Differences of computably enumerable sets

Steffen Lempp*
Department of Mathematics
University of Wisconsin-Madison
Madison, WI 53706-1388
USA
lempp@math.wisc.edu

André Nies†
Department of Mathematics
University of Chicago
5734 University Avenue
Chicago, IL 60637-1514
USA
nies@math.uchicago.edu

February 23, 2000

Abstract

We consider the lower semilattice $\mathcal{D}$ of differences of c.e. sets under inclusion. It is shown that $\mathcal{D}$ is not distributive as a semilattice, and that the c.e. sets form a definable subclass.

1 Introduction

A persistent open problem about the lattice $\mathcal{E}$ of computably enumerable (c.e.) sets under inclusion is to determine the least number k such that the Σ_k-theory is undecidable. Lachlan [6] proved that the Σ_2–theory in

*Partially supported by NSF-grant DMS–9504474.
†Partially supported by NSF-grant DMS–9500983.
0 AMS Subject Classification 03D25
0 d. c. e. set, difference, lattices

the language of lattices is decidable, while one of the various known proofs of undecidability for $\mathrm{Th}(\mathcal{E})$, in that case due to Harrington, shows that in fact the Σ_8–theory in the language of lattices is undecidable (see [10], p. 381 for a sketch of that proof). Thus a very unsatisfying gap of 6 quantifier alternations remains. The reason why the undecidability proofs are so "bad" is that the coding used is very indirect. For instance, first one codes the class of finite symmetric graphs (which has an hereditarily undecidable Σ_2–theory) in the class of recursive Boolean pairs ([1]), and in a second step, the latter class is coded in $\mathcal{E}$ (see [8] for details about how to prove undecidability of fragments of theories). Each step involves quite a complex coding, which yields an increase of three quantifier alternations.

Since $\mathcal{E}$ seems to be very well behaved for properties definable with few quantifier alternations, it is not at all clear how to obtain a better coding. Ideally, one would want to have a coding of a sufficiently complex class, like the class of finite symmetric graphs, using only Σ_1–formulas with parameters. By the methods developed in [8], this would give the undecidability of the Σ_3–theory. However, such a proof is not possible since it would show that the class of finite distributive lattices with the reduction property has an undecidable theory, contrary to a result of Ershov. The argument is as follows: Suppose that, via some scheme of Σ_1 formulas we can code each finite symmetric graph (V, E), using appropriate parameters $\overline{p}$ (see [8] for definitions). Let L be a finite distributive sublattice of $\mathcal{E}$ which contains $\overline{p}$, all the elements of $\mathcal{E}$ representing the vertices in V and also witnesses for all Σ_1–formulas involved to code (V, E). Then L, and in fact any distributive lattice H such that $L \subseteq H \subseteq \mathcal{E}$ codes (V, E) via the same scheme and parameters. Now let H be such a lattice which is also finite and satisfies the reduction property. In this way, we have obtained a uniform coding of a complex class in the class of finite distributive lattices with the reduction property. We conclude that the best we can hope for to obtain by the standard coding methods is undecidability of the Σ_4–theory, which still would require a far more direct coding than the ones presently known.

Here we propose a new view of $\mathcal{E}$, which may eventually lead to such a more direct coding. We consider the structure $\mathcal{D}$ of differences of c.e. sets under inclusion. This structure coincides with the second level of Ershov's difference hierarchy. $\mathcal{D}$ is closed under intersections, since

$$(A_1 - B_1) \cap (A_2 - B_2) = (A_1 \cap A_2) - (B_1 \cup B_2). \tag{1.1}$$

$\mathcal{D}^*$ will denote the structure $\mathcal{D}$ modulo finite differences. For notational reasons, we formulate most of our results in the setting of $\mathcal{D}^*$, not $\mathcal{D}$. We first collect some simple facts about $\mathcal{D}$ and $\mathcal{D}^*$. The first one shows that any undecidability proof for a low–level fragment of $\mathrm{Th}(\mathcal{D})$ would yield the same result for $\mathcal{E}$, which justifies the program suggested above.

Proposition 1.1 *The lower semilattice $\mathcal{D}$ can be interpreted in the lattice $\mathcal{E}$, using only quantifier free formulas without parameters. The same holds for $\mathcal{D}^*$ and $\mathcal{E}^*$.*

Proof. We ambiguously represent the element $A-B$ of $\mathcal{D}$ by the pair of c.e. sets (A, B). Then (1.1) gives a formulas to define the infimum (and hence inclusion) in terms of pairs as desired. The same formula works for $\mathcal{D}^*$. An explicit way to define inclusion is

$$A_1 - B_1 \subseteq A_2 - B_2 \Leftrightarrow (A_1 \subseteq A_2 \cup B_1 \ \wedge \ A_1 \cap B_2 \subseteq B_1).$$

$\diamondsuit$

Conventions. We use the notational convention that, if a set X in $\mathcal{D}$ is given, the corresponding lower case letter x denotes the element X^* of $\mathcal{D}^*$. Conversely, if $y \in \mathcal{D}^*$ is given, then Y denotes an element of $\mathcal{D}$ such that $Y^* = y$. We denote $\emptyset^*, \omega^*$ by $0, 1$ respectively. If $X = A - B$, A, B c.e. then we assume that A, B are equipped with enumerations such that $\forall s[B_s \subseteq A_{s+1}]$. We say that an element m *enters* X when m is enumerated into A, and *leaves* X when, later, m is enumerated into B. The elements of $\mathcal{D}$ are called difference c.e. (d.c.e.) sets. Letters A, B, C, D always denote c.e. sets. A *split* of a c.e. set A is a c.e. set $B \subseteq A$ such that $A - B$ is c.e.

Proposition 1.2 *$\mathcal{D}^*$ is not a lattice.*

Proof. We construct $D_0, D_1 \in \mathcal{D}$ such that $\sup(d_0, d_1)$ fails to exist. If $x = \sup(d_0, d_1)$ then w.l.o.g. we can assume that $D_0, D_1 \subseteq X$. So it is enough to build for each X a "counterexample" $D_X \supseteq D_0, D_1$ such that the following requirements are met:

$$P_n^X : X \supseteq D_0, D_1 \Rightarrow |X - D_X| \geq n.$$

For in that case, $d_x \not\geq x$, so not $x = \sup(d_0, d_1)$. The strategy for P_n^X is as follows: if P_{n-1}^X is met, i.e. if already $|X - D_X| \geq n - 1$, enumerate a new candidate m for P_n^X into D_0. If m does not appear in X, we win P. If m appears in X then we extract m from D_0, so if m stays in X, we win because we have increased $|X - D_X|$ by one. If, however, m leaves X later, then we enumerate m into D_1. So $m \in D_1 - X$, so we win again. Combining the strategies is routine. (A less elementary proof using major subsets also works here.) $\diamondsuit$

Proposition 1.3 *If $A - B$ is coinfinite, then there is a coinfinite c.e. C such that $A - B \subseteq C$.*

Proof. If A is coinfinite, let $C = A$. Else $\overline{B}$ is coinfinite, so pick an infinite computable $R \subseteq B$ and let $C = \overline{R}$. $\diamondsuit$

We next consider lattice embeddings. The property that a finite lattice L can be embedded (preserving meets and joins) into $\mathcal{D}^*$ is a Σ_2 property of $\mathcal{D}^*$ in the language of partial order, and hence, by proposition 1.1, a Σ_2 property of $\mathcal{E}^*$ in the language of lattices. So the question whether this property holds can in principle be answered by invoking Lachlan's decision procedure for the Σ_2–theory of $\mathcal{E}^*$ [6]. However, due to the technical complexity of Lachlan's procedure it is often easier to give a direct proof. In this way we establish the following result, which shows that $\mathcal{D}^*$ is not distributive as a lower semilattice (see [9]). This supports our expectation that coding in $\mathcal{D}^*$ on a low quantifier level may turn out to be less restricted than coding in $\mathcal{E}^*$.

Proposition 1.4 (Implicit in [6]) *The five-element nonmodular lattice, N_5, can be embedded into $\mathcal{D}^*$, preserving meet, join and least element.*

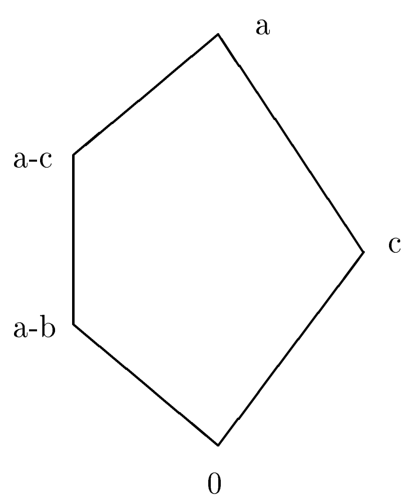

Figure 1: An embedding of N_5

Sketch of a proof. We build c.e. sets A, B, C such that $\emptyset \subset_\infty C \subset_\infty B \subset_\infty A$, and $\sup(a - b, c) = a$. Then an embedding of N_5 is obtained as shown in

Figure 1. Along with making $C, A - B$ and $B - C$ infinite, we meet the supremum requirements

$$N_V : A - B, C \subseteq V \Rightarrow A \subseteq^* V.$$

The main problem is to make $B - C$ infinite, i.e. to meet for each k the requirement $P_k : |B - C| \geq k$. We outline a strategy to put a new element x into $B - C$ in the context of a higher priority N_V requirement. First, we enumerate x into A. Then x must appear in V, else we win N_V in a finitary way (and P_k starts with a new x, but can now disregard N_V). Now we put x into B. Then we have succeeded (x is in $B - C$), unless x leaves V, threatening to make us loose N_V. But in this case, we enumerate x into C and, again, we win N_V in a finitary way. ♢

Also by a direct proof, we obtained the opposite result for M_5.

Proposition 1.5 (Implicit in [6]) *The five element modular nondistributive lattice M_5 cannot be embedded into $\mathcal{D}^*$.*

♢

2 The definability of $\mathcal{D}^*$ in $\mathcal{E}^*$

We now analyze cupping properties and complementation in $\mathcal{D}^*$. This leads to our main result that $\mathcal{E}^*$, viewed as a subclass, is definable in $\mathcal{D}^*$ without parameters. Analogous definability results have been obtained by Cooper for the c.e. degrees [2], viewed as a subclass of the Δ^0_2–degrees, and by the second author for $\mathcal{E}^*$, viewed as a subclass of the uppersemilattice of c.e. equivalence relations modulo finite differences [7]. Recall that $A \subset_m B$ iff

$$A \subset_\infty B \text{ and } \forall C\ (B \cup C = \omega \Rightarrow A \cup C =^* \omega).$$

We write $A \subseteq^*_m B$ if $A \subseteq^* B$ and

$$(A \subset_m B \cup A \text{ or } B - A \text{ finite}).$$

Note that $A \subseteq^*_m B$ means that B^* has no "cupping partner" above A^*. Thus, $A \subseteq^*_m B \Leftrightarrow$

$$\forall D[B \cup D =^* \omega \ \wedge \ D \subset_\infty \omega \Rightarrow A \not\subseteq^* D],$$

which is equivalent to $\forall D[\overline{D} \subseteq^* B \wedge |\overline{D}| = \infty \Rightarrow A \cap \overline{D} \neq^* \emptyset]$. Therefore, for $A \subset_\infty B$, $A \subset_m B$ iff $B - A$ does not $*$-contain an infinite co-c.e. set (and therefore no infinite c.e. set – compare this to proposition 1.3).

A complement of $x \in \mathcal{D}^*$ is a y such that $x \wedge y = 0, x \vee y = 1$. If A is c.e. then clearly $\overline{a} = \overline{A}^*$ is a complement of a in $\mathcal{D}^*$. We now prove that all complements are of the form $\overline{B}^*$ for B "close to" A.

Lemma 2.1 *Suppose A is c.e. Then the complements of A^* in $\mathcal{D}^*$ are precisely those sets $\overline{B}^*$ s.t. $A \subseteq_m^* B$, B c.e.*

Proof. If B is such, then $A \cap \overline{B} =^* \emptyset$. Moreover, $\sup(A^*, \overline{B}^*) = 1$: else there would be an c.e. w s.t. $A^*, \overline{B}^* \leq w < 1$, whence B^* would have a cupping partner above A^*. Now suppose $(C - D)^*$ is a complement of A^*. Then $A \cup C =^* \omega$, so by the reduction principle,

$$A \cup R =^* \omega \ \wedge \ R \subseteq^* C$$

for some recursive R. Since $A \cap (C - D) =^* \emptyset$, this implies

$$C - D =^* R - D.$$

So $C - D$ is co-c.e. Let $\overline{B} = C - D$, B c.e. Then $A \subseteq_m^* B$. Otherwise there would be a c.e. E s.t. $A \subseteq^* E \subset_\infty \omega$ but $B \cup E =^* \omega$, i.e. $a, \overline{b} \leq e < 1$. $\diamondsuit$

Lemma 2.2 *Suppose $B \subseteq A$ and $D \subseteq C$. Then the following are equivalent:*

(i) $(A - B)^* \vee (C - D)^* = 1$

(ii) $A \cup C =^* \omega \ \wedge \ B \cap D$ *finite* $\wedge \ A \subseteq_m^* A \cup D \ \wedge \ C \subseteq_m^* C \cup B$

Proof (See figure 2). (i) $\rightarrow$ (ii). Clearly $(C - D), (A - B) \subseteq A \cup C$ and $C - D, A - B \subseteq^* \overline{B \cap D}$. So $A \cup C$ and $\overline{B \cap D}$ must be cofinite. Now suppose $A \subseteq E$ and $A \cup D \cup E =^* \omega$. We have to show that E is cofinite. Clearly $\overline{A} \cap \overline{D} \subseteq^* E$ and $A \subseteq E$ implies $\overline{D} \subseteq^* E$. Thus $A - B, C - D \subseteq^* E$. So by (i), E is cofinite. Thus $A \subseteq_m^* A \cup D$. Similarly $C \subseteq_m^* C \cup B$.
(ii) $\rightarrow$ (i). By proposition 1.3, it is enough to show that, if $A - B, C - D \subseteq^* X$, X c.e., then X is cofinite. Clearly $A \subseteq^* X \cup B$. Moreover, since $A \cup C =^* \omega$,

$$\omega =^* (C - D) \cup (D \cup A) \subseteq X \cup (D \cup A).$$

So $A \subseteq_m^* A \cup D$ implies that $X \cup B =^* \omega$. Symmetrically, $X \cup D =^* \omega$ and hence because $B \cap D =^* \emptyset$,

$$X =^* (X \cup B) \cap (X \cup D) =^* \omega.$$

$\diamondsuit$

The following corollary gives an approximation to distributivity.

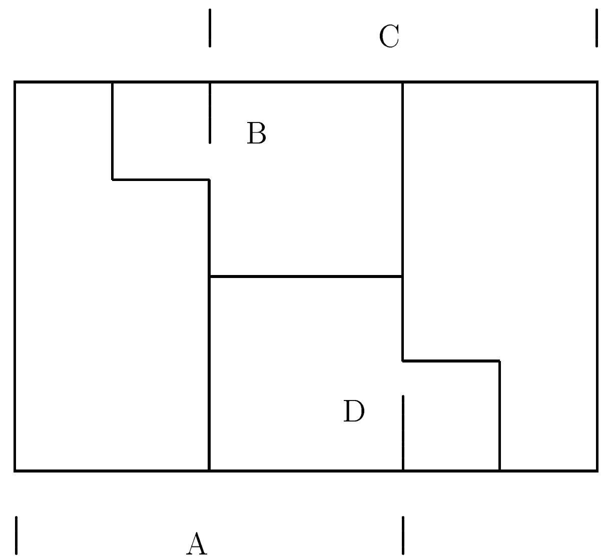

Figure 2: Proof of Lemma 2.2

Corollary 2.3 *For each $v \in \mathcal{D}^*$, $F = \{w : v \vee w = 1\}$ is closed under infima.*

Proof. Suppose $v = (A - B)^*$, and $(C_i - D_i)^* \in F$ for $i = 0, 1$. We show that $((C_0 \cap C_1) - (D_0 \cup D_1))^* \in F$. Clearly $A \cup (C_0 \cap C_1) =^* \omega$ and $B \cap (D_0 \cup D_1) =^* \emptyset$. A routine computation shows the major subset relations: e.g. for $A \subseteq^*_m (D_0 \cup D_1)$, if $A \cup D_0 \cup D_1 \cup E =^* \omega$, then $A \cup D_1 \cup E =^* \omega$, so $A \cup E =^* \omega$. $\diamondsuit$

We now obtain the definability of $\mathcal{E}^*$ as a subclass of $\mathcal{D}^*$.

Theorem 2.4 *An element of $\mathcal{D}^*$ is c.e. iff it is the supremum (in $\mathcal{D}^*$) of two elements which have a unique complement.*

Proof. Let $v \in \mathcal{D}^*$. First, if v is c.e., then choose c.e. disjoint sets A_0, A_1 of low degree such that $V = A_0 \cup A_1$. Then, in $\mathcal{D}^*, v = a_0 \vee a_1$. Moreover, since each a_i is low, but major subsets are high [So 87, XI.1.19], Lemma 2.1 implies that a_0, a_1 have a unique complement: $\overline{A_i}^*$ is a complement of a_i, and, if $(C - D)^*$ is a complement, where $A_i \cup C = \omega$ and $A_i \cap C \subseteq^* D$, then $A_i \subseteq^*_m A_i \cup D$. Therefore $D \subseteq^* A_i$ which implies $C - D =^* \overline{A_i}$.

For the other direction, it is sufficient to show that, if $(A - B)^*$ has a unique complement $(C - D)^*$ then $A - B$ must be c.e. Then, if an element

of $\mathcal{D}^*$ is the sup of two elements with a unique complement, it is c.e. as the supremum of two c.e. elements of $\mathcal{D}^*$. To show this, we use Lemma 2.2.
Since $A \cup C =^* \omega$, we can choose a computable set R s.t. $R \subseteq^* A$ and $\overline{R} \subseteq^* C$.
Case 1. C is recursive. By Lemma 2.2, $C \subseteq^*_m C \cup B$, which implies $C =^* C \cup B$, i.e. $B \subseteq^* C$. Since $A \cap C \subseteq^* B \cup D$ and $B \cap D =^* \emptyset$, it follows that $A - B =^* (A - C) \cup (A \cap D)$. So $A - B$ is c.e. (see Fig. 2).
Case 2. Otherwise, by [6], choose a small major subset $U \subset_{\mathrm{sm}} C$ (see [10] for a definition). Notice that U $*$-contains precisely those splits of C which are recursive ($U \subset_m C$ implies that U $*$-contains all recursive splits, and $U \subset_s C$ implies that all such splits are recursive). Thus, $\overline{R} \subseteq U$. Let $\widetilde{C} = U \cup D$. We claim that also $(\widetilde{C} - D)^*$ is a complement of $(A - B)^*$. To verify this, we check Lemma 2.2. Clearly, $\widetilde{C} - D \subseteq C - D$, so $(A - B) \cap (\widetilde{C} - D) = \emptyset$. Moreover, $\overline{R} \subseteq \widetilde{C}$, so $A \cup \widetilde{C} =^* \omega$. Finally $\widetilde{C} \subseteq^*_m C \subseteq^*_m C \cup B$, so $\widetilde{C} \subseteq_m \widetilde{C} \cup B$. Since we didn't change D, the hypotheses of Lemma 2.2 are satisfied.

Assume that $A - B$ is not c.e. We claim that, in this case,

$$\widetilde{C} - D \subset_\infty C - D$$

so that $(A - B)^*$ has two different complements. Assume that $C - D =^* \widetilde{C} - D$. Since $B \cap D =^* \emptyset$, $B \cap C \subseteq^* C - D \subseteq^* \widetilde{C} - D$. Thus $B \cap C \subseteq^* U$. But $S = R \cap B \cap C$ is a split of C with $\overline{R} \cup D$ as the other component since $R \cap C \subseteq^* A \cap C \subseteq^* B \cup D$. So S must be recursive. Let $X = \overline{R} \cup S \cup \overline{B}$ (X is co-c.e.). Then $A - B \subseteq^* X$ and $C \subseteq^* S \cup \overline{R} \cup D \subseteq^* X$. We will show that $\overline{X} =^* R \cap (B - S)$ is infinite. This contradicts $\sup((A - B)^*, (C - D)^*) = 1$. Assume $\overline{X}$ is finite. Then, "on R", $B =^* S$, so we have $B \subseteq^* C$. We will show that in this case,

$$A - B =^* (R - S) \cup (D \cap A)$$

so that $A - B$ is c.e. because S is recursive. Note that, if $B \subseteq^* C$, then $R - S =^* R - B$. So we get the inclusion "$\supseteq^*$" immediately from $R \subseteq A$ and $B \cap D = \emptyset$. For the inclusion "$\subseteq^*$" , consider $n \in A - B$. We can assume that $n \notin R$. Then $n \in A \cap C \subseteq^* B \cup D$, so for almost all relevant n, $n \in A \cap D$ because $n \notin B$. ♢

Corollary 2.5 $\{v \in \mathcal{D}^* : v \text{ c.e.}\}$ *is definable in* $\mathcal{D}^*$ *without parameters.*

♢

Corollary 2.6 $\mathrm{Aut}(\mathcal{E}^*) \cong \mathrm{Aut}(\mathcal{D}^*)$ *via the map* H *defined by*

$$H(\Phi)(a - b) = \Phi(a) - \Phi(b).$$

Proof. First we show that, for each $\Phi \in \mathrm{Aut}(\mathcal{E}^*), H(\Phi)$ is well-defined and an automorphism: Notice that for $a, b, c, d, \in \mathcal{E}^*$

$$\begin{aligned} a - b \leq c - d &\Leftrightarrow a \wedge d \leq b \ \wedge \ a \leq c \vee b \\ &\Leftrightarrow \Phi(a) \wedge \Phi(d) \leq \Phi(b) \ \wedge \ \Phi(a) \leq \Phi(c) \vee \Phi(b) \\ &\Leftrightarrow H(\Phi)(a-b) \leq H(\Phi)(c-d) \end{aligned}$$

Next, $\mathcal{E}^* = \{v \in \mathcal{D}^* : v \text{ c.e.}\}$ is a definable set which generates $\mathcal{D}^*$ under $\wedge$ and complementation. Hence H is $1-1$ and, for each $\Psi \in \mathrm{Aut}(\mathcal{D}^*)$, $\Psi = H(\Psi \restriction (\mathcal{E}^*))$. ♢

For the notions from model theory used in the following corollary, see [4], Ch. 5.

Corollary 2.7 *The structures $\mathcal{E}^*$ and $\mathcal{D}^*$ are bi-interpretable.*

Proof. In the introduction, we gave an interpretation $\mathcal{D}^* = \Gamma(\mathcal{E}^*)$, representing $v \in \mathcal{D}^*$ by pairs $a, b \in \mathcal{E}^*$ s.t. $v = a - b$. Theorem 2.4 gives an interpretation $\mathcal{E}^* = \Delta(\mathcal{D}^*)$.

We have to show that the isomorphisms

$$G : \mathcal{E}^* \cong \Delta(\Gamma(\mathcal{E}^*))$$

$$H : \mathcal{D}^* \cong \Gamma(\Delta(\mathcal{D}^*))$$

are definable in $\mathcal{E}^*$ and $\mathcal{D}^*$ respectively. For the first, note that G maps $a \in \mathcal{E}^*$ to a pair (b, c) representing a in $\mathcal{D}^*$. Then it is enough to notice that $\{(a; b, c) : a = b - c\}$ is definable in $\mathcal{E}^*$. For H, we have to show that the relation

$$(*) \qquad \{x; a, b : a, b \text{ c.e.} \ \wedge \ x = a - b\}$$

is definable in $\mathcal{D}^*$. Since $\mathcal{D}^*(\leq a) \cong \mathcal{D}^*$ for any c.e. $a \neq 0$, we can first assume $a = 1$ to obtain a formula $\widetilde{\psi}(b, x)$ defining "b c.e. $\wedge\, x = \overline{b}$". Then the formula $\psi(a, b, x) = \widetilde{\psi}^{[0,a]}(b, x)$ ($\widetilde{\psi}$ relativized to $[0, a]$) will define $(*)$. Recall from the proof of Theorem 2.4 that

$$\begin{aligned} \{v \in \mathcal{D}^* : v \text{ c.e. low}\} &\subseteq \{v : v \text{ has a unique complement}\} \\ &\subseteq \{v : v \text{ c.e.}\} \end{aligned}$$

So the desired formula is $\widetilde{\psi}(b, x) \equiv \exists b_0, b_1$

$$\text{"}b_0, b_1 \text{ have unique complements"} \ \wedge \ b = b_0 \vee b_1 \ \wedge \ x = \overline{b}_0 \wedge \overline{b}_1.$$

REFERENCES

[1] S. Burris and H.P. Sankappanavar, *A course in universal algebra*, Springer 1981.

[2] S. B. Cooper *On a conjecture of Kleene and Post*, University of Leeds preprint series (1993)

[3] L. Harrington and A. Nies, *Coding in the lattice of enumerable sets*, to appear.

[4] W. Hodges, *Model Theory*, Encyclopedia of mathematics and its applications 42, Cambridge University Press, 1993.

[5] A. Lachlan, *On the Lattice of Recursively Enumerable Sets*, TAMS 130(1968), 1–37.

[6] A. Lachlan, *The elementary theory of recursively enumerable sets*, Duke Math. J. 35 (1968), 123–146

[7] A. Nies, *Recursively enumerable equivalence relations modulo finite differences*, Math. Logic Quarterly 40 (1994), 490-518.

[8] A. Nies, *Undecidable fragments of elementary theories*, Algebra Universalis 35 (1996), 8–33.

[9] P. Odifreddi, *Classical Recursion Theory*, Vol. 1, North-Holland 1989

[10] R. Soare, *Recursively Enumerable Sets and Degrees*, Springer 1987.