 5.3.2. The examples of filters presented in Section 5.1 are clearly not ultrafilters. Also, by Theorem 5.2.9, the club filter on a regular uncountable cardinal κ is not an ultrafilter.

Definition 5.3.3. For any fixed $i_0 \in I$, we have an ultrafilter

$$U = \{X \subseteq I \mid i_0 \in X\}.$$

Such ultrafilters are called *principal ultrafilters*.

Remark 5.3.4. Principal ultrafilters are considered uninteresting, because they are completely determined by a single element of I. Note that every ultrafilter on a finite set is principal. We have the following lemma and theorem giving the existence of nonprincipal ultrafilters.

Lemma 5.3.5. For each filter F on I, there is an ultrafilter U such that $F \subseteq U$.

Proof. Consider the set of filters on I which include F, ordered by inclusion. By Zorn's Lemma, this partial ordering has a maximal element, U. It is easy to check that U is an ultrafilter. $\square$

Theorem 5.3.6. For any infinite set I, there exists a nonprincipal ultrafilter on I.

Proof. Let F be the Frechet filter on I, i.e., $F = \{X \subseteq I \mid I \setminus X \text{ finite}\}$. Apply Lemma 5.3.5 to get an ultrafilter U extending F. Clearly U is nonprincipal. $\square$

Remark 5.3.7. It is difficult to find specific, natural examples of nonprincipal ultrafilters. In fact, it is consistent with ZFC that there is no definable nonprincipal ultrafilter on ω. To see this, note that the fair coin measure μ on 2^ω is invariant under the mapping $X \mapsto \omega \setminus X$, hence no nonprincipal ultrafilter on ω is μ-measurable, but in the Solovay model (see Remark 6.4.10) all definable subsets of 2^ω are μ-measurable.

5.4 Ultraproducts and ultrapowers

Definition 5.4.1 (ultraproducts). Let (A_i, E_i), $i \in I$, be an indexed family of relational structures. Thus for all $i \in I$ we have $A_i \neq \emptyset$ and $E_i \subseteq A_i \times A_i$. Consider the product

$$\textstyle\prod_{i \in I} A_i = \{\langle a_i \rangle_{i \in I} \mid \forall i \in I\,(a_i \in A_i)\}.$$

Given an ultrafilter U on I, define an equivalence relation $\approx$ on $\prod_{i \in I} A_i$ by

$$\langle a_i \rangle_{i \in I} \approx \langle b_i \rangle_{i \in I} \iff \{i \in I \mid a_i = b_i\} \in U.$$

Let A^* be the set of equivalence classes,

$$A^* = \textstyle\prod_{i \in I} A_i \,/ \approx.$$

Define a binary relation $E^* \subseteq A^* \times A^*$ by

$$[\langle a_i \rangle_{i\in I}]E^*[\langle b_i \rangle_{i\in I}] \iff \{i \in I \mid a_i E_i b_i\} \in U,$$

where $[\langle a_i \rangle_{i\in I}]$ is the equivalence class of $\langle a_i \rangle_{i\in I}$. The relational structure (A^*, E^*) is called an *ultraproduct.* We write

$$(A^*, E^*) = \textstyle\prod_{i\in I}(A_i, E_i)/\,U.$$

Remark 5.4.2. The idea behind ultraproducts is that (A^*, E^*) is in some sense the "average" of the structures (A_i, E_i), $i \in I$, where the average is taken with respect to the $0, 1$-valued measure U on I. This idea is confirmed by the following theorem.

Theorem 5.4.3 (Los). For all L-formulas $\varphi(x_1, \ldots, x_n)$, $L = \{\in, =\}$, and for all $a_1^*, \ldots, a_n^* \in A^*$, we have

$$(A^*, E^*) \models \varphi(a_1^*, \ldots, a_n^*) \iff \{i \in I \mid (A_i, E_i) \models \varphi(a_{1i}, \ldots, a_{ni})\} \in U,$$

where $a_1^* = [\langle a_{1i} \rangle_{i\in I}]$, $\ldots$, $a_n^* = [\langle a_{ni} \rangle_{i\in I}]$.

Proof. The proof is by induction on L-sentences with parameters from A^*. For atomic sentences the statement is true by definition of (A^*, E^*). Suppose $\varphi = \neg\,\psi$. Then $(A^*, E^*) \models \neg\,\psi \iff (A^*, E^*) \not\models \psi$. By the induction hypothesis, this holds if and only if $\{i \in I \mid (A_i, E_i) \models \psi\} \notin U$. Since U is an ultrafilter, this holds if and only if $\{i \in I \mid (A_i, E_i) \models \neg\,\psi\} \in U$.

Now suppose $\varphi = \psi_1 \wedge \psi_2$. Since $(A^*, E^*) \models \varphi$ if and only if $(A^*, E^*) \models \psi_1$ and $(A^*, E^*) \models \psi_2$, we have by the induction hypothesis that $(A^*, E^*) \models \varphi$ if and only if

$$\{i \in I \mid (A_i, E_i) \models \psi_1\} \in U \text{ and } \{i \in I \mid (A_i, E_i) \models \psi_2\} \in U.$$

Since ultrafilters are closed under intersection, this holds if and only if

$$\{i \in I \mid (A_i, E_i) \models \psi_1 \wedge \psi_2\} \in U,$$

i.e., $\{i \in I \mid (A_i, E_i) \models \varphi\} \in U$.

Finally, suppose $\varphi = \exists x\, \psi(x)$. If $(A^*, E^*) \models \exists x\, \psi(x)$, let $a^* \in A^*$ be such that $(A^*, E^*) \models \psi(a^*)$. Then by induction hypothesis

$$\{i \in I \mid (A_i, E_i) \models \psi(a_i)\} \in U,$$

where $a^* = [\langle a_i \rangle_{i\in I}]$. Hence $\{i \in I \mid (A_i, E_i) \models \exists x\, \psi(x)\} \in U$. Conversely, assume $\{i \in I \mid (A_i, E_i) \models \exists x\, \psi(x)\} \in U$. For each $i \in I$ use the Axiom of Choice to pick $a_i \in A_i$ such that $(A_i, E_i) \models \psi(a_i)$ if possible, otherwise let $a_i \in A_i$ be arbitrary. Then $\{i \in I \mid (A_i, E_i) \models \psi(a_i)\} \in U$. Hence by inductive hypothesis $(A^*, E^*) \models \psi(a^*)$, where $a^* = [\langle a_i \rangle_{i\in I}]$. Hence $(A^*, E^*) \models \exists x\, \psi(x)$. This completes the proof. $\square$

As an application of Los's Theorem, we now give an elegant proof of the Compactness Theorem.

Theorem 5.4.4. Let S be a set of sentences in the language with equality and one binary relation symbol. If every finite subset of S is satisfiable, then S is satisfiable.

Proof. Let I be the set of finite subsets of S. By hypothesis, for each $s \in I$ there is a structure (A_s, E_s) satisfying all the sentences in s. Let F be the filter on I generated by $\{X_\varphi \mid \varphi \in S\}$ where $X_\varphi = \{s \in I \mid \varphi \in s\}$. Let U be an ultrafilter extending F. Finally, let (A^*, E^*) be the ultraproduct $\prod_{s \in I}(A_s, E_s)/U$. For each $\varphi \in S$ we have $X_\varphi \in U$, hence $\{s \in I \mid (A_s, E_s) \models \varphi\} \in U$, hence by Los's Theorem $(A^*, E^*) \models \varphi$. Thus (A^*, E^*) satisfies S. $\square$

Remark 5.4.5. In our discussion of ultraproducts, we have dealt only with the language $\{\in, =\}$ with one binary predicate plus equality. However, it is routine to generalize to arbitrary languages for the predicate calculus. Thus we really do have a proof of the full Compactness Theorem.

We now consider the special case of ultraproducts where all of the structures (A_i, E_i) are the same.

Definition 5.4.6 (ultrapowers). An *ultrapower* is an ultraproduct

$$(A^*, E^*) = \prod_{i \in I}(A_i, E_i)/U$$

where each A_i is some fixed set A and each E_i is some fixed relation $E \subseteq A \times A$, for all $i \in I$. In this case we write

$$(A^*, E^*) = \prod(A, E)/U$$

and refer to (A^*, E^*) as the ultrapower of (A, E) by U. Note that $A^* = A^I/U$.

Remark 5.4.7. For any ultrapower (A^*, E^*) of (A, E), there is a canonical elementary embedding of (A, E) into (A^*, E^*) given by $a \mapsto [c_a]$ where $c_a = \langle a \rangle_{i \in I}$. In trivial cases, e.g., when A is finite or U is principal, our elementary embedding is onto A^*, so we get nothing new. In general, A^* contains new elements, so (A^*, E^*) is a proper elementary extension of (A, E).

Exercise 5.4.8. Show that the canonical embedding of (A, E) into (A^*, E^*) is onto if and only if U is $|A|^+$-additive.

5.5 An elementary embedding of V

Definition 5.5.1 (measurable cardinals). A *measurable cardinal* is an uncountable cardinal κ such that there exists a nonprincipal κ-additive ultrafilter on (any set of cardinality) κ.

Remark 5.5.2. Following Von Neumann, we identify cardinals with initial ordinals, and we identify ordinals with transitive sets well ordered by $\in$. Thus for any ordinal α we have $\alpha = \{\beta \mid \beta < \alpha\}$. In particular, κ is itself a set of cardinality κ. Since the existence of a nonprincipal κ-additive ultrafilter on one set of size κ implies the existence of a similar ultrafilter on any other set of size κ, we may define a measurable cardinal to be an uncountable cardinal κ such that there exists a κ-additive nonprincipal ultrafilter on κ itself.

Theorem 5.5.3. If κ is measurable, then κ is strongly inaccessible. That is, κ is regular, and $2^\lambda < \kappa$ for all $\lambda < \kappa$.

Proof. Let U be a κ-additive nonprincipal ultrafilter on κ. Since U is nonprincipal, $\{\beta\} \notin U$ for all $\beta < \kappa$. Hence by κ-additivity, for all $\alpha < \kappa$ we have $\alpha = \bigcup_{\beta<\alpha}\{\beta\} \notin \kappa$. Hence by κ-additivity again, for any $X \subseteq \kappa$ with $|X| < \kappa$ we have $\bigcup X = \bigcup_{\alpha\in X} \alpha \subsetneqq \kappa$, i.e., $\sup X < \kappa$. Thus κ is regular.

We next show that $\lambda < \kappa$ implies $2^\lambda < \kappa$. Fix $\lambda < \kappa$ and assume toward a contradiction that $f : \kappa \to P(\lambda)$ is one-to-one. For each $\beta < \lambda$ let X_β be either $\{\alpha < \kappa \mid \beta \in f(\alpha)\}$ or $\{\alpha < \kappa \mid \beta \notin f(\alpha)\}$, whichever is in U. This is a valid definition of X_β, because U is an ultrafilter. Since $\lambda < \kappa$ and U is κ-additive, we have $X = \bigcap_{\beta<\lambda} X_\beta \in U$. Since U is nonprincipal, there are two distinct elements $\alpha_1 \neq \alpha_2$ in X. By construction of X we have $\beta \in f(\alpha_1) \iff \beta \in f(\alpha_2)$ for all $\beta < \lambda$. Hence $f(\alpha_1) = f(\alpha_2)$, contradicting our assumption that f is one-to-one. We conclude that $2^\lambda < \kappa$. □

Corollary 5.5.4. The existence of a measurable cardinal is not provable in ZFC.

Proof. In light of Theorem 5.5.3 and the fact that ZFC proves that "'there exists an inaccessible cardinal" implies Con(ZFC), we see that ZFC proves that "there exists a measurable cardinal" implies Con(ZFC). By Gödel's theorem, ZFC does not prove Con(ZFC). Hence ZFC does not prove that a measurable cardinal exists. □

Next we shall use a measurable cardinal to construct an elementary embedding of the universe V into an inner model M. In the next section we shall use this technique to show that measurable cardinals are very large – larger than inaccessible cardinals, Mahlo cardinals, etc.

Definition 5.5.5. Let κ be a measurable cardinal. Let U be a κ-additive, nonprincipal ultrafilter on κ. Let V denote the universe of set theory. We define V^* to be the ultrapower V^κ/U.

Remark 5.5.6. Instead of the universe of set theory, we could use a countable transitive model of ZFC which satisifes "there exists a measurable cardinal."

Remark 5.5.7. Los's Theorem implies that V^* is a model of ZFC. We next show that V^* is isomorphic to a transitive model of ZFC.

Lemma 5.5.8. The ultrapower $(V^*, \in^*)$ is well founded.

Proof. Suppose that V^* is not well founded. Let $\langle a_n^*\rangle_{n\in\omega}$ be a descending sequence with respect to $\in^*$. For each $n \in \omega$ choose $\langle a_{n\alpha}\rangle_{\alpha<\kappa}$ such that a_n^* is the equivalence class $[\langle a_{n\alpha}\rangle_{\alpha<\kappa}]$. Let $Y_n = \{\alpha < \kappa \mid a_{n+1,\alpha} \in a_{n\alpha}\}$. By Los's

Theorem, $Y_n \in U$. Put $Y = \bigcap_n Y_n$. Then $Y \in U$, because U is κ-additive. Hence $Y \neq \emptyset$. Fix $\alpha \in Y$. Then $a_{n+1,\alpha} \in a_{n,\alpha}$ for each n, contradicting the well foundedness of V. We conclude that V^* is well founded. $\square$

Theorem 5.5.9. Let κ be a measurable cardinal. Then there is an inner model M of V and an elementary embedding $j : V \to M$.

Proof. Let U be a nonprincipal κ-additive ultrafilter on κ and let V^* be the ultrapower V^κ/U. Let $i : V \to V^*$ be the canonical elementary embedding. By Lemma 5.5.8, V^* is well founded, so let M be the Mostowski collapse of V^*. A general property of the collapse is that M is a definable class. Therefore M is an inner model of V. Define $j = \pi \circ i$, where $\pi : V^* \to M$ is the collapsing map. It is clear that j is an elementary embedding of V into M. $\square$

Lemma 5.5.10. Let $j : V \to M$ be the elementary embedding constructed in Theorem 5.5.9. Then $j(\alpha) = \alpha$ for every ordinal $\alpha < \kappa$, but $j(\kappa) > \kappa$.

Proof. To show that j is the identity on ordinals less than κ, it suffices to show that for all $[\langle \alpha_\gamma \rangle_{\gamma<\kappa}] \in V^*$, if $[\langle a_\gamma \rangle_{\gamma<\kappa}] < [c_\alpha] = i(\alpha)$ for some $\alpha < \kappa$, then $[\langle a_\gamma \rangle_{\gamma<\kappa}] = [c_\beta]$ for some $\beta < \alpha$. Note that $\{\gamma < \kappa \mid a_\gamma < \alpha\} \in U$. By κ-additivity, there exists $\beta < \alpha$ such that $\{\gamma < \kappa \mid a_\gamma = \beta\} \in U$. Thus in V^* we see that the ordinals $< [c_\alpha]$ are just $\{[c_\beta] \mid \beta < \alpha\}$, which has order type α. Hence, $j(\alpha) = \pi([c_\alpha]) = \alpha$.

Since j is order preserving, we have $j(\kappa) > j(\alpha) = \alpha$ for all $\alpha < \kappa$. Thus $j(\kappa) \geq \kappa$. Put $d = \langle \gamma \rangle_{\gamma<\kappa}$. For all $\alpha < \kappa$ we have $i(\kappa) = [c_\kappa] > [d] > [c_\alpha] = i(\alpha)$. Applying π, we obtain $j(\kappa) > \pi([d]) > \alpha$ for all $\alpha < \kappa$, hence $j(\kappa) > \kappa$. $\square$

We have proved the following result.

Theorem 5.5.11. If κ is a measurable cardinal, then there exist a transitive inner model M of V such that $\mathrm{Ord} \subseteq M \subseteq V$ and an elementary embedding $j : V \to M$ such that $j(\alpha) = \alpha$ for all $\alpha < \kappa$, and $j(\kappa) > \kappa$.

Remark 5.5.12. The converse of Theorem 5.5.11 also holds. See Theorem 5.6.5 below.

5.6 Largeness and normality

We now show that measurable cardinals are very large. There are many types of large cardinals. We define Mahlo cardinals and show that measurable cardinals are "larger" than inaccessible and Mahlo cardinals, in the sense that a measurable cardinal necessarily has many inaccessible and Mahlo cardinals below it.

Theorem 5.6.1. If κ is a measurable cardinal, then κ is greater than the least inaccessible cardinal.

Proof. By Theorem 5.5.3, κ is inaccessible in V. Let $j : V \to M$ be an elementary embedding as in Theorem 5.5.11. Thus κ is inaccessible in M, because $M \subseteq V$ and inaccessibility is downward absolute. Now $j(\kappa)$ is also inaccessible in M, because j is an elementary embedding. Because $j(\kappa) > \kappa$, there is an inaccessible cardinal in M which is strictly less than $j(\kappa)$. This pulls back to V, so V contains an inaccessible cardinal strictly less than κ. $\square$

Corollary 5.6.2. If κ is a measurable cardinal, then κ is the limit of inaccessible cardinals, hyper-inaccessible cardinals, etc.

Proof. Fix $\alpha < \kappa$ and repeat the previous argument. We have that $M \models j(\kappa) > \kappa > \alpha$, where κ is inaccessible. Thus $M \models \exists\lambda\,(j(\kappa) > \lambda > \alpha \wedge \lambda \text{ is inaccessible})$. Pulling back to V, we see that $V \models \exists\lambda\,(\kappa > \lambda > \alpha \wedge \lambda \text{ is inaccessible})$. $\square$

Definition 5.6.3. A *Mahlo cardinal* is an inaccessible cardinal κ such that every club in κ contains an inaccessible cardinal less than κ. I.e., the set of inaccessible cardinals $< \kappa$ is stationary in κ.

Theorem 5.6.4. If κ is a measurable cardinal, then κ is Mahlo, hyper-Mahlo, etc.

Proof. Let $C \subseteq \kappa$ be a club. Then $j(C)$ is club in $j(\kappa)$, since j is an elementary embedding. However, for any $\alpha < \kappa$ we have $\alpha \in C \iff \alpha = j(\alpha) \in j(C))$. Thus $j(C) \cap \kappa = C$, so $M \models j(C) \cap \kappa$ is unbounded in κ. Reasoning in M, $\kappa = \sup(j(C) \cap \kappa) \in j(C)$ and κ is inaccessible. Thus in M there is a $\lambda < j(\kappa)$ such that λ is inaccessible and $\lambda \in j(C)$ so $V \models \exists\lambda < \kappa\,(\lambda \in C)$. $\square$

We now prove the converse of Theorem 5.5.11.

Theorem 5.6.5. Let M be an inner model of V such that $j : V \to M$ is an elementary embedding. Let κ be the first ordinal moved by j, i.e., $j(\alpha) = \alpha$ for all $\alpha < \kappa$, and $j(\kappa) > \kappa$. Then κ is a measurable cardinal in V.

Proof. Define

$$U = \{X \subseteq \kappa \mid \kappa \in j(X)\}.$$

We claim that U is a nonprincipal κ-additive ultrafilter on κ. It is straightforward to verify that U is a filter. Moreover, U is nonprincipal: for any $\alpha < \kappa$, $j(\{\alpha\}) = \{\alpha\} \notin U$. It remains to verify that U is κ-additive. Fix $\lambda < \kappa$ and let X_β, $\beta < \lambda$, be subsets of κ. Since $j(\lambda) = \lambda$, we have $j(\bigcap_{\beta<\lambda} X_\beta) = \bigcap_{\beta<\lambda} j(X_\beta)$. Hence $\kappa \in j(\bigcap_{\beta<\lambda} X_\beta)$ if and only if $\kappa \in j(X_\beta)$ for all $\beta < \lambda$. Thus $\bigcap_{\beta<\lambda} X_\beta \in U$ if and only if $j(X_\beta) \in U$ for all $\beta < \lambda$. Thus U is κ-additive. $\square$

Theorem 5.6.6. If κ is measurable, then $\{\lambda < \kappa \mid \lambda \text{ is inaccessible, Mahlo, hyper-Mahlo, etc.}\}$ is stationary in κ.

Proof. Let U be the ultrafilter constructed in the proof of Theorem 5.6.5. The proof of Theorem 5.6.4 shows that $\{\lambda < \kappa \mid \lambda \text{ is inaccessible, Mahlo, hyper-Mahlo, etc.}\}$ belongs to U. The same proof also shows that every club set $C \subseteq \kappa$ belongs to U, and from this it follows that every member of U is stationary. $\square$

We end this section by noting that the ultrafilter constructed in the proof of Theorem 5.6.5 has an additional interesting property.

Definition 5.6.7 (normal ultrafilters). An ultrafilter U on κ is said to be *normal* if it is closed under diagonal intersection. That is, if $X_\gamma \in U$ for all $\gamma < \kappa$, then $\triangle_{\gamma<\kappa} X_\gamma \in U$, where

$$\triangle_{\gamma<\kappa} X_\gamma = \{\alpha < \kappa \mid \forall \gamma < \alpha \ (\alpha \in X_\gamma)\}.$$

Lemma 5.6.8. The ultrafilter U constructed in the proof of Theorem 5.6.5 is normal.

Proof. Given $X_\gamma \in U$ for all $\gamma < \kappa$, we want to show that $\triangle_\gamma X_\gamma \in U$. Straightforward computation shows that

$$j(\triangle_{\gamma<\kappa} X_\gamma) = \triangle_{\gamma<j(\kappa)} j(X_\gamma) = \{\alpha < j(\kappa) \mid \alpha \in \textstyle\bigcap_{\gamma<\alpha} j(X_\gamma)\}.$$

But $\kappa \in j(X_\gamma)$ for all $\gamma < \kappa$. Hence $\kappa \in j(\triangle_{\gamma<\kappa} X_\gamma)$, i.e., $\triangle_{\gamma<\kappa} X_\gamma \in U$. □

Combining previous results, we have:

Theorem 5.6.9. Let κ be a measurable cardinal. Then there exists a normal, κ-additive, nonprincipal ultrafilter on κ.

Proof. By Theorem 5.5.11 there is an elementary embedding $j : V \to M$, where M is an inner model of V and κ is the least ordinal moved by j. Apply Theorem 5.6.5 and Lemma 5.6.8 to obtain a normal ultrafilter on κ. □

Remark 5.6.10. Instead of using an elementary embedding, it is possible to give a combinatorial proof of Theorem 5.6.9 which directly constructs the normal ultrafilter.

5.7 Ramsey's Theorem

In this section we digress to prove a combinatorial theorem known as Ramsey's Theorem. Let X be any set. For $k \in \omega$, let $[X]^k$ denote the set of k-element subsets of X:

$$[X]^k = \{s \subseteq X \mid |s| = k\}.$$

We consider colorings of $[X]^k$ with finitely many colors $C_1, \ldots, C_l$.

Theorem 5.7.1 (Ramsey). Let X be an infinite set, and let $k, l \geq 1$. If $[X]^k = C_1 \cup \cdots \cup C_l$ then there exists an infinite set $Y \subseteq X$ such that $[Y]^k \subseteq C_i$ for some i.

Proof. Without loss of generality, assume $X = \omega$. The proof will proceed by induction on k, which we call the *exponent*. The base case, $k = 1$, amounts to what is called the Pigeonhole Principle: if an infinite set is broken into finitely many pieces, then one of the pieces must be infinite.

We now assume Ramsey's Theorem for exponent k and prove it for exponent $k+1$. Let $[\omega]^{k+1} = C_1 \cup \cdots \cup C_l$. For each $a \in \omega$ and $1 \leq i \leq l$ define

$$C_i^a = \{s \in [\,\omega \setminus \{0,\ldots,a\}\,]^k \mid \{a\} \cup s \in C_i\}.$$

We construct a strictly increasing sequence $\langle a_n \rangle$ of natural numbers. At the same time we construct a nested sequence of infinite sets $\langle X_n \rangle$. The construction proceeds by induction on n. To begin, let $X_0 = \omega$ and $a_0 = 0$. At stage $n+1$ we have that X_n is an infinite subset of ω. Let a_n be the least element of X_n. We have $[X_n \setminus \{a_n\}]^k \subseteq C_i^{a_n} \cup \cdots \cup C_l^{a_n}$, so by Ramsey's Theorem for exponent k let X_{n+1} be an infinite subset of $X_n \setminus \{a_n\}$ such that $[X_{n+1}]^k \subseteq C_i^{a_n}$ for some i. Note that $a_n < a_{n+1} =$ the least element of X_{n+1}. This finishes the construction.

Define $A = \{a_n \mid n \in \omega\}$. By construction, for any t and t' in $[A]^{k+1}$, if t and t' have the same least element, then t and t' both belong to C_i for some i. Define

$$A_i = \{a \in A \mid \forall t \in [A]^{k+1}\,(a = \min(t) \Rightarrow t \in C_i)\}.$$

By construction, $A = A_1 \cup \cdots \cup A_l$. By the Pigeonhole Principle, let i be such that A_i is infinite. Then $[A_i]^{k+1} \subseteq C_i$. This completes the proof. □

Example 5.7.2. We illustrate one consequence of Ramsey's theorem in the case $k = 2$. Let K_ω be the complete graph on ω vertices. Suppose that the edges of K_ω are colored with finitely many colors. Then there is an infinite subgraph G of K_ω such that G is a complete graph and the edges between the vertices of G are all the same color.

5.8 Indiscernibles and EM-sets

A classic application of Ramsey's Theorem is the construction of models with indiscernibles. Two elements in a structure are said to be *indiscernible* if they satisfy exactly the same formulas (without parameters) with one free variable. We generalize this to infinite sets of indiscernibles.

Definition 5.8.1 (indiscernibles). Let (A, E) be a relational structure for the language L with one binary predicate symbol and equality. Let I be a subset of A, and let $<$ be a linear ordering of I. We say that $(I, <)$ is a *set of indiscernibles* in (A, E) if for all L-formulas $\varphi(x_1, \ldots, x_k)$ with free variables $x_1, \ldots, x_k$, $k \geq 1$, and all sequences $a_1 < \cdots < a_k$ and $b_1 < \cdots < b_k$ of elements of I,

$$(A, E) \models \varphi(a_1, \ldots, a_k) \iff (A, E) \models \varphi(b_1, \ldots, b_k).$$

Theorem 5.8.2. Let (A, E) be a relational structure with A an infinite set, and let $(I, <)$ be any linearly ordered set. Then there is a relational structure (A', E') elementary equivalent to (A, E) such that (A', E') contains $(I, <)$ as a set of indiscernibles.

Proof. We work with the language $L' = L \cup I$ consisting of L plus constant symbols for the elements of I. We will show that a certain L'-theory T is consistent. T consists of:

1. all L-sentences true in (A, E),
2. the sentence $a \neq b$ for all distinct $a, b \in I$,
3. all sentences of the form $\varphi(a_1, \ldots, a_k) \iff \varphi(b_1, \ldots, b_k)$, where $\varphi(x_1, \ldots, x_k)$ is an L-formula with the free variables shown, and $a_1 < \cdots < a_k \in I$, $b_1 < \cdots < b_k \in I$.

Clearly any structure (A', E') satisfying T has $(I, <)$ as a set of indiscernibles. To show that T is satisfiable, we will use the Compactness Theorem and Ramsey's Theorem.

Let T_0 be a finite subset of T. We show that T_0 is satisfiable. Let $\varphi_1, \ldots, \varphi_n$ be the finitely many L-formulas φ as in part 3 of the definition of T which occur in T_0. By adding dummy variables as needed, we may assume that all of $\varphi_1, \ldots, \varphi_n$ have the same free variables, say $x_1, \ldots, x_k$ for some fixed k.

Fix a linear ordering $<$ of A. We partition $[A]^k$ into 2^n subsets. For each $s \subseteq \{1, \ldots, n\}$ define $C_s \subseteq [A]^k$ by

$$\{a_1 < \cdots < a_k\} \in C_s \iff s = \{i \mid (A, E) \models \varphi_i(a_1, \ldots, a_k)\}.$$

Then $[A]^k = \bigcup_s C_s$. By Ramsey's Theorem we obtain an infinite set $X \subseteq A$ such that $[X]^k \subseteq C_s$ for some s. We then use elements of X to interpret the finitely many constants from I which occur in T_0. Thus T_0 is satisfiable in (A, E). $\square$

Given an infinite set of indiscernibles, it is natural to make the following definition.

Definition 5.8.3 (EM-sets). Let $(I, <)$ be an infinite set of indiscernibles in a structure (A, E). The *EM-set* (Ehrenfeucht/Mostowski set) of $(I, <)$ in (A, E) is the set of L-formulas $\varphi(x_1, \ldots, x_n)$, $n < \omega$, such that $(A, E) \models \varphi(a_1, \ldots, a_n)$ for all $a_1 < \ldots < a_n \in I$.

Remark 5.8.4. Abstractly, a set of L-formulas is an EM-set if and only if

$$\{\varphi(c_{i_1}, \ldots, c_{i_n}) \mid i_1 < \ldots < i_n \in \omega, \varphi(x_1, \ldots, x_n) \in S, n \in \omega\}$$

is a maximal consistent set of sentences in the language $L' = L \cup \{c_i \mid i < \omega\}$.

Theorem 5.8.5 (stretching indiscernibles). Let S be an EM-set and let $(J, <)$ be an infinite linear ordering. Then there is an L-structure containing $(J, <)$ as a set of indiscernibles with S as its EM-set.

Proof. Put $S_J = \{\varphi(a_1, \ldots, a_n) \mid \varphi(x_1, \ldots, x_n) \in S, n < \omega, a_1 < \ldots < a_n \in J\}$. Thus S_J is a set of L'-sentences, where $L' = L \cup J$. Since S is an EM-set, S_J is finitely satisfiable. Hence S_J is satisfiable. By construction of S_J, any model of S_J contains a set of indiscernibles which is a copy of $(J, <)$. $\square$

We now consider a special model-theoretic situation where the stretching of indiscernibles is functorial.

Definition 5.8.6 (definable Skolem functions). A structure (A, E) is said to have *definable Skolem functions* if for each L-formula $\varphi(x_1, \ldots, x_n, y)$ there exists an L-formula $\widehat{\varphi}(x_1, \ldots, x_n, y)$ such that (A, E) satisfies

$$\forall x_1 \ldots \forall x_n \forall y \, [\, \widehat{\varphi}(x_1, \ldots, x_n, y) \Rightarrow \varphi(x_1, \ldots, x_n, y)\,]$$

and

$$\forall x_1 \ldots \forall x_n \, [\, (\exists y \, \varphi(x_1, \ldots, x_n, y)) \Rightarrow \exists !\, y \, \widehat{\varphi}(x_1, \ldots, x_n, y)\,].$$

Here $\exists !\, y$ is an abbreviation for "there exists a unique y".

Examples 5.8.7. Many common structures have definable Skolem functions.

1. $(\mathbb{N}, +, \cdot, <)$ has definable Skolem functions, because if there is a number satisfying a formula then we can pick the least one. Thus

$$\widehat{\varphi}(x_1, \ldots, x_n, y) \;\equiv\; \varphi(x_1, \ldots, x_n, y) \wedge \neg \exists z \, (z < y \wedge \varphi(x_1, \ldots, x_n, z)).$$

2. The real number system $(\mathbb{R}, +, \cdot)$ has definable Skolem functions. This is an easy consequence of quantifier elimination for $(\mathbb{R}, +, \cdot, 0, 1, <, =)$.

3. Any structure can be expanded to a structure for a larger language with definable Skolem functions, by adding extra functions, using the Axiom of Choice.

Theorem 5.8.8 (the definable hull). If (A, E) has definable Skolem functions, then for all $X \subseteq A$ there is a smallest elementary submodel of (A, E) containing X. This model, denoted $\mathrm{Hull}(X)$, consists of those elements $a \in A$ which are definable over (A, E) allowing parameters from X.

Proof. The proof is a straightforward application of the Tarski criterion for elementary submodels. $\square$

Definition 5.8.9. An EM-set S is said to have *definable Skolem functions* if it is the EM-set of an infinite set of indiscernibles $(I, <)$ in a structure (A, E) which has definable Skolem functions.

Proposition 5.8.10. Let S be an EM-set with definable Skolem functions. To any linear ordering $(J, <)$ we can associate a unique L-structure $\mathrm{Hull}_S(J) = \mathrm{Hull}(J)$ within (A, E) where (A, E) is any L-structure with $(J, <)$ as a set of indiscernibles with S as its EM-set. The construction of $\mathrm{Hull}_S(J)$ does not depend on the choice of (A, E).

Proof. The existence of $\mathrm{Hull}_S(J)$ is given by Theorems 5.8.5 and 5.8.8. Thus $\mathrm{Hull}_S(J)$ is a structure with $(J, <)$ as a set of indiscernibles and S as its EM-set. To prove uniqueness, assume that both (A, E) and (A', E') have $(J, <)$ as a set of indiscernibles with EM-set S. Because $S$is an EM-set, $(A, E, j)_{j \in J}$ is elementarily equivalent to $(A', E', j)_{j \in J}$. Hence there is a natural isomorphism f of $\mathrm{Hull}(J, (A, E))$ onto $\mathrm{Hull}(J, (A', E'))$. Namely, if $a \in \mathrm{Hull}(J, (A, E))$, let $f(a) =$ the unique $a' \in \mathrm{Hull}(J, (A', E'))$ such that $(A, E, a, j)_{j \in J}$ is elementarily equivalent to $(A', E', a', j)_{j \in J}$. $\square$

Remark 5.8.11. Note that Hull_S is functorial. I.e., if $(I, <)$ is a subordering of $(J, <)$, then $\mathrm{Hull}_S(I)$ is canonically an elementary submodel of $\mathrm{Hull}_S(J)$.

Definition 5.8.12 (definable well ordering). A structure (A, E) is said to be *definably well ordered* if there exists a binary relation $\prec$ on A such that

1. $\prec$ is a linear ordering of A.
2. $\prec$ is definable over (A, E) without parameters.
3. (A, E) satisfies "every definable set has a $\prec$-least element". That is, for each L-formula $\varphi(y)$ whose free variables include y, (A, E) satisfies the universal closure of
$$(\exists y\, \varphi(y)) \Rightarrow \exists y\, (\varphi(y) \wedge \neg \exists z\, (z \prec y \wedge \varphi(z))).$$

Thus $\prec$ is something like a well ordering of A with respect to sets in $\mathrm{Def}((A, E))$.

Remark 5.8.13. If (A, E) is definably well ordered, then (A, E) has definable Skolem functions. Namely, put
$$\widehat{\varphi}(x_1, \ldots, x_n, y) \;\equiv\; \varphi(x_1, \ldots, x_n, y) \wedge \neg \exists z\, (z \prec y \wedge \varphi(x_1, \ldots, x_n, z)).$$

5.9 Measurable cardinals and L

Recall that L, the class of constructible sets, is the smallest inner model of V. For several reasons, $V{=}L$ has been proposed as an axiom of set theory. Some advantages of this proposal are:

1. It settles many set theoretic questions, such as the GCH, Souslin's Hypothesis, etc.
2. It is a simplifying assumption, restricting our attention to constructible sets.
3. It is known to be consistent with ZFC. In fact, by the Shoenfield Absoluteness Theorem, the theory $\mathsf{ZFC} + V{=}L$ is conservative over ZFC for Π^1_3 sentences.

The main disadvantage of $V{=}L$ is that it restricts our notion of set. For example, $V{=}L$ implies that measurable cardinals do not exist, as we now prove.

Theorem 5.9.1 (Scott). If a measurable cardinal exists, then $V \neq L$.

Proof. Let κ be the smallest measurable cardinal. Let U be a κ-additive non-principal ultrafilter on κ. Let $i : V \to V^* = V^\kappa/U$ be the canonical elementary embedding. Let $\pi : V^* \cong M$ be the transitive collapse of V^*. Let $j : V \to M$ be given by $j = \pi \circ i$. Then M is an inner model, $j : V \to M$ an elementary embedding, and $j(\kappa) > \kappa$. Since $V \models \kappa$ is the smallest measurable cardinal, $M \models j(\kappa)$ is the smallest measurable cardinal. Thus $M \models \kappa$ is not a measurable cardinal. Therefore $U \notin M$. Hence $V \supsetneqq M$. Since $L \subseteq M$, we conclude that $V \supsetneqq L$. □

We now go on to show that the existence of a measurable cardinal implies that $P(\omega) \cap L$ is countable. Moreover, we shall show that every uncountable successor cardinal of L is collapsed in V, and this implies that V is not a forcing extension of L. Our tools for these proofs will be indiscernibles and EM-sets.

We begin with the following Ramsey-type theorem. Recall from Theorem 5.6.9 that every measurable cardinal carries a normal ultrafilter.

Theorem 5.9.2. Let κ be a measurable cardinal, and let U be a normal ultrafilter on κ. Then for all colorings $[\kappa]^n = C_1 \cup \cdots \cup C_l$ there exists $X \in U$ such that $[X]^n \subseteq C_i$ for some i.

Proof. The proof is similar to the proof of Ramsey's Theorem. We proceed by induction on n. The base case $n = 1$ is clear. For the induction step, we are given $[\kappa]^{n+1} = C_1 \cup \cdots \cup C_l$. For each $\alpha < \kappa$ put

$$C_i^\alpha = \{s \in [\kappa]^n \mid \alpha < \min(s) \text{ and } \{\alpha\} \cup s \in C_i\}.$$

By inductive hypothesis there exists $X_\alpha \in U$ such that $[X_\alpha]^n \subseteq C_i^\alpha$ for some $i = i_\alpha$, $1 \le i \le l$. Note that $\kappa = Y_1 \cup \cdots \cup Y_l$ where $Y_i = \{\alpha < \kappa \mid i_\alpha = i\}$. Let i be such that $Y_i \in U$. Put $X = Y_i \cap \triangle_{\alpha<\kappa} X_\alpha$. We claim that $[X]^{n+1} \subseteq C_i$. Given $t \in [X]^{n+1}$ we have $t = \{\alpha\} \cup s$, where $\alpha < \min(s)$ and $\alpha \in Y_i$, hence $s \in [X_\alpha]^n \subseteq C_i^\alpha$, hence $t \in C_i$. □

Corollary 5.9.3. There exists $X \subseteq \kappa$ such that $X \in U$ and X is a set of indiscernibles in $(L_\kappa, \in|L_\kappa)$ ordered by $<$ in κ.

Proof. For each $\{\in, =\}$-formula $\varphi(x_1, \ldots, x_n)$ we have $[\kappa]^n = C_\varphi \cup C_{\neg\varphi}$, where $C_\varphi = \{\{\alpha_1 < \cdots < \alpha_n\} \mid L_\kappa \models \varphi(\alpha_1, \ldots, \alpha_n)\}$. Therefore we can find $X_\varphi \in U$ such that $[X_\varphi]^n \subseteq C_\varphi$ or $[X_\varphi]^n \subseteq C_{\neg\varphi}$. Set $X = \bigcap_\varphi X_\varphi$. □

Definition 5.9.4 (definition of $0^\#$). We let $0^\#$ denote the EM-set of a set of indiscernibles $X \in U$ for L_κ.

Remark 5.9.5. Our definition of $0^\#$ appears to depend on the choice of a measurable cardinal κ and a normal ultrafilter U. However, it can be shown that $0^\#$ is independent of κ and U.

Remark 5.9.6. For any limit ordinal δ, the structure $(L_\delta, \in|L_\delta)$ has a definable well ordering, and hence also has definable Skolem functions. (The existence of a definable well ordering of L_δ is a basic property of the constructible sets, used in proving that L satisfies the Axiom of Choice.) It follows that $0^{\#}$ is an EM-set with definable Skolem functions. Let κ and X be as in the definition of $0^{\#}$. Since $\mathrm{Hull}(X)$ is an elementary submodel of L_κ, $\mathrm{Hull}(X)$ is well founded and satisfies $V{=}L$. Hence, by Lemmas 4.4.4 and 4.5.7, $\mathrm{Hull}(X)$ is isomorphic to L_κ.

Definition 5.9.7 (nice EM-sets). Let S be an EM-set with definable Skolem functions. We say that S is *nice* if, for all well orderings $(I,<)$, $\mathrm{Hull}_S((I,<))$ is well founded. Note that niceness for countable well orderings implies niceness for arbitrary well orderings. Thus niceness is a Π^1_2 property.

Lemma 5.9.8. $0^{\#}$ is a nice EM-set for $V{=}L$.

Proof. It follows from the definition that $0^{\#}$ is an EM-set for $V{=}L$. Suppose $0^{\#}$ is not nice. Let $(I,<)$ be a well ordering such that $\mathrm{Hull}_{0^{\#}}(I)$ is not well founded. Let $\{a_n\}_{n\in\omega}$ be a descending sequence in $\mathrm{Hull}_{0^{\#}}(I)$. Let $J \subseteq I$ be countable so that $\{a_n \mid n \in \omega\} \subseteq \mathrm{Hull}_{0^{\#}}(J)$. Thus $\mathrm{Hull}_{0^{\#}}(J)$ is not well founded. On the other hand, since J is a countable well ordering, it is isomorphic to a subordering of X, where X is as in the definition of $0^{\#}$. Hence $\mathrm{Hull}_{0^{\#}}(J)$ embeds into $\mathrm{Hull}_{0^{\#}}(X)$, which is well founded, a contradiction. $\square$

Theorem 5.9.9 (Rowbottom). The existence of a measurable cardinal implies that $P(\omega)\cap L$ is countable.

Proof. Look at $\mathrm{Hull}(X) \cong L_\kappa$ as in the definition of $0^{\#}$. By Gödel we have $P(\omega)\cap L \subseteq L_\kappa$. Hence for each $A \in P(\omega)\cap L$ we have

$$A = \{k \in \omega \mid L_\kappa \vDash \varphi(\underline{k}, a_1, \ldots, a_n)\}$$

for some formula φ and $a_1 < \cdots < a_n \in X$. Since X is a set of indiscernibles, the truth value of $\varphi(\underline{k}, a_1, \ldots, a_n)$ does not depend on the choice of $a_1 < \cdots < a_n \in X$. Hence there are only countably many possibilities for A. Thus $P(\omega)\cap L$ is countable. $\square$

We also have the following more general result.

Theorem 5.9.10 (Rowbottom). Assume there exists a measurable cardinal. Then for any infinite cardinal λ of L we have $|P(\lambda)\cap L| = |\lambda|$. Hence $(\lambda^+)^L$ is not a cardinal of V.

Proof. Let λ^+ be the next cardinal after λ in V. Using $0^{\#}$ as the EM-set, form $\mathrm{Hull}(\lambda^+)$. We know that $\mathrm{Hull}(\lambda^+)$ is well founded and satisfies $V{=}L$, hence is $\cong L_\delta$ for some limit ordinal $\delta \geq \lambda^+$. (Actually one can show that $\delta = \lambda^+$.) It follows that $L_\delta = \mathrm{Hull}(X)$ where $X \subseteq \delta$ is a set of indiscernibles of order type λ^+. Let Y be an initial segment of X of cardinality $|\lambda|$ such that $\lambda \subseteq \mathrm{Hull}(Y)$. For each $a < \lambda$ let $\psi_a(x)$ be a formula with parameters from Y such that a is unique $a \in L_\delta$ such that $L_\delta \vDash \psi_a(a)$. By Gödel, each $A \in P(\lambda)\cap L$ belongs to $L_{\lambda^+} \subseteq L_\delta = \mathrm{Hull}(X)$, so

$$A = \{a < \lambda \mid L_\delta \vDash \exists x\,(\psi_a(x) \wedge \varphi(x, b_1, \ldots, b_n))\}$$

for some formula $\varphi(x, b_1, \cdots, b_n)$ with parameters $b_1 < \cdots < b_n \in X$. Since $X \setminus Y$ is a set of indiscernibles over Y in L_δ, there are only $|Y| = \lambda$ many possibilities for A. Hence $|P(\lambda) \cap L| = |\lambda|$. It follows that $(\lambda^+)^L = (2^\lambda)^L$ is not a cardinal of V. $\square$

Corollary 5.9.11. Assume there exists a measurable cardinal. Then every uncountable cardinal of V is a strong limit cardinal in L. Hence, every regular uncountable cardinal of V is inaccessible in L.

Proof. Let κ be an uncountable cardinal. For all $\lambda < \kappa$ we have $|P(\lambda) \cap L| < \kappa$, hence $(\lambda^+)^L = (2^\lambda)^L < \kappa$. This shows that κ is a strong limit cardinal in L. If κ is regular, it is regular in L, hence inaccessible in L by what we have already proved. $\square$

Remark 5.9.12. One can actually prove that, if there exists a measurable cardinal, then every uncountable cardinal of V is inaccessible in L.

Corollary 5.9.13. If there exists a measurable cardinal, or even if $0^\#$ exists, then V is not a forcing extension of L.

Proof. Let G be L-generic with respect to a poset $P \in L$. Since P has the $|P|^+$-chain condition, P preserves all cardinals of L which are $\geq (|P|^+)^L$. But we have seen that $0^\#$ collapses arbitrarily large cardinals of L. Thus $\exists\, 0^\#$ implies $V \neq L[G]$. $\square$

Remark 5.9.14. In proving Rowbottom's Theorem and its corollaries, we did not use the measurable cardinal, but only the existence of $0^\#$. Furthermore, the only property of $0^\#$ that we used is that it is a nice EM-set for $V{=}L$.

Remark 5.9.15. Let $\exists\, 0^\#$ denote the assertion that there exists a nice EM-set for $V{=}L$. Clearly $\exists\, 0^\#$ is a Σ^1_3 sentence. Thus we have another example of a Σ^1_3 sentence which is not absolute. (Compare Corollary 4.6.2.) Namely, $\exists\, 0^\#$ is true if a measurable cardinal exists, and false if $V = L$ or if $V =$ a forcing extension of L.

5.10 The # operator

In this section we note some additional facts about $0^\#$, and we relativize to consider $f^\#$ for all $f \in \omega^\omega$.

Remark 5.10.1. Recall that $0^\#$ is by definition an EM-set for the language of set theory, $\{\in, =\}$. In particular, $0^\#$ is a set of $\{\in, =\}$-formulas. Identifying formulas with their Gödel numbers, we have $0^\# \subseteq \omega$. Clearly $0^\# \notin L$. In fact, the proof of Theorem 5.9.9 shows that $f \leq_T 0^\#$ for all $f \in \omega^\omega \cap L$.

Silver has proved the following additional properties of $0^\#$.

1. For any limit ordinal δ, $\mathrm{Hull}_{0^\#}(\delta) \cong L_\lambda$ where λ is an inaccessible cardinal of L.

2. For any regular uncountable cardinal κ of V, we have $L_\kappa = \mathrm{Hull}_{0^\#}(C)$ where $C \subseteq \kappa$ is a club of indiscernibles in L_κ.

3. The singleton set $\{0^\#\}$ is Π^1_2. Namely, $0^\#$ can be defined as the unique EM-set for $V{=}L$ which is nice and has some additional defining properties. The additional properties are simple syntactic conditions, hence arithmetical.

We now introduce a set-theoretic analog of Turing degrees.

Definition 5.10.2 (L-degrees). For $f, g \in \omega^\omega$ we say f *is constructible from* g, abbreviated $f \leq_L g$, if $f \in L[g]$. Note that $f \leq_L f$, and

$$f \leq_L g,\, g \leq_L h \Rightarrow f \leq_L h.$$

Thus we have a reducibility notion, analogous to Turing reducibility. The *L-degree* or *degree of constructibility* of $f \in \omega^\omega$ is

$$\deg_L(f) = \{g \mid f \equiv_L g\}.$$

Clearly the L-degrees are partially ordered by $\leq_L$, and $\deg_L(f \oplus g)$ is the least upper bound of $\deg_L(f)$ and $\deg_L(g)$.

Example 5.10.3. By forcing over L with perfect subtrees of $2^{<\omega}$, we obtain $g \in 2^\omega$ of *minimal* L-degree, i.e., $g \notin L$ and for all $f \leq_L g$ either $f \in L$ or $f \equiv_L g$. See Example 3.8.1 (Sacks). Similarly, many other problems and methods for Turing degrees can be lifted up to L-degrees.

Remark 5.10.4 (the L-jump). For any $f \in \omega^\omega$ we can relativize the definition of $0^\#$ to f. Namely, define $f^\#$ to be the EM-set for a club of indiscernibles in $(L_\kappa[f], \in | L_\kappa[f], f)$ where κ is any regular uncountable cardinal. The *sharp operator* $f \mapsto f^\#$ behaves as a jump operator for L-degrees. We have $f <_L f^\#$, and moreover $f \leq_L g \Rightarrow f^\# \leq_L g^\#$, so the sharp operator is well defined on L-degrees. In order to have a theory of L-degrees analogous to Turing degrees, it is convenient to assume $\forall f\, \exists g\, (f^\# = g)$, abbreviated $\forall f\, \exists f^\#$.

Remark 5.10.5. Relativizing the fact that $0^\#$ is a Π^1_2 singleton, we see that the 2-place predicate $f^\# = g$ is Π^1_2. Hence the sentence $\forall f\, \exists f^\#$ is Π^1_4. Because this sentence is lightface projective, it cannot literally imply the existence of large cardinals. For example, if $\forall f\, \exists f^\#$ is true in V, then it is true in R_κ where κ is the first inaccessible cardinal, and clearly $R_\kappa \vDash \mathsf{ZFC} + \neg\, \exists$ inaccessible cardinal. On the other hand, $\forall f\, \exists f^\#$ implies that every uncountable cardinal of V is inaccessible in $L[f]$ for all f, etc. Thus $\forall f\, \exists f^\#$ may be viewed as a kind of large cardinal axiom in some vague sense.

Remark 5.10.6. Instead of assuming the existence of a measurable cardinal, one can derive $\forall f\, \exists\, f^\#$ under the weaker assumption that there exists a Ramsey cardinal.

Definition 5.10.7 (Ramsey cardinals). A *Ramsey cardinal* is an uncountable cardinal κ such that for all $F : [\kappa]^{<\omega} \to \{0, 1\}$ there exists $X \subseteq \kappa$ of cardinality κ such that

$$\forall n \; |\mathrm{rng}(F \restriction [X]^n)| = 1.$$

Here we are writing $[\kappa]^{<\omega} = \bigcup_{n<\omega} [\kappa]^n = \{\text{finite subsets of } \kappa\}$.

Remark 5.10.8. It follows from Theorem 5.9.2 that every measurable cardinal is Ramsey.

Moreover, every measurable cardinal is a limit of Ramsey cardinals, etc. (To see this, let $j : V \to M$ be an elementary embedding with $j(\kappa) > \kappa$ and $j(\alpha) = \alpha$ for all $\alpha < \kappa$. Then $V \models \kappa$ is measurable, hence $V \models \kappa$ is Ramsey. Therefore $M \models \kappa$ is Ramsey, because $P(\kappa) \subseteq M$. Hence $M \models \exists \lambda < j(\kappa)$ such that λ is Ramsey, hence $V \models \exists \lambda < \kappa$ such that λ is Ramsey. Etc.)

It can also be shown that every Ramsey cardinal is inaccessible, Mahlo, etc. Also, the existence of a Ramsey cardinal implies (but is not equivalent to) $\forall f \, \exists f^{\#}$.

Chapter 6

Determinacy

Under construction .... FIXME

6.1 Games and determinacy

Definition 6.1.1. To each set $S \subseteq \omega^\omega$ we associate an *infinite game with perfect information*, $G(S)$, a.k.a., the *Gale/Stewart game*. There are two players, I and II. A play of the game consists of a series of moves where initially I picks $n_0 \in \omega$, then II picks $n_1 \in \omega$, then I picks $n_2 \in \omega$, and so on. At stage $2i$ player I picks n_{2i}, and at stage $2i+1$ player II picks n_{2i+1}. This game is said to have perfect information, because at stage j in the play of the game, both I and II are aware of $n_0, n_1, \ldots, n_{j-1}$. At the end of the game, a function $h \in \omega^\omega$ is defined by $h(i) = n_i$ for all i. We declare that I wins if $h \in S$, and II wins if $h \notin S$.

Remark 6.1.2. The motivating question throughout this chapter will be, for which S is it possible for I or II to always win. In order to explain this, we first define precisely how the function h is formed, and what it means for player I or player II to have a winning strategy.

Definition 6.1.3. Define Seq_I and Seq_{II} as follows:

$$\begin{aligned}\mathrm{Seq}_I &= \{\sigma \in \mathrm{Seq} \mid \mathrm{lh}(\sigma) \text{ is even}\},\\ \mathrm{Seq}_{II} &= \{\sigma \in \mathrm{Seq} \mid \mathrm{lh}(\sigma) \text{ is odd}\}.\end{aligned}$$

A *strategy for I* is a function $f_I : \mathrm{Seq}_I \to \omega$. A *strategy for II* is a function $f_{II} : \mathrm{Seq}_{II} \to \omega$. Thus a strategy is a function that takes the current history of the game and produces the next move, for either I or II.

Definition 6.1.4. Given strategies f_I and f_{II} for I and II respectively, define a function $h = f_I \otimes f_{II}$ as follows:

$$h(2i) = f_I(h[2i]), \quad h(2i+1) = f_{II}(h[2i+1]).$$

Recall that $h[k] = \langle h(0), \ldots, h(k-1)\rangle$. Thus $f_I \otimes f_{II}$ is the play of the game where I and II play according to their strategies f_I and f_{II} respectively.

Definition 6.1.5. The strategy f_I is a *winning strategy for I in $G(S)$* provided $f_I \otimes f_{II} \in S$ for all f_{II}. Similarly, f_{II} is a *winning strategy for II in $G(S)$* provided $f_I \otimes f_{II} \notin S$ for all f_I.

Obviously players I and II cannot both have a winning strategy in $G(S)$. We are interested in games which admit a winning strategy for one of the players. Such games are said to be *determined*.

Definition 6.1.6. The game $G(S)$ is *determined* if either I or II has a winning strategy for $G(S)$.

Definition 6.1.7 (the Axiom of Determinacy). The Axiom of Determinacy, abbreviated AD, is the statement that $G(S)$ is determined for all $S \subseteq \omega^\omega$.

Remark 6.1.8. There is a plausibility argument for AD, which runs as follows. A sentence A in first order logic can be written in prenex form as

$$A \;\equiv\; \exists n_0 \, \forall n_1 \, \exists n_2 \, \forall n_3 \, \cdots \, n_k \, S(n_0, n_1, n_2, n_3, \ldots, n_k).$$

Then A can be read as asserting the existence of a winning strategy for I. Namely, I can choose n_0 such that for all n_1 that II choses, I can choose n_2, and so on. Similarly, we can read $\neg A$ as asserting the existence of a winning strategy for II in a similar way:

$$\neg A \;\equiv\; \forall n_0 \, \exists n_1 \, \forall n_2 \, \exists n_3 \, \cdots \, n_k \, \neg S(n_0, n_1, n_2, n_3, \ldots, n_k).$$

Thus the Law of the Excluded Middle, $A \vee \neg A$, asserts determinacy for finite games. The Axiom of Determinacy extends this to infinite games, i.e., we have

$$\begin{aligned} &\exists n_0 \, \forall n_1 \, \cdots \, \exists n_{2i} \, \forall n_{2i+1} \, \cdots \, S(n_0, n_1, \ldots, n_{2i}, n_{2i+1}, \ldots) \\ \vee \;\; &\forall n_0 \, \exists n_1 \, \cdots \, \forall n_{2i} \, \exists n_{2i+1} \, \cdots \, \neg S(n_0, n_1, \ldots, n_{2i}, n_{2i+1}, \ldots) \end{aligned}$$

where $S(n_0, n_1, \ldots, n_{2i}, n_{2i+1}, \ldots)$ is an ω-ary predicate on ω.

Remark 6.1.9. We shall prove that AD is false. However, the proof uses the Axiom of Choice, and it is known that ZFC proves determinacy for some specific classes of sets, e.g., Borel sets. Furthermore, it is believed that ZF (without the Axiom of Choice) is consistent with AD, and that ZFC is consistent with the assumption of determinacy for a wide class of sets, known as the projective sets. See below.

We now exhibit a set $S \subseteq \omega^\omega$ for which the game $G(S)$ is not determined.

Theorem 6.1.10. There exists $S \subseteq \omega^\omega$ such that $G(S)$ is not determined. Hence AD is false.

Proof. For each $f : \mathrm{Seq}_I \to \omega$ put $A_f = \{f \otimes g \mid g : \mathrm{Seq}_{II} \to \omega\}$. Thus A_f is the set of plays where I follows the strategy f. Similarly, for each $g : \mathrm{Seq}_{II} \to \omega$ put $B_g = \{f \otimes g \mid f : \mathrm{Seq}_I \to \omega\}$, the set of plays where II follows the strategy g. Put $\kappa = 2^{\aleph_0}$. Clearly each A_f and each B_g is of cardinality κ. Therefore, by transfinite induction along a well ordering of ω^ω of order type κ, we can construct (the characteristic function of) a set $S \subseteq \omega^\omega$ such that $A_f \setminus S \neq \emptyset$ for all f, and $B_g \cap S \neq \emptyset$ for all g. Clearly $G(S)$ is not determined. $\square$

6.2 Open and Borel determinacy

While ZFC refutes full determinacy, it can be shown that ZFC proves determinacy for certain classes of sets. Below we shall show that open games are determined. We first need some definitions and lemmas.

Definition 6.2.1. Given $\sigma \in \mathrm{Seq}$ and f_I and f_{II}, define $f_I \otimes_\sigma f_{II} = h$ by

$$h(k) = \begin{cases} \sigma(k) & \text{if } k < \mathrm{lh}(\sigma), \\ f_I(h[k]) & \text{if } k \geq \mathrm{lh}(\sigma) \text{ and k is even,} \\ f_{II}(h[k]) & \text{if } k \geq \mathrm{lh}(\sigma) \text{ and k is odd.} \end{cases}$$

Thus $f_I \otimes_\sigma f_{II}$ is the play in which I and II follow strategies f_I and f_{II} respectively, starting from position σ.

Definition 6.2.2. In the game $G(S)$, $\sigma \in \mathrm{Seq}$ is a *winning position for I* if there exists f_I such that for all f_{II}, $f_I \otimes_\sigma f_{II} \in S$. Similarly, σ is a winning position for II in $G(S)$ if there exists f_{II} such that for all f_I, $f_I \otimes_\sigma f_{II} \notin S$.

Lemma 6.2.3. We have that σ is a winning position for I if and only if $\mathrm{lh}(\sigma)$ is even and $\exists n\, (\sigma^\frown\langle n\rangle$ is a winning position for $I)$, or $\mathrm{lh}(\sigma)$ is odd and $\forall n\, (\sigma^\frown\langle n\rangle$ is a winning position for $I)$. A similar lemma holds for σ being a winning position for II.

Proof. Suppose for instance that $\mathrm{lh}(\sigma)$ is odd and $\forall n\, (\sigma^\frown\langle n\rangle$ is a winning position for $I)$. Then for each n, by the Countable Axiom of Choice, pick f_n a winning strategy for I starting at $\sigma^\frown\langle n\rangle$. Define a winning strategy f_I for I starting at σ by $f_I(\sigma^\frown\langle n\rangle^\frown\tau) = f_n(\sigma^\frown\langle n\rangle^\frown\tau)$ for all $n \in \omega$ and all $\tau \in \mathrm{Seq}$ of even length. $\square$

Theorem 6.2.4. If $S \subseteq \omega^\omega$ is open or closed, then $G(S)$ is determined.

Proof. Assume that S is open. (The proof for S closed is similar.)

Assume I does not have a winning strategy for $G(S)$. We shall define a winning strategy f_{II} for II. The idea behind f_{II} will be that II plays so as to avoid winning positions for I. For all σ of odd length, if there exists n such that $\sigma^\frown\langle n\rangle$ is not a winning position for I, define $f_{II}(\sigma)$ to be such an n. Otherwise, define $f_{II}(\sigma) = 0$.

We claim that, for all f_I and k, $(f_I \otimes f_{II})[k]$ is not a winning position for I. This is proved by induction on k, using Lemma 6.2.3. Put $h = f_I \otimes f_{II}$. For $k = 0$, since I does not have a winning strategy for $G(S)$, the empty sequence $\langle\rangle = h[0]$ is not a winning position for I. Now assume inductively that $h[k]$ is not a winning position for I. If k is even, then by Lemma 6.2.3 $h[k]^\frown\langle n\rangle$ is not a winning position for I for any n, in particular $h[k+1]$ is not a winning position for I. If k is odd, then by Lemma 6.2.3 there exists n such that $h[k]^\frown\langle n\rangle$ is not a winning position for I, hence $h(k) = f_{II}(h[k])$ is such an n. Thus $h[k+1] = h[k]^\frown\langle h(k)\rangle$ is not a winning positon for I.

Next we claim that f_{II} is a winning strategy for II. To see this, recall that S is open, hence $S = \omega^\omega \setminus [T]$ where $T \subseteq \mathrm{Seq}$ is a tree. Clearly any $\sigma \notin T$ is a winning position for I. Hence by our previous claim we have that, for all f_I and all k, $(f_I \otimes f_{II})[k] \in T$. Hence $f_I \otimes f_{II} \in [T]$, i.e., $f_I \otimes f_{II} \notin S$. This completes the proof. □

Remark 6.2.5. If A is an arbitrary set and $S \subseteq A^\omega$, we can define the game $G(S)$ analogously to the above. Instead of playing elements of ω, elements of A are played. The same proof as above shows that if $S \subseteq A^\omega$ is open or closed, then $G(S)$ is determined. Note that, for $S \subseteq A^\omega$, S being closed is equivalent to $S = [T]$, the paths through a tree $T \subseteq A^{<\omega}$.

Remark 6.2.6. Historically, the determinacy of open and closed sets was proved simultaneously with the introduction of Gale/Stewart games. As time went on, determinacy of F_σ sets, G_δ sets, $F_{\sigma\delta}$ sets, $G_{\delta\sigma}$ sets, etc., was proved, via more and more difficult proofs. Eventually Martin proved the ultimate generalization of these results: all Borel sets are determined.

Definition 6.2.7 (Borel sets). The *Borel sets* in a topological space are the smallest class of sets containing the open and closed sets and closed under complementation, countable union, and countable intersection. The *rank* of a Borel set is the number of times these operations are applied to obtain the set.

Remark 6.2.8. Note that the rank of a Borel set is a countable ordinal. It is known that there exist Borel sets in ω^ω of all ranks $\alpha \in \Omega$. Here Ω denotes the set of countable ordinals.

Theorem 6.2.9 (Martin). For all Borel sets $S \subseteq \omega^\omega$, $G(S)$ is determined.

Proof. We omit the details of the proof, but see Remark 6.2.10 below. The details are presented in Martin [8] and in Kechris [7]. □

Remark 6.2.10. The proof of Borel determinacy proceeds by induction on Borel rank. A key ingredient in the proof is the consideration of games on A^ω where A is an arbitrary set. Borel games $S \subseteq \omega^\omega$ are reduced to open games in A^ω, where A is an appropriately large set. If S is Borel of rank α, then A is of cardinality $\beth_\alpha$. As a byproduct, one obtains determinacy of Borel games on A^ω for arbitrary A, and the proof of this uses open games on $R_\alpha(A)$, the αth iterated powerset of A, where $\alpha \in \Omega$. Note that $|R_\alpha(A)| = \beth_\alpha(|A|)$.

Remark 6.2.11. In the rest of this chapter we consider determinacy for a wider class of sets $S \subseteq \omega^\omega$, known as the projective sets.

6.3 Projective sets

The projective hierarchy is a classification of sets similar to the arithmetical hierarchy. Sets in the projective hierarchy can be thought of as sets of reals that have a simple description.

Definition 6.3.1 (the projective hierarchy). $S \subseteq \omega^\omega$ is said to be $\mathbf{\Sigma}^1_n$ if and only if S is $\Sigma^{1,f}_n$ for some $f \in \omega^\omega$. Thus we have

$$\mathbf{\Sigma}^1_n = \bigcup_{f \in \omega^\omega} \Sigma^{1,f}_n.$$

The definitions for $\mathbf{\Pi}^1_n$, $\mathbf{\Delta}^1_n$, $\mathbf{\Sigma}^0_n$, $\mathbf{\Pi}^0_n$, $\mathbf{\Delta}^0_n$ are similar. Note the use of boldface letters. We extend these notions to arbitrary Polish spaces in the obvious way. For any Polish space X, a set $S \subseteq X$ is said to be *projective* if $S \in \bigcup_{n=0}^\infty \mathbf{\Sigma}^1_n$, i.e., S is (boldface) $\mathbf{\Sigma}^1_n$ for some $n < \omega$.

Remark 6.3.2. The (boldface) *projective hierarchy* is a variant of the lightface projective hierarchy which was introduced in Definition 4.2.1. Our use of boldface letters $\mathbf{\Sigma}, \mathbf{\Pi}, \mathbf{\Delta}$ rather than lightface letters Σ, Π, Δ denotes the fact that we are allowing arbitrary parameters from ω^ω. Compare Remark 2.3.10. In particular $\mathbf{\Sigma}^0_1 =$ open, $\mathbf{\Pi}^0_1 =$ closed, $\mathbf{\Sigma}^0_2 = F_\sigma$, $\mathbf{\Pi}^0_2 = G_\delta$, etc., and this may be called the *boldface arithmetical hierarchy*. See also Rogers [11, Chapters 15 and 16].

Remark 6.3.3. Projective sets are usually viewed as sets which can be described in a relatively simple way. Indeed, $S \subseteq \omega^\omega$ is projective if and only if S is definable with parameters over the standard model of second order arithmetic, $(P(\omega), \omega, +, \cdot, =, \in)$. More dramatically, the projective sets in Euclidean space $\mathbb{R}^k$ are just the sets which are definable with parameters over the real number system with the integers as an extra predicate, i.e., over the structure $(\mathbb{R}, \mathbb{Z}, +, \cdot, =)$.

Remark 6.3.4 (descriptive set theory). The boldface arithmetical and projective hierarchies are studied in the subject known as *descriptive set theory*, going back to Borel, Lebesgue, Hausdorff, Souslin et al. From the axiomatic viewpoint, it is known that the study of higher levels of the projective hierarchy, $\mathbf{\Delta}^1_2$ and beyond, is delicate, in that basic properties of these sets are known to be independent of ZFC. See Jech [5, Chapter 7].

Remark 6.3.5 (classical descriptive set theory). On the other hand, the lowest levels of the projective hierarchy, $\mathbf{\Delta}^1_1$ and $\mathbf{\Sigma}^1_1$, are very well understood, and their basic properties can be proved in ZFC. For example, the next two theorems go back to Souslin and provide alternative characterizations of the $\mathbf{\Delta}^1_1$ and $\mathbf{\Sigma}^1_1$ sets. We omit the proofs of these theorems, but see the textbook of Kechris [7].

Definition 6.3.6 (Borel sets). Let X be a Polish space. The *Borel sets* in X are the smallest family of sets in X including the open sets and closed under complementation and countable union and intersection. Thus the Borel sets include the boldface arithmetical hierarchy, i.e., $\mathbf{\Sigma}^0_n$ and $\mathbf{\Pi}^0_n$ for all $n < \omega$, and extends this into the transfinite. See also Definition 6.2.7.

Theorem 6.3.7. *S is Borel if and only if S is $\mathbf{\Delta}^1_1$.*

Definition 6.3.8 (analytic sets). Let X be a Polish space. $S \subseteq X$ is *analytic* if $S = \text{range}(F)$ for some continuous function $F : \omega^\omega \to X$.

Theorem 6.3.9. *S is analytic if and only if S is $\mathbf{\Sigma}^1_1$. Hence, S is coanalytic (the complement of an analytic set) if and only if S is $\mathbf{\Pi}^1_1$.*

6.4 Consequences of projective determinacy

We consider the statement that all projective Gale/Stewart games are determined.

Definition 6.4.1 (projective determinacy). We define *projective determinacy*, abbreviated PD, to be the statement that the game $G(S)$ is determined for all projective sets $S \subseteq \omega^\omega$. Also, $\mathbf{\Sigma}^1_n$ *determinacy*, abbreviated $\mathbf{\Sigma}^1_n$-AD, is the statement that $G(S)$ is determined for all $\mathbf{\Sigma}^1_n$ sets S, etc. Thus we have $\text{PD} \equiv \forall n\,(\mathbf{\Sigma}^1_n\text{-AD})$.

We begin by noting that PD is not a theorem of ZFC.

Theorem 6.4.2. *If $V{=}L$ holds, then PD fails. In fact, Δ^1_2 determinacy fails.*

Proof. Assume $V{=}L$. By Corollary 4.6.5 there is a Δ^1_2 well ordering $\prec$ of ω^ω. Using this well ordering in the proof of Theorem 6.1.10, we obtain a Δ^1_2 set $S \subseteq \omega^\omega$ such that $A_f \setminus S \neq \emptyset$ for all f and $B_g \cap S \neq \emptyset$ for all g. Hence $G(S)$ is not determined. $\square$

Remark 6.4.3. We shall see later that even Σ^1_1 determinacy is not provable in ZFC. In fact, Σ^1_1 determinacy fails in L and all forcing extensions of L. Moreover, Harrington has shown that Σ^1_1 determinacy is equivalent to the existence of $0^\#$, and $\mathbf{\Sigma}^1_1$ determinacy is equivalent to $\forall f\,\exists f^\#$. It is also known that ZFC plus the existence of measurable cardinals is not sufficient to prove Δ^1_2 determinacy.

Remark 6.4.4. On the other hand, Martin's Theorem 6.2.9 gives us $\mathbf{\Delta}^1_1$ determinacy, in ZFC. In addition, Martin has shown that $\mathbf{\Sigma}^1_1$ determinacy holds provided a measurable cardinal exists (see Theorem 6.6.1 below). Furthermore, Woodin has shown that PD holds provided a supercompact cardinal exists. Now of course measurable cardinals are known to be very large, and supercompact cardinals are known to be even much larger. Nevertheless, it is believed that the existence of a supercompact cardinal is consistent with ZFC. If this is so, then it would follow that PD is consistent with ZFC.

Remark 6.4.5. An important reason for considering PD is that it answers many questions about the structure of projective sets. Because of this, PD has been proposed as a reasonable psuedo-axiom to add to ZFC.

For example, it is well known and provable in ZFC that $\mathbf{\Sigma}^1_1$ sets (1) are Lebesgue measurable, (2) have the property of Baire, and (3) have the perfect set property, i.e., they are countable or contain a perfect set. The generalization of these regularity properties to higher projective classes is problematic, but assuming PD one has the following results.

Theorem 6.4.6. Assume PD. Then:

1. (PLM) In 2^ω, $[0,1]$, $\mathbb{R}^n$ etc., every projective set is Lebesgue measurable.
2. (PBC) In any Polish space, every projective set has the property of Baire.
3. (PPS) In any Polish space, every projective set either is countable or contains a perfect set.

Proof. In order to prove PD $\Rightarrow$ PLM, we first note the following lemma.

Lemma 6.4.7. PLM is equivalent to the following statement, PLM(0):

> If S is projective and $\mu(Z) = 0$ for all for all measurable $Z \subseteq S$, then $\mu(S) = 0$.

Here μ denotes Lebesgue measure.

Proof. Trivially PLM implies PLM(0). Conversely, assume PLM(0), and suppose A is projective. Let $\mu^*(A)$ be the outer measure of A. For each $n < \omega$ choose an open set $U_n \supseteq A$ such that $\mu(U_n) \leq \mu^*(A) + 1/2^n$. Put $B = \bigcap_n U_n$. Since B is a G_δ set, B is measurable and projective. In particular $B \setminus A$ is projective. Also, it is clear that if $Z \subseteq B \setminus A$ is measurable then $\mu(Z) = 0$. Hence by PLM(0) we have $\mu(B \setminus A) = 0$. It follows that A is measurable, with $\mu(A) = \mu^*(A) = \mu(B)$. $\square$

Proof of PD $\Rightarrow$ PLM. Assume PD. We shall prove PLM(0). Assume $S \subseteq [0,1]$ is projective such that $\mu(Z) = 0$ for all measurable $Z \subseteq S$. Fix $\epsilon > 0$. We shall show that $\mu^*(S) \leq \epsilon$. Since this holds for all $\epsilon > 0$, we will have $\mu(S) = 0$.

Consider the following game, called a *covering game*. I plays a sequence of 0's and 1's $\langle a_n \rangle_n$ defining a real number $x = \sum_{n=0}^\infty a_n/2^{n+1}$ in $[0,1]$. II plays a sequence of (Gödel numbers of) finite unions of rational open intervals U_n in $[0,1]$ such that $\mu(U_n) \leq \epsilon/2^{2n+1}$ for all n. I wins if and only if $x \in S$ and $x \notin \bigcup_{n<\omega} U_n$. Thus II is trying to cover S. Clearly this game is projective.

We claim that I does not have a winning strategy. Suppose f_I is a winning strategy for I. Let Z be the set of reals played by I according to f_I, i.e., $Z = \{x \in [0,1] \mid \exists \langle U_n \rangle_n \, (I \text{ plays } x \text{ using } f_I \text{ in response to } II \text{ playing } \langle U_n \rangle_n)\}$. By construction $Z \subseteq S$, and clearly Z is $\mathbf{\Sigma}^1_1$, using h as a parameter. Hence Z is measurable, so by our assumption on S we have $\mu(Z) = 0$. In particular there exists $\langle U_n \rangle_n$ such that $Z \subseteq \bigcup_n U_n$ and $\mu(U_n) < \epsilon/2^{2n+1}$ for all n. Then II can win against f_I by playing $\langle U_n \rangle_n$, a contradiction. This proves our claim.

Since I does not have a winning strategy, PD implies that II has a winning strategy, call it f_{II}. We shall use f_{II} to show that $\mu^*(S) \le \epsilon$. For each $\sigma \in 2^{<\omega}$ let V_σ be the U_n played by II using f_{II} at stage $n = \mathrm{lh}(\sigma)$ in response to I playing σ. Note that $\mu(V_\sigma) \le \epsilon/2^{2n+1}$. Put $V = \bigcup_{\sigma \in 2^{<\omega}} V_\sigma$. Note that, since f_{II} is a winning strategy for II, $S \subseteq V$. We have

$$\mu(V) \le \sum_{\sigma \in 2^{<\omega}} \mu(V_\sigma) \le \sum_{n=0}^{\infty} \sum_{\mathrm{lh}(\sigma)=n} \frac{\epsilon}{2^{2n+1}} = \sum_{n=0}^{\infty} 2^n \frac{\epsilon}{2^{2n+1}} = \sum_{n=0}^{\infty} \frac{\epsilon}{2^{n+1}} = \epsilon.$$

Hence $\mu^*(S) \le \epsilon$. This completes the proof. $\square$

Proof of PD $\Rightarrow$ PBC. Assume PD. Let $S \subseteq \omega^\omega$ be projective. We shall show that S has the property of Baire, i.e., there exists an open set U such that $(S \setminus U) \cup (U \setminus S)$ is meager. Consider the game $G^{**}(S)$ played as follows. Players I and II take turns choosing finite sequences $\sigma_0, \tau_0, \ldots, \sigma_n, \tau_n, \ldots$ with

$$\sigma_0 \subset \tau_0 \subset \cdots \subset \sigma_n \subset \tau_n \subset \cdots.$$

Put $f = \bigcup_n \sigma_n = \bigcup_n \tau_n \in \omega^\omega$. I wins if $f \in S$, and II wins if $f \notin S$. Clearly this game is projective.

Claim 1. II has a winning strategy if and only if S is meager. FIXME

Claim 2. FIXME

Let $X = \{\sigma \in \omega^\omega \mid FIXME\}$, and put $U = \{f \in \omega^\omega \mid \exists \sigma \in X\,(\sigma \subset f)\}$. Then U is open and $(S \setminus U) \cup (U \setminus S)$ is meager. This completes the proof. $\square$

Proof of PD $\Rightarrow$ PPS. Assume PD. Let $S \subseteq 2^\omega$ be projective. We shall show that S is countable or contains a perfect set. Consider the following game $G^*(S)$, known as a *star game*. I chooses $\sigma_0 \in \omega^{<\omega}$, then II chooses $i_0 \in \{0,1\}$, then I chooses $\sigma_1 \supseteq \sigma_0{}^\frown\langle i_0\rangle$, then II chooses $i_1 \in \{0,1\}$, then I chooses $\sigma_2 \supseteq \sigma_1{}^\frown\langle i_1\rangle$, ... Put $f = \bigcup_n \sigma_n \in 2^\omega$. I wins if $f \in S$, and II wins if $f \notin S$. Clearly this game is projective.

Claim 1. If I has a winning strategy, then S includes a perfect set. FIXME

Claim 2. If II has a winning strategy, then S is countable. FIXME

By PD either I or II has a winning strategy, so the proof is complete. $\square$

This completes the proof of Theorem 6.4.6. $\square$

Remark 6.4.8. The proof of Theorem 6.4.6 generalizes to the setting of AD, the full Axiom of Determinacy. Namely, in $\mathsf{ZF} + \mathrm{AD} + \mathrm{DC}$ we can prove that arbitrary sets are Lebesgue measurable and have the property of Baire and the perfect set property. Of course, each of these three statements is easily refutable using the Axiom of Choice.

Remark 6.4.9. None of the above regularity properties of projective sets are provable in ZFC. For example, assume $V{=}L$, and let $\prec$ be a Δ^1_2 well ordering of ω^ω as in Corollary 4.6.5. Using $\prec$ as in the proof of Theorem 6.4.2, we can construct a Δ^1_2 set $S \subseteq 2^\omega$ such that neither S nor $2^\omega \setminus S$ contains a perfect set. It follows that S is not Lebesgue measurable, does not have the property of

Baire, and does not have the perfect set property. Thus PLM, PBC, and PPS fail for S. More generally, if $\omega^\omega \subseteq L[f]$ for some $f \in \omega^\omega$, then we can construct a $\Delta_2^{1,f}$ set for which PLM, PBC, and PPS fail. In addition, it is known that PLM, PBC, and PPS fail in many other models of ZFC.

Remark 6.4.10 (the Solovay model). Solovay has constructed an interesting model of ZFC in which PLM, PBC, and PPS all hold. Furthermore, this model can even be a forcing extension of L.

Specifically, let M be any countable transitive model of ZFC + GCH + $\exists$ an inaccessible cardinal, κ. Consider a forcing extension $M[G]$ which collapses all cardinals $< \kappa$ to $\aleph_0$ but leaves κ uncountable. Here G is an M-generic filter on the partial ordering $P \in M$ defined by $P = \{p \mid p$ is a finite partial function from $\kappa \times \omega$ into κ such that $p((\alpha, n)) \leq \alpha$ for all $(\alpha, n) \in \mathrm{dom}(p)\}$. As usual, $p \leq q \iff p \supseteq q$. We know that $M[G] \models \mathsf{ZFC}$, and it is not difficult to show that $\aleph_1^{M[G]} = \kappa$. The model $M[G]$ is known as *the Solovay model*. Solovay has shown that $M[G] \models \text{PLM} + \text{PBC} + \text{PPS}$. Thus, the consistency of ZFC+PLM+PBC+PPS follows from the consistency of ZFC+$\exists$ an inaccessible cardinal.

Moreover, since M can satisfy $V{=}L$, and $M[G]$ is a forcing extension of M, we see that ZFC + PLM + PBC + PPS is consistent with V being a forcing extension of L. This is interesting, because we shall see later that PD (in fact Σ_1^1-AD) fails in all forcing extensions of L.

Remark 6.4.11. It is known that Solovay's assumption of an inaccessible cardinal in the ground model cannot be omitted. Namely, the following statements are pairwise equivalent:

1. The perfect set property for $\mathbf{\Pi}_1^1$ sets.
2. The perfect set property for $\mathbf{\Sigma}_2^1$ sets.
3. $\forall f \in \omega^\omega$ ($\omega^\omega \cap L[f]$ is countable).
4. $\forall f \in \omega^\omega$ ($\aleph_1$ is inaccessible in $L[f]$).

In particular, PPS imples that $\aleph_1$ is inaccessible in L.

It is also known that PLM implies that $\aleph_1$ is inaccessible in L, but PBC does not imply this. These results and much more on set-theoretic aspects of the continuum may be found in Bartoszynski/Judah [1].

Remark 6.4.12 (the Ramsey property). In addition to Lebesgue measurability, the property of Baire, and the perfect set property, there are many other regularity properties which have been considered. One of the most interesting is the *Ramsey property*. For $X \subseteq \omega$ we write $[X]^\omega =$ the set of infinite subsets of X. A set $S \subseteq [\omega]^\omega$ is said to be *Ramsey* if there exists $X \in [\omega]^\omega$ such that $[X]^\omega \subseteq S$ or $[X]^\omega \cap S = \emptyset$. It is known that $\mathbf{\Sigma}_1^1$ sets are Ramsey, and $V{=}L$ implies the existence of a Δ_2^1 set which is not Ramsey. Let PRP be the statement that all projective sets are Ramsey. It is known that the Solovay model satisfies PRP. It seems reasonable to conjecture that PD implies PRP, but this appears to be an open question.

Another aspect of projective sets is the question of uniformization:

Definition 6.4.13 (uniformization). Let Γ be a class of sets, e.g., $\Gamma = \Pi^1_1$. By Γ *uniformization* we mean the statement that, for all $R \subseteq \omega^\omega \times \omega^\omega$ in Γ, there exists $\widehat{R} \subseteq R$ in Γ such that

$$\forall f\,[\,(\exists g\, R(f,g)) \iff (\exists\,\text{unique}\ g)\, \widehat{R}(f,g)\,].$$

Remark 6.4.14. Note that uniformization for a lightface projective class Γ easily implies uniformization for the corresponding relativized or boldface class $\boldsymbol{\Gamma}$, where

$$\boldsymbol{\Gamma} = \bigcup_{f\in\omega^\omega} \Gamma^f.$$

For example, Π^1_1 uniformization easily implies $\boldsymbol{\Pi}^1_1$ uniformization.

Remark 6.4.15 (Kondo's Theorem). Π^1_1 uniformization is provable in ZFC. It follows that $\boldsymbol{\Pi}^1_1$ uniformization is provable in ZFC. This is a famous, classical result known as Kondo's Theorem. See Kechris [7].

Theorem 6.4.16. PD implies Π^1_n uniformization, for $n = 3, 5, 7, \ldots$.

Proof. See Kechris [7]. $\square$

Remark 6.4.17. Π^1_n uniformization easily implies Σ^1_{n+1} uniformization. In particular, ZFC proves Σ^1_2 uniformization, and $\mathsf{ZFC}+\mathrm{PD}$ proves Σ^1_n uniformization for $n = 4, 6, 8, \ldots$. On the other hand, using a Δ^1_2 well ordering as in Corollary 4.6.5, it can be shown that $\mathsf{ZFC}+\mathrm{V{=}L}$ proves Σ^1_n uniformization for all $n \geq 3$. Thus the behavior of the projective classes with respect to uniformization is quite different under the contrasting assumptions PD and $V{=}L$.

Remark 6.4.18. We do not know whether it is possible for Π^1_3 uniformization, or even $\boldsymbol{\Pi}^1_3$ uniformization, to hold in a forcing extension of L.

6.5 Turing degree determinacy

Determinacy is of importance in mathematical logic beyond descriptive set theory. In particular, determinacy has striking consequences for the structure of the Turing degrees, as we shall now see.

Lemma 6.5.1. Let $S \subseteq \omega^\omega$, and consider the game $G(S)$. If f_I is a winning strategy for I, then every Turing degree $\geq \deg_T(f_I)$ contains a member of S. If f_{II} is a winning strategy for II, then every Turing degree $\geq \deg_T(f_{II})$ contains a member of $\omega^\omega \setminus S$.

Proof. Let f_I be a winning strategy for I in $G(S)$. Given $g \geq_T f_I$, let h be the result of playing g against f_I, i.e., $h = f_I \otimes f_{II}$ where $f_{II}(\sigma) = g(n)$ for all $\sigma \in \mathrm{Seq}_{II}$ of length $2n+1$, for all n. By construction we have $f_{II} \equiv_T g$, hence $h \leq_T f_I \oplus g \equiv_T g$. Also, $h \in S$, since f_I is a winning strategy for I. Furthermore, $g \leq_T h$, in fact $h = f \oplus g$ for a certain f. Thus $h \equiv_T g$, and this gives the first part of the lemma. The second part is similar. $\square$

Theorem 6.5.2 (Martin). Let $S \subseteq \omega^\omega$ be closed under Turing equivalence. I has a winning strategy in $G(S)$ if and only if $\exists f\,(\forall g \geq_T f)\,(g \in S)$. II has a winning strategy in $G(S)$ if and only if $\exists f\,(\forall g \geq_T f)\,(g \notin S)$.

Proof. This follows easily from the previous lemma. □

Corollary 6.5.3. Let $S \subseteq \omega^\omega$ be Borel and closed under Turing equivalence. Then there exists f such that $(\forall g \geq_T f)\,(g \in S)$ or $(\forall g \geq_T f)\,(g \notin S)$.

Proof. Immediate from Theorems 6.2.9 and 6.5.2. □

Corollary 6.5.4. Assume PD. Let $S \subseteq \omega^\omega$ be projective and closed under Turing equivalence. Then there exists f such that $(\forall g \geq_T f)\,(g \in S)$ or $(\forall g \geq_T f)\,(g \notin S)$.

Corollary 6.5.5. The following is provable in $\mathsf{ZF} + \mathrm{AD}$. Let $S \subseteq \omega^\omega$ be closed under Turing equivalence. Then there exists f such that $(\forall g \geq_T f)\,(g \in S)$ or $(\forall g \geq_T f)\,(g \notin S)$.

Remark 6.5.6 (the Martin filter). Recall that $\mathcal{D}_T$ is the set of all Turing degrees. By a *cone of Turing degrees* we mean the set of all Turing degrees $\geq$ some fixed Turing degree. Clearly the cones generate a countably additive filter on $\mathcal{D}_T$. This filter is called the *Martin filter*. Corollaries 6.5.3, 6.5.4, 6.5.5 assert that the Martin filter is an ultrafilter with respect to certain sets of Turing degrees, under certain assumptions. This phenomenon is known as *Turing degree determinacy*. If we assume full AD, then the Martin filter is actually an ultrafilter on *all* sets of Turing degrees, the so-called *Martin ultrafilter* on $\mathcal{D}_T$. Of course, this conclusion is easily refutable using the Axiom of Choice.

Example 6.5.7 (a cone of minimal covers). Here is an example of Turing degree determinacy. A Turing degree $\mathbf{b}$ is said to be a *minimal cover* if there exists $\mathbf{a} < \mathbf{b}$ such that $\mathbf{b}$ is *minimal over* $\mathbf{a}$, i.e., there is no $\mathbf{c}$ such that $\mathbf{a} < \mathbf{c} < \mathbf{b}$. Clearly the set of minimal covers is Borel (in fact Σ^0_5). Relativizing Theorem 2.8.10, we see that for all $\mathbf{a}$ there exists $\mathbf{b} > \mathbf{a}$ such that $\mathbf{b}$ is minimal over $\mathbf{a}$, hence in particular $\mathbf{b}$ is a minimal cover. It follows by Corollary 6.5.3 that there exists a cone of minimal covers, i.e., there exists a Turing degree $\mathbf{b}_0$ such that every $\mathbf{b} \geq \mathbf{b}_0$ is a minimal cover. Without determinacy, this result would be highly non-obvious.

6.6 $\boldsymbol{\Sigma}^1_1$ determinacy

Theorem 6.6.1 (Martin). If there exists a measurable cardinal, then $\boldsymbol{\Sigma}^1_1$ determinacy holds.

Proof. We use the fact that the existence of a measuarable cardinal implies the existence of a set of indiscernable ordinals.

We will use the Kleene-Brouwer ordering $\leq_{KB}$ of $\omega^{<\omega}$. The relevant properties of this ordering are that it is a definable linear order of Seq and the for any tree $T \subset \mathrm{Seq}$, T has a path iff T contains a $\leq_{KB}$-descending sequence.

I	$f(0)$		$f(1)$		$f(2)$		$\ldots$
II		$\langle g(0), t(0)\rangle$		$\langle g(1), t(1)\rangle$		$\langle g(n), t(n)\rangle$	$\ldots$

Figure 6.1: The game $G'(S)$

Let S be a Σ^1_1-set. Our goal is to show that the game G_S is determined. We use Kleene normal form to find a primitive recursive relation $\Theta(a, b, c, d)$ such that $f \oplus g \in S \iff \exists h \forall n \Theta(f[n], g[n], h[n], n)$. Hence for each $f \oplus g$ there is a tree $T_{f\oplus g}$ such that $f \oplus g \in S$ iff $T_{f\oplus G}$ is not well founded. We decompose $T_{f\oplus g}$ into a countable increasing union of finite trees, $T_{f\oplus g} = \cup_n T^*_{f[n],g[n]}$, where

$$T^*_{f[n],g[n]} = \{\sigma \in \mathrm{Seq} \mid |\sigma| < n \wedge \#(\sigma) < n \wedge \Theta(f[n], g[n], \sigma, |\sigma|\}$$

We define an auxiliary game $G'(S)$. In this game I and II alternate playing elements of $f \oplus g$, but II also plays at each stage a $t_n : T^*_{f[n],g[n]} \to \mathrm{Ord}$. Each $t(n)$ is order-preserving: $\sigma \leq KB\tau$ iff $f(\sigma) < f(\tau)$. For each n, $t(n + 1)$ must extends $t(n)$. Player II wins if the function $t = \cup t(n)$ is an order-preservig map from $T_{f\oplus g}$ to the ordinals.

It can be seen that $G'(S)$ is an open game for player I, so $G'(S)$ is determined. Now a winning strategy for II in $G'(S)$ gives a winning strategy for II in G_S; player II can just play the functions t_n in secret.

It remains to show that a winning strategy for I in $G'(S)$ yields a winning strategy for I in G_S. The difficulty is that the winning strategy for I in $G'(S)$ requires a map of the form $t(n)$ in order to predict the next move, but II does not give these functions when playing G_S. So I must guess a suitable map. We omit the proof that if I chooses the maps $t(n)$ so that their ranges are contained in a set of indiscernibles then the strategy for I in $G'(S)$ gives a winning strategy in G_S. $\square$

Remark 6.6.2. The above proof can be refined to show that $\boldsymbol{\Sigma}^1_1$ determinacy is a consequence of the assumption that sharps exist, i.e., $\forall f \, \exists f^\#$. Harrington has proved that $\boldsymbol{\Sigma}^1_1$ determinacy is in fact equivalent to $\forall f \, \exists f^\#$. Moreover, Σ^1_1 determinacy is equivalent to the existence of $0^\#$. Below we prove the weaker result that Σ^1_1 determinacy fails in all forcing extensions of L. Compare Section 5.10. See also Simpson [16].

6.7 Hyperarithmetic theory

Before proving that Σ^1_1 determinacy fails in every forcing extension of L, we briefly cover some basic aspects of hyperarithmetic theory. Roughly speaking, hyperarithmetic theory is a generalization of recursion theory obtained by replacing the recursive sets with the Δ^1_1 sets.

Definition 6.7.1. The *code* of $E \subseteq \omega \times \omega$ is the characteristic function of $\{2^m 3^n \mid mEn\}$. For $f \in \omega^\omega$ we define

$$\mathcal{O}^f = \{e \in \omega \mid \{e\}^f \text{ is the code of a well ordering of } \omega\}.$$

For each $e \in \mathcal{O}^f$, let $|e|^f$ be the order type of the well ordering encoded by $\{e\}^f$. Let $\omega_1^f = \sup\{|e|^f \mid e \in \mathcal{O}\}$. Thus ω_1^f is the least ordinal not recursive in f.

We are already familiar with iterating the Turing jump operator finitely many times as $\mathbf{a}$, $\mathbf{a}'$, $\mathbf{a}''$, ..., $\mathbf{a}^{(n)}$, ... It is also possible to iterate the Turing jump operator transfinitely through the ordinals. For details, see for instance Simpson [17].

Definition 6.7.2. For $e \in \mathcal{O}^f$ we define H_e^f to be the result of iterating the Turing jump operator along the well ordering encoded by $\{e\}^f$ starting with f. At limit stages we take the recursive join. A theorem of Spector asserts that the Turing degree of H_e^f depends only on the ordinal $|e|^f$ and the Turing degree of f. Namely, if $e_1 \in \mathcal{O}^{f_1}$, $e_2 \in \mathcal{O}^{f_2}$, $|e_1|^{f_1} = |e_2|^{f_2}$, $f_1 \equiv_T f_2$, then $H_{e_1}^{f_1} \equiv_T H_{e_2}^{f_2}$. Thus we may define the αth Turing jump of a Turing degree $\mathbf{a}$ as $\mathbf{a}^{(\alpha)} = \deg_T(H_e^f)$, where $\deg_T(f) = \mathbf{a}$ and $|e|^f = \alpha$.

Definition 6.7.3. A function $f \in \omega^\omega$ is *hyperarithmetical in* g if $f \leq_T H_e^g$ for some $e \in \mathcal{O}^g$. We abbreviate this as $f \leq_{\mathrm{HYP}} g$.

The following theorem of Kleene describes the relationship between relative hyperarithmeticity and the projective hierarchy.

Theorem 6.7.4 (Kleene). $f \leq_{\mathrm{HYP}} g \iff f \in \Delta_1^{1,g}$.

If we take g to be recursive, then we have the following result.

Corollary 6.7.5. Each $f \in \omega^\omega$ is hyperarithmetical if and only if $f \in \Delta_1^1$

Remark 6.7.6. The relation $\leq_{\mathrm{HYP}}$ is reflexive and transitive; that is $f \leq_{\mathrm{HYP}} f$ and if $f \leq_{\mathrm{HYP}} g$ and $g \leq_{\mathrm{HYP}} h$, then $f \leq_{\mathrm{HYP}} h$.

As in the case of Turing equivalence and Turing degrees, we use $\leq_{\mathrm{HYP}}$ to define an equivalence relation and a corresponding degree notion.

Definition 6.7.7. $f \equiv_{\mathrm{HYP}} g$ if and only if $f \leq_{\mathrm{HYP}} g$ and $g \leq_{\mathrm{HYP}} f$. The equivalence classes of $\equiv_{\mathrm{HYP}}$ are called *hyperdegrees*.

Before defining the hyperarithmetical analog of the Turing jump operator, we note the following lemma.

Lemma 6.7.8. $\mathcal{O}^f$ is a complete $\Pi_1^{1,f}$. That is, for all $A \subseteq \omega$, $A \in \Pi_1^{1,f} \iff A \leq_m \mathcal{O}^f$.

Proof. The proof uses the Kleene Normal Form Theorem, plus the Kleene/Brouwer ordering. We omit the details, but see Rogers [11]. □

This justifies the following definition.

Definition 6.7.9 (hyperjump). The *hyperjump* of g is $\mathcal{O}^g$.

Just as the Turing jump is an operator sending each Turing degrees to a higher Turing degree, the hyperjump is an operator sending each hyperdegree to a higher hyperdegree.

Lemma 6.7.10. $\mathcal{O}^g$ is a complete $\Pi_1^{1,g}$ set. I.e., for all $A \subseteq \omega$, $A \in \Pi_1^{1,g} \iff A \leq_m \mathcal{O}^g$.

Therefore, g is hyperarithmetical in $\mathcal{O}^g$, and so $g <_{\mathrm{HYP}} \mathcal{O}^g$. We also have $g \leq_{\mathrm{HYP}} h \Rightarrow \mathcal{O}^g \leq_{\mathrm{HYP}} \mathcal{O}^h$; in fact, $g \leq_{\mathrm{HYP}} h \iff \mathcal{O}^g \leq_m \mathcal{O}^h$. These properties are similar to the properties of the Turing jump.

Lemma 6.7.11. The relation $\{(f,g) \mid f \leq_{\mathrm{HYP}} g\}$ is Π_1^1.

Proof. $f \leq_{\mathrm{HYP}} g \iff \exists e\ (e \in \mathcal{O}^g$ and $\forall x\ x = H_e^g \Rightarrow f \leq_T x)$. The quantifier $\exists e\ e \in \mathcal{O}^g$ is Π_1^1 while the statement $\forall x\ x = H_e^g \Rightarrow f \leq_T x$ is arithmetical: recall that the Turing jumps and Turing degree were arithmetically definable. Therefore the entire sentence is Π_1^1. □

Lemma 6.7.12. Suppose $f \leq_{\mathrm{HYP}} g$. Then $\mathcal{O}^f \leq_{\mathrm{HYP}} g \iff w_1^f < \omega_1^g$.

Proof. Suppose $\mathcal{O}^f \leq_{\mathrm{HYP}} g$. Then $\Sigma_{e \in \mathcal{O}\{}$ is a well-ordering of ω with order type $\alpha \leq_{\mathrm{HYP}}$. Then $\alpha < with\omega_1^g$ and so $\omega_1^f < \omega_g^1$ as required.

Conversely, let $\omega_1^f \leq \omega_1^g$. Then ω_1^f is the order type of (ω, R) for some well-ordering R. So $\mathcal{O}^f = \{e \mid \{e\}^f$ is a well-ordering of $\omega\} = \{e \mid \exists f\ f : \{e\}^f \to^{o.p} (\omega, R)\}$. This is a $\Sigma_1^{1,f}$ sentence and therefore $\Sigma_1^{1,f}$ and since $f \leq_{\mathrm{HYP}} g$, $\mathcal{O}^f$ is then $\Sigma_1^{1,g}$. Since $\mathcal{O}^f$ is $\Pi_1^{1,f}$ (and so $\Pi_1^{1,g}$), $\mathcal{O}^f$ is $\Delta_1^{1,g}$, and so by a previous theorem, $\mathcal{O}^f \leq_{\mathrm{HYP}} g$, as required. □

Remark 6.7.13. The previous lemma implies that the hyperdegrees have a nicer structure and are better behaved than the Turing degrees. For example, it is known that there exists an infinite descending sequence of Turing degrees separated by Turing jumps, i.e. $\mathbf{a}'_{n+1} < \mathbf{a}_n$ for all $n < \omega$. This cannot happen in the hyperdegrees, because it would imply the existence of an infinite descending sequence of ordinals.

Surprisingly, the ordinals hyperarithmetic in g are precisely the ordinals computable in g.

Lemma 6.7.14. For $g \in \omega^\omega$, $\omega_g^1 = \sup\{\alpha \mid \alpha \leq_T g\} = \sup\{\alpha \mid \alpha \leq_{\mathrm{HYP}} g\}$.

Proof. Suppose (ω, R) is a well-ordering of ω with R being $\Sigma_1^{1,g}$. The order type of (ω, R) is an ordinal α with $\alpha < \omega_1^g$. If not, then we have

$$\begin{aligned} \mathcal{O}^g &= \{e \mid \{e\}^g \text{ is a code for a well-ordering of } \omega\} \\ &= \{e \mid \exists f\ f \text{ is an order-preserving map from } \{e\}^g \to (\omega, R)\} \end{aligned}$$

Therefore $\mathcal{O}^g$ is $\Sigma_1^{1,g}$, contradicting $g <_{\mathrm{HYP}} \mathcal{O}^g$. □

Lemma 6.7.15 (Kleene Basis Theorem). Let $S \subseteq \omega^\omega$ be $\Sigma_1^{1,g}$. If $S \neq \emptyset$ then there exists $f \in S$ such that $f \leq_T \mathcal{O}^g$.

Proof. Use the Kleene normal form to write $S = \{f \mid \exists h \forall n\ R(f[n], g[n], h[n])\}$, where R is recursive. We write $(\omega \times \omega)^{<\omega}$ for $\bigcup \omega^n \times \omega^n$. Define a tree T_S:

$$T_S = \{(\sigma, \tau) \in (\omega \times \omega)^{<\omega} \ \mid \forall n \leq \mathrm{lh}(\sigma) = \mathrm{lh}(\tau) R(\sigma[n], g[n], \tau[n])\}$$

Then S is nonempty iff T is not well-founded. Define $\hat{T}$ to be the tree of all finite subsequences of $[T]$. So $(\sigma, \tau) \in \hat{T}$ iff there is a path through T starting with (σ, τ). Note that $\hat{T}$ is a pruning of T such that $\hat{T}$ is tidy; every node in $\hat{T}$ has an infinite path through it. Also, $[\hat{T}] = [T]$. The statement that $\hat{T}$ is not well-founded is $\Sigma_1^{1,g}$, so $T \leq_T \mathcal{O}^g$. As $\hat{T}$ is tidy, there is a recursive path through $\hat{T}$; namely, the left-most. That path through $\hat{T}$ is recursive in $\mathcal{O}^g$. Since a path through $\hat{T}$ is a path through T, there is then an $f \in S$ with $f \leq \mathcal{O}^g$. □

Theorem 6.7.16. If S is $\Sigma_1^{1,g}$ and $S \neq \emptyset$, then there exists $f \in S$ such that $f \leq \mathcal{O}^g$ and $\omega_1^f \leq \omega_1^g$.

Proof. Define $S' = \{f_1 \otimes f_2 \mid f_1 \in S \wedge f_2 \leq_{\mathrm{HYP}} f_1 \oplus g\}$. Since the statement $f_1 \in S$ is $\Sigma_1^{1,g}$ and the statement $f_2 \leq_{\mathrm{HYP}} f_1 \oplus g$ is $\Sigma_1^{1,g}$, S' is $\Sigma_1^{1,g}$. Note that S' is non-empty: if f_2 is the hyperjump of $f_1 \oplus g$, then $f_1 \oplus f_2$ is in S'.

By the Kleene Basis Theorem, there exists $f_1 \oplus f_2 \in S'$ such that $f_1 \oplus f_2 \leq \mathcal{O}^g$. Note that $f_1 \in S$, $f_1 \leq \mathcal{O}^g$, and $g \leq_T f_1 \oplus g <_{\mathrm{HYP}} f_1 \oplus f_2 \oplus g \leq_T \mathcal{O}^g$. Therefore $\omega_1^{f_1 \oplus g} \leq \omega_1^g$ (otherwise, $\mathcal{O}^g$ is hyperarithmetical in f). Thus, $\omega_1^f \leq \omega_1^g$. □

Corollary 6.7.17. If S is $\Sigma_1^{1,g}$ and nonempty, then there exists $f \in S$ with $\omega_1^f \leq \omega_1^g$.

Corollary 6.7.18. For all g there exists f such that $g <_{\mathrm{HYP}} f <_{\mathrm{HYP}} \mathcal{O}^g$.

Proof. Define $S = \{f \oplus g \mid f \not\leq_{\mathrm{HYP}} g\}$. Then as S is $\Sigma_1^{1,g}$ and non-empty, we can find an $f \oplus g \in S$ such that $f \oplus g \leq_T \mathcal{O}^g$ and $\omega_1^{f \oplus g} \leq \omega_1^g$. Therefore $g <_{\mathrm{HYP}} f \oplus g \oplus \mathcal{O}^g$. □

Remark 6.7.19. As the previous results imply, many results that are true in the Turing degrees relativize to the hyperdegrees. The hyperjump is analogous to the Turing jump, the hyperdegrees are analogous to the Turing degrees, and so on. For example, it is possible to use Sacks forcing to construct a minimal hyperdegree.

6.8 Admissible sets

The study of admissible sets links set theory with hyperarithmetic theory. We define Kripke-Platek set theory, a fragment of ZF, and explore some properties of its models.

Definition 6.8.1. Kripke-Platek set theory (KP) is a first-order theory in the language $L = \{=, \in\}$. This fragment contains the axioms of extensionality, pairing, union, infinity (in the form which says that ω exists), and empty set from ZF. In addition, KP contains the following axiom schemes:

1. Δ_0-comprehension, which contains the universal closure of each formula of the form
$$\exists y \forall z[z \in y \iff z \in x \wedge \phi(z)]$$
where ϕ is a Δ_0 formula which does not mention y.

2. Δ_0-bounding, which contains the universal closure of each formula of the form
$$[\forall z \in y \exists v \phi(v, z)] \Rightarrow \exists u \forall z \in y \exists v \in u \phi(v, z)$$

3. The foundation scheme, which contains the universal closure of each formula of the form
$$[\exists z \phi(z)] \Rightarrow \exists z[\phi(z) \wedge \neg \exists y \in z \phi(y)]$$
where ϕ is an arbitrary L-formula.

Definition 6.8.2. Let (A, R) be a relational structure. We define the *well-founded part* (A_0, R_0) of (A, R). Let
$$A_0 = \{a \in A \mid \text{no infinite strictly } R\text{-decreasing sequence begins with } a\}$$
and let $R_0 = R \cap A_0 \times A_0$.

The well-founded part of a model of KP behaves nicely, as we shall see. First, we show that Δ_0 formulas are absolute to the well-founded part of a model.

Lemma 6.8.3. Let (A, R) be a relational structure and let (A_0, R_0) be its well-founded part. Take any Δ_0 formula $\phi(x_0, \ldots, x_k)$ with the free variables shown. For any $a_0, \ldots, a_k \in A_0$,
$$(A, R) \models \phi(a_0, \ldots, a_k) \iff (A_0, R_0) \models \phi(a_0, \ldots, a_k).$$

Proof. The proof follows immediately from the fact that the quantifiers in a Δ_0 formula are bounded and R_0 is a restriction of R. $\square$

Theorem 6.8.4. Let (A, R) be a model of KP, and let (A_0, R_0) be the well-founded part. Then (A_0, R_0) is a model of KP.

Proof. It is straightforward to show that (A_0, R_0) satisfies the axioms of extensionality, pairing, unions, empty set, and infinity, and that (A_0, R_0) satisfies the foundation scheme. If $a, b \in (A, R)$ with $a \subset b$ and $b \in A_0$, then $a \in A_0$. This implies that (A_0, R_0) is closed under Δ_0-comprehension.

It remains to show that (A_0, R_0) satisfies Δ_0 bounding. Suppose that there is a $y \in A_0$ such that
$$(A_0, R_0) \models \forall z \in y \exists v \phi(v, z)$$
for a Δ_1 formula ϕ. We need to show that there is a $u \in A_0$ such that $(A_0, R_0) \models \forall z \in y \exists v \in u \phi(v, z)$. From outside A_0, we see that there is an ordinal $\beta \in A$ such that
$$\forall z \in y \exists v \in A_0[\text{rank}(v) < \beta \wedge \phi(v, z)$$

Hence there is some $u \in A$ of rank less than β such that

$$(A, R) \models \forall z \in y \exists v \in u \phi(v, z). \tag{6.1}$$

Because the formula in (6.1) is absolute, it holds in (A_0, R_0). $\square$

Definition 6.8.5. A set A is *admissible* if $(A, \in \restriction A)$ is a model of KP. An ordinal α is admissible if L_α is a model of KP. If M is an admissible set, we let $\mathrm{height}(M) = \mathrm{Ord} \cap M$; so $\mathrm{height}(M)$ is the limit of the ordinals contained in M.

Remark 6.8.6. Let M be admissible and let $\alpha = \mathrm{height}(M)$. Then L_α is contained in the well-founded part of M, so α is admissible.

Remark 6.8.7. We can use the method of forcing to extend models of KP, because this theory proves the basic forcing lemmas. In proving these theorems, because models of KP are not closed under relative definability, we must change the notion of dense set slightly. For M a countable admissible set and P a partial order in M, we say that a filter G on P is M-generic if G meets every dense subset of P which is *definable* over M. In this case, $M[G]$ will be a model of KP of the same height as M.

One sharp result which can be obtained: if $\phi(x_0, \ldots, x_k)$ is a Δ_0 formula with the free variables shown, then the set of tuples $\langle p, a_0, \ldots, a_k \rangle$ such that $p \in P$ and $p \Vdash \phi(a_0, \ldots, a_k)$ is definable in M.

Remark 6.8.8. For each $g \in \omega^\omega$, $L_{\omega_1^g}$ is an admissible set of height ω_1^g. In fact, $L_{\omega_1^g}(g)$ is the smallest admissible set containing g. This implies that $L_{\omega_1^{CK}}$ is the smallest admissible set. Moreover, $f \leq_{\mathrm{HYP}} g$ iff $f \in L_{\omega_1^g}(g)$.

Remark 6.8.9. Let M be an admissible set and (A, R) a well ordering in M. Then there is an ordinal $\alpha \in M \cap \mathrm{Ord}$ such that α is the order type of (A, R). However, KP does not prove that for every well ordering (A, R) there is an ordinal which is the order type of (A, R). This is because of the existence of *pseudo well orderings*, linear orderings which have no hyperarithmetic descending sequences but are not well orderings.

6.9 Admissibility and cardinal collapsing

In this section, we will show that Σ^1_1 determinacy fails in all forcing extensions of L. We will use the method of forcing over admissible sets to obtain this result.

We next introduce, by way of example, the concept of a semigeneric collapse. Let β be an uncountable ordinal, and let α be the first admissible ordinal greater than β. Let P be the notion of forcing which collapses β to ω, and let G be a $L_{\alpha+1}$-generic filter on P (the requirement that G be $L_{\alpha+1}$-generic is exactly the requirement that G meets every dense set definable over L_α). As usual, we let $g = \cup G$ be the generic surjection $\omega \to \beta$. Define $X = \{2^m 3^n \mid g(m) < g(n)\}$. The set X is a semigeneric collapse, and every semigeneric collapse is of this form..

Definition 6.9.1. A set $X \subset \omega$ is a *semigeneric collapse* if X is a code for a well ordering of ω of order type β obtained from an $L_{\alpha+1}$-generic collapse of β, where α is the least admissible ordinal larger than β.

It can be seen that the set $\{X \mid X \text{ is a semigeneric collapse}\}$ is Δ^1_2. If X is a semigeneric collapse of β and α is the least admissible greater than β, then $\omega_1^X = \alpha$. In fact, every admissible ordinal is obtained this way:

Theorem 6.9.2 (Sacks). Every admissible ordinal α is of the form ω_1^X for some semigeneric collapse X.

We next prove a lemma which will be important for following results. The lemma says that in forcing extensions of L, there are semigeneric collapses of arbitrarily high hyperdegree.

Lemma 6.9.3. Let $f \in \omega^\omega$ be an element of a forcing extension $L[G]$. Then $f \leq_{\text{HYP}} X$ for a semigeneric collapse X.

Proof. FIXME $\square$

Definition 6.9.4. We define two axioms of determinacy for projective sets:

- Σ^1_n *Projective Determinacy* (Σ^1_n-PD) is the axiom which states that every Σ^1_1 set is determined.
- Σ^1_n *Projective Turing Degree Determinacy* (Σ^1_n-PTD) is the statement that for every Σ^1_1 set S closed under Turing equivalence there is a cone of Turing degrees C such that $C \subseteq S$ or $C \cap S = \emptyset$.

Projective determinacy (PD) is Σ^1_1-PD; projective Turing degree determinacy (PTD) is Σ^1_n-PTD. The boldface versions of these concepts are defined analogously.

Lemma 6.9.5. The following statements hold:

1. PD $\Rightarrow$ PTD
2. For each $n \in \omega$, Σ^1_n-PD $\Rightarrow \Sigma^1_n-$PTD.
3. For each $n \in \omega$, $\boldsymbol{\Sigma}^1_n-$PD $\Rightarrow \boldsymbol{\Sigma}^1_n-$PTD.

Our next goal is to prove that Σ^1_1-PD is not consistent with $V = L$.

Theorem 6.9.6. Projective Turing degree determinacy implies that V is not a forcing extension of L.

We delay the proof of this theorem until later.

Remark 6.9.7. Although it may appear that Σ^1_1-PD is stronger than Σ^1_1-PTD, Harrington has shown the equivalence

$$\Sigma^1_n - \text{PD} \iff \Sigma^1_n - \text{PTD} \iff 0^\# \text{ exists.}$$

The boldface version of this result also holds:

$$\mathbf{\Sigma}^1_n - \text{PD} \iff \mathbf{\Sigma}^1_n - \text{PTD} \iff \forall f\,[f^{\#} \text{ exists}].$$

We will not prove Harrington's theorem.

Towards a proof of Theorem 6.9.6, we define a crucial set $\mathcal{C} \subset \omega^\omega$:

$$\begin{aligned}\mathcal{C} = \{f \in \omega^\omega \mid \quad & \exists E \subset \omega^\omega [E \leq_T f \wedge (\omega, E) \models \mathsf{KP} \\ & \wedge \omega_1^f \text{ is isomorphic to an initial segment of } (\omega, E)\}.\end{aligned}$$

Proposition 6.9.8. The set $\mathcal{C}$ is Σ^1_1 and closed under Turing equivalence.

Lemma 6.9.9. For each $g \in \omega^\omega$ there is some $f \in \omega^\omega$ such that $f \geq_T g$ and $f \in \mathcal{C}$.

Proof. Let $g \in \omega^\omega$ be given. Consider the set S^g given by

$$\begin{aligned}S^g = \{E \in \omega^\omega \mid \quad & (\omega, E) \models \mathsf{KP} \\ & \wedge \omega_1^g \text{ is isomorphic to an initial segment of } (\omega, E)\}\end{aligned}$$

It is straightforward to show that S^g is Σ^1_1. To see that S^g is nonempty, let E be a code for the admissible set $L_{\omega_1^g}(g)$. We apply the Low Basis Theorem to find $E \in S^g$ such that $\omega_1^{X \oplus g} = \omega_1^g$. The set $g \oplus E$ satisfies the conclusion of the lemma. $\square$

Proof of Theorem 6.9.6. Let Θ be the sentence

$$\Theta \equiv \forall f \exists X [X \text{ is a semigeneric collape} \wedge f \leq_{\text{HYP}} X].$$

Recall that Lemma 6.9.3 says that $V = L \Rightarrow \Theta$. We will show that $\Sigma^1_1 - \text{PD} \Rightarrow \neg\,\Theta$.

We assume PTD, which along with Lemma 6.9.9 implies that $\mathcal{C}$ contains a cone of Turing degrees. Let f_0 be the base of this cone. We will show that $f_0 \notin L[G]$.

Suppose that $f_0 \in L_{\omega_1^X}[X]$, where X is a semigeneric collapse. Let $\alpha = \omega_1^X$, and let β be the order type of X. So $\alpha > \beta$ and X codes an $L_{\alpha+1}$-generic filter G of the collapse of β to ω.

We note that $L_{\omega_1^X}[X] = L_\alpha[X] = L_\alpha[G]$.

If $f_0 \in L_\alpha[G]$, then there is an $E \leq_T f_0$ such that $E \models \mathsf{KP}$ and α is isomorphic to an initial segment of (ω, E).

This implies that L_α is a subset of the collapse of the well founded part of (ω, E). Let π be the canonical collapsing map. Choose γ such that $\beta < \gamma < \alpha$ and $L_\gamma[X]$ contains G, $\pi^{-1}{\restriction}P$, $\pi^{-1}(\omega)$ and E.

Let h be hyperarithmetic in X but not in $L_{\gamma+1}[X]$, and let $t = \{\langle p, m, n\rangle \mid p \Vdash \dot{h}(m) = n\}$. Then $h(m) = n \iff \exists p \in G[(\omega, E) \models \pi^{-1}(\langle p, n, m\rangle) \in \pi^{-1}(t)$. So $h \in L_{\gamma+1}$, a contradiction. $\square$

Bibliography

[1] Tomek Bartoszynski and Haim Judah, *Set Theory: On the Structure of the Real Line*, A. K. Peters, 1995, IX + 546 pages.

[2] J. Barwise, H. J. Keisler, and K. Kunen (eds.), *The Kleene Symposium*, Studies in Logic and the Foundations of Mathematics, North-Holland, 1980, XX + 425 pages.

[3] Ulrich Felgner, *Models of ZF-Set Theory*, Lecture Notes in Mathematics, no. 223, Springer-Verlag, 1971, VI + 173 pages.

[4] Leo Harrington, *McLaughlin's conjecture*, 11 pages, unpublished, November 1976.

[5] Thomas Jech, *Set Theory*, Academic Press, 1978, XI + 621 pages.

[6] Thomas J. Jech, *The Axiom of Choice*, Studies in Logic and the Foundations of Mathematics, North-Holland, 1973, XI + 202 pages.

[7] Alexander S. Kechris, *Classical Descriptive Set Theory*, Graduate Texts in Mathematics, Springer-Verlag, 1985, XVIII + 402 pages.

[8] Donald A. Martin, *A purely inductive proof of Borel determinacy*, [9], 1985, pp. 303–308.

[9] A. Nerode and R. A. Shore (eds.), *Recursion Theory*, Proceedings of Symposia in Pure Mathematics, American Mathematical Society, 1985, VII + 528 pages.

[10] Michael O. Rabin, *Computable algebra, general theory and theory of computable fields*, Transactions of the American Mathematical Society **95** (1960), 341–360.

[11] Hartley Rogers, Jr., *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, 1967, XIX + 482 pages.

[12] Joseph J. Rotman, *The Theory of Groups*, second ed., Allyn and Bacon, 1973, X + 342 pages.

[13] Gerald E. Sacks, *Forcing with perfect closed sets*, [14], 1971, pp. 331–355.

[14] D. S. Scott (ed.), *Axiomatic Set Theory, Part 1*, Proceedings of Symposia in Pure Mathematics, vol. 13, American Mathematical Society, 1971, VI + 474 pages.

[15] Joseph R. Shoenfield, *Unramified forcing*, [14], 1971, pp. 357–381.

[16] Stephen G. Simpson, *Minimal covers and hyperdegrees*, Transactions of the American Mathematical Society **209** (1975), 45–64.

[17] ———, *The hierarchy based on the jump operator*, [2], 1980, pp. 203–212.

[18] ———, *Foundations of Mathematics*, Unpublished lecture notes, Department of Mathematics, Pennsylvania State University, 86 pages, 1995–2004.

[19] Hisao Tanaka, *A property of arithmetic sets*, Proceedings of the American Mathematical Society **31** (1972), 521–524.

[20] B. L. van der Waerden, *Modern Algebra*, revised English ed., Ungar, New York, 1953, Volume I, XII + 264 pages, Volume II, IX + 222 pages.