Difference sets and computability theory

Rod Downey [a,1] Zoltán Füredi [b] Carl G. Jockusch, Jr [b,2]
Lee A. Rubel [3]

[a] *Department of Mathematics, Victoria University of Wellington, P.O. Box 600, Wellington, New Zealand*

[b] *Department of Mathematics, University of Illinois, 1409 West Green St., Urbana, IL 61801-2917, USA*

Abstract

For a set A of non-negative integers, let $D(A)$ (the difference set of A) be the set of non-negative differences of elements of A. Clearly, if A is computable, then $D(A)$ is computably enumerable. We show (as partial converses) that every simple set which contains 0 is the difference set of some computable set and that every computably enumerable set is computably isomorphic to the difference set of some computable set. Also, we prove that there is a computable set which is the difference set of the complement of some computably enumerable set but not of any computably enumerable set. Finally, we show that every arithmetic set is in the Boolean algebra generated from the computable sets by the difference operator D and the Boolean operations.

1 Introduction and Notation

For a set $A \subseteq \omega = \{0, 1, 2, \ldots\}$, let $D(A) = \{|a - b| : a, b \in A\}$. We call $D(A)$ the *difference set* of A. This paper is a sequel to [2], which was a study of the sets which have a given set as their difference set or k-th difference set, where D^k is the k-fold iteration of the difference operator D. Other papers

[1] Some of this research was carried out while Downey was a Visiting Professor at Cornell University. Downey's research is partially supported by the Victoria University IGC and by the New Zealand Marsden Fund for Basic Science.

[2] This work was supported by grants DMS 92-02833 and DMS 95-03398 from the National Science Foundation.

[3] Lee A. Rubel died March 25, 1995. He is greatly missed by his coauthors. His work was supported by grant DMS 91-23478 from the National Science Foundation.

on difference sets include [1], [3], [4], [5] and [6]. In the current paper we use the concepts and methods of computability theory (recursion theory) to compare the "complexity" of a set A with that of its difference set $D(A)$. For example, it is clear that if A is a computable set, then $D(A)$ is a computably enumerable (c.e.) set. We show that there is a computable set A such that $D(A)$ is noncomputable. In fact we show in Theorem 1 that every simple c.e. set is of the form $D(A)$ for some computable set A and in Theorem 5 that *every* c.e. set is computably isomorphic to a set of the form $D(A)$ with A computable. Thus, $D(A)$ may be considerably more complex than A, as one might expect from the unbounded existential quantifier which arises in the definition of $D(A)$. In the opposite direction, it is obvious that there are sets A such that $D(A)$ is "simpler" than A. For example, it is easily seen that there are uncountably many sets A such that $D(A) = \omega$. It is more interesting to give an example of a computable set R such that there exists a set X with $D(X) = R$, but *every* such set X is complex. This demonstrates that the difference operator cannot be effectively inverted. We show in Theorem 6 that there is a computable set R such that R is not the difference set of any c.e. set, yet R is the difference set of a co–c.e. set. One goal behind the results in both this paper and [2] was to characterize the family of all difference sets or else to show that this family is not Borel. (The latter result would indicate that no reasonable characterization is possible.) After hearing a talk based on an earlier draft of this paper, J. Schmerl [6, Theorem 1] in fact proved that this family is Σ^1_1-complete and hence not Borel. In fact he obtained a considerably more general result [6, Theorem 3] which he used to answer a number of open questions from [2] and in the area of the current paper. In Theorem 9 we prove that every arithmetical set can be obtained from computable sets by repeated use of the difference operator and Boolean operations.

Our notation is mostly standard, except for some changes in terminology. The traditional word "recursive" is replaced by "computable" and the phrase "recursively enumerable" is replaced by "computably enumerable" or its abbreviation "c.e.". Similarly, "recursively isomorphic" is replaced by "computably isomorphic". These changes were suggested by R. Soare, and a thoughtful discussion of the reasons for them is given in [7].

2 C.e. sets as difference sets of computable sets

The following result implies that the difference set of a computable set may be noncomputable.

Theorem 1 *Let B be any simple set such that $0 \in B$. Then there is a computable set R such that $D(R) = B$.*

Proof. The following lemma is well–known.

Lemma 2 *Every simple set contains arbitrarily long strings of consecutive integers.*

Proof. Let A be simple, and prove by induction on k that A contains the interval $[a, a+k]$ for infinitely many a. This is obvious for $k = 0$. Assume now that it is true for k. Let $B = \{a : [a, a+k] \subseteq A\}$, and let $C = \{a+k+1 : a \in B\}$. Then B is c.e. and is infinite by inductive hypothesis, so C is infinite. Hence $C \cap A$ is infinite, from which it follows that A contains $[a, a+k+1]$ for infinitely many a, completing the induction.

□

It now suffices to prove the following lemma, which is an effective version of the result that every set containing 0 and containing arbitrarily long intervals is a difference set. (This latter result is due to Sárközy and appears in [3].)

Lemma 3 *If A is a computably enumerable set such that $0 \in A$ and A contains arbitrarily long intervals, then there is a computable set R such that $D(R) = A$.*

Proof. The set R will be constructed as the union of a chain $R_0 \subseteq R_1 \subseteq \dots$ of finite sets. To ensure that $D(R) = A$ we require that $D(R_n) \subseteq A$ for all n and that $a_n \in D(R_{n+1})$, where $a_0, a_1, \dots$ is an effective enumeration of A. To make R computable we require that the canonical index of R_n should be a computable function of n and that $\max R_n < \min(R_{n+1} \setminus R_n)$. The sets R_n are defined recursively. Let $R_0 = \emptyset$. Given R_n, let k be the least number such that $k > \max R_n$ such that $D(R_n \cup \{k, k+a_n\}) \subseteq A$. Such a number k exists because $0, a_n \in A$, $D(R_n) \subseteq A$ and A contains arbitrarily long intervals. Let $R_{n+1} = R_n \cup \{k, k+a_n\}$ for this k.

□

□

Remark 4 *The following extension of Theorem 1 holds: For each $k \geq 1$ each simple set B with $0 \in B$ has the form $D^k(R)$ for some computable set R, where $D^1 = D$ and $D^{k+1} = D \circ D^k$. This follows from [2, Theorem 8.2] and the fact that each simple set is $t-$big for all t, as defined in Definition 8.1 of [2]. The latter fact can be proved by showing that if B is simple, there is no strongly computable sequence of pairwise disjoint finite sets of bounded cardinality all intersecting $\overline{B}$. This is well-known and is proved by an induction similar to that used to prove Lemma 3.*

It is easily seen that not every c.e. set may be obtained as the difference set of a computable set. In fact, there are computable sets, such as the set of powers of 2, which are not difference sets at all. (If an infinite set A is a difference set, then every element of A must be expressible in infinitely many ways as the difference of two elements of A.) On the other hand, the following result shows that the difference sets of computable sets occur in all computable isomorphism types of c.e. sets.

Theorem 5 *For any c.e. set A there is a computable set R such that A is computably isomorphic to $D(R)$.*

Proof. Let a c.e. set A be given. We construct a computable set R such that

$$(\forall n)[n \in A \iff n^2 \in D(R)] \tag{1}$$

and such that the set of nonsquares in $D(R)$ is computable.

We explain first why this suffices. By Theorem 1 we may assume without loss of generality that A is not simple. Also, we may assume that A is infinite and coinfinite. (If A is cofinite, it is a difference set by Lemma 3. If A is finite, then $D(A)$ is also finite. There are difference sets of every finite size since $D(\emptyset) = \emptyset$ and $D([0,n]) = [0,n]$, and c.e. sets of the same finite cardinality are computably isomorphic.) Since A is neither simple nor cofinite, there is an infinite computable set A_0 which is disjoint from A. Since A is infinite, there is an infinite computable set A_1 which is contained in A.

We show under the above hypotheses that $D(R) \equiv A$. For this it suffices to show that $A \leq_1 D(R)$ and $D(R) \leq_1 A$, by Myhill's isomorphism theorem. The former follows at once from (1). To show that $D(R) \leq_1 A$, inductively define a $1-1$ computable function h such that $D(R) = h^{-1}(A)$. Assume inductively that $h(i)$ has been defined for all $i < n$. Further, we assume that for all $i < n$, either $h(i) \in A_0 \cup A_1$, or, for some j, $i = j^2$ and $h(i) = j$. If n is not a square, determine effectively whether or not n is in $D(R)$. If n is not in $D(R)$, let $h(n)$ be the least element of A_0 which exceeds $h(i)$ for all $i < n$. If n is in $D(R)$, do the same with A_1 in place of A_0. Suppose now that n is a square, say $n = j^2$. Set $h(n) = j$ unless j is already a value of h. If j is already a value of h, then $j \in A_0 \cup A_1$. If $j \in A_k$ (where $k \leq 1$), let $h(n)$ be the least element of A_k which exceeds all current values of h. It is then easy to show by induction on n that $n \in D(R)$ iff $h(n) \in A$. Since h is a $1-1$ computable function, we conclude that $D(R) \leq_1 A$. This concludes the proof that it suffices to make (1) hold and arrange that the set of non-squares in $D(R)$ be computable.

We now give the construction of a computable set R to meet the above requirements. As in Lemma 3, we obtain R as the union of a chain $R_0 \subseteq R_1 \subseteq$

... of finite sets given effectively by canonical indices. We let $R_0 = \emptyset$ and $R_{n+1} = R_n \cup \{k, k + a_n^2\}$, where $a_0, a_1, \ldots$ is an effective enumeration of A and k is chosen appropriately. Specifically, we require that $k > \max R_n$ so that $\max R_n < \min(R_{n+1} \setminus R_n)$. Further, we require that all elements of $D(R_{n+1}) \setminus D(R_n)$ other than a_n^2 should be nonsquares and should exceed all elements of $D(R_n)$. Since all such elements have the form $k - r$ or $k + a_n^2 - r$ with $r \in R_n$, this may be achieved by choosing k sufficiently large and in a sufficiently large gap between consecutive squares. It is then easy to see that R has the necessary properties. In particular, the construction gives an effective enumeration of the non-squares in $D(R)$ in increasing order.

□

3 Impossibility of effective inversion of the difference operator

The following result shows that a computable set can be a difference set and yet not be the difference set of any c.e. set.

Theorem 6 *There is a computable set R such that R is the difference set of a co–c.e. set but R is not the difference set of any c.e. set.*

Proof. We construct a c.e. set A such that $D(\overline{A})$ is computable and A meets the following requirements for all e:

$$N_e : \quad |\overline{A}| \geq e + 1 \tag{2}$$
$$P_e : \quad W_e \text{ infinite } \longrightarrow D(\overline{A}) \neq D(W_e)$$

The main source of difficulty in meeting the above requirements is that we must ensure that $D(\overline{A})$ is computable. Thus, to meet P_e, we cannot simply wait until sufficiently large elements appear in $D(W_e)$ and then (if necessary) add elements to A to make those elements disappear from $D(\overline{A})$. Instead, we take advantage of the fact that the appearance of finitely many elements in W_e can create infinitary patterns in $D(W_e)$ (since those elements are involved in infinitely many differences if W_e is infinite). We can then add elements to A and put further restrictions on A so as to prevent those infinitary patterns from occurring in $D(\overline{A})$. Of course, this must be done so as to preserve any of the finitely many membership decisions which have (irrevocably) been made for $D(\overline{A})$ so that we can make $D(\overline{A})$ computable.

To make the above idea more precise, note that if W_e is infinite and F is a finite subset of W_e, then $D(W_e)$ contains infinitely many translates of $-F$, in particular all sets of the form $a - F$ for $a \in W_e$, $a > \max F$. Thus, to meet P_e it suffices to ensure that, if W_e is infinite, there is a finite set $F \subseteq W_e$ such that $D(\overline{A})$ contains only finitely many translates of $-F$. For this, it is obviously necessary (replacing W_e by $\overline{A}$ in the above argument) that $\overline{A}$ should not contain any translate of F. As the construction proceeds, we modify our approximation to $\overline{A}$ so that it does not contain any translate of F. This is done so that any membership decisions made about $D(\overline{A})$ are preserved. Further care is then necessary to ensure that $D(\overline{A})$ contains only finitely many translates of $-F$. The following lemma shows that this can be done.

Lemma 7 *Let C be a finite set, let $F_1, F_2, \ldots, F_n$ be 3-element sets, and let s and t be numbers with $t < s$. Suppose that $C \cap [0,t]$ contains no translate of any F_i. Then there is a finite set $\hat{C}$ such that $|\hat{C}| \geq s+1$, $\hat{C} \cap [0,t] = C \cap [0,t]$, $D(C) \cap [0,s] = D(\hat{C}) \cap [0,s]$, $\hat{C}$ does not contain any translate of any F_i, and $\hat{C} \setminus C$ does not contain any element of $[0,s]$. Further, if $1 \leq i \leq n$ and each element of $D(C) \setminus D(C \cap [0,t])$ exceeds $\max F_i + t$, then any translate of $-F_i$ contained in $D(\hat{C})$ is contained in $D(C)$.*

Proof. We first prove the result ignoring the requirement that $|\hat{C}| \geq s+1$ and then at the end indicate the easy modification of the argument that may be used to meet this condition. Let $\hat{C} = C_0 \cup C_1$, where $C_0 = C \cap [0,t]$, $D^* = D(C) \backslash D(C_0)$ and $C_1 = \cup_{d \in D^*} \{b_d, b_d + d\}$. Here the numbers b_d for $d \in D^*$ should be chosen sufficiently large, sufficiently far apart, and with differences sufficiently far apart for the proof given below to work. First, regardless of the choice of the b_d's, it is clear that $D(C) \subseteq D(\hat{C})$. Also, by choosing $b_d > t$ for each $d \in D^*$, we ensure that $C \cap [0,t] = \hat{C} \cap [0,t]$. Next, any element of $D(\hat{C}) - D(C)$ must have the form $u - v$ where $u \in \{b_e, b_e + e\}$ for some $e \in D^*$ and either $v \in \{b_d, b_d + d\}$ for some $d \in D^*$ with $b_d < b_e$, or $v \leq t$. Let m be the greatest element of $D(C)$. To ensure that all elements of $D(\hat{C}) \setminus D(C)$ exceed s we require that $b_e > b_d + m + s$ for $d, e \in D^*$ with $b_d < b_e$ and that $b_a > s + t$ for any b_a with $a \in D^*$. Since $b_a > s$ for all $a \in D^*$, it follows that all elements of $\hat{C} \setminus C$ also exceed s.

We now check that $\hat{C}$ does not contain any translate of any F_i. Suppose for a contradiction that $\{a, b, c\} \subseteq \hat{C}$ and $\{a, b, c\}$ is a translate of F_i, where $a < b < c$. Then $c \notin C_0$ since C_0 contains no translate of F_i. Hence c has the form b_e or $b_e + e$ for some $e \in D^*$. Then $a \in C_0$, or a has the form b_d or $b_d + d$ for some $d \in D^*$ with $b_d < b_e$. Therefore $a - c \geq b_e - t$ or $a - c \geq b_e - b_d - d$ where $b_d < b_e$. This can be avoided by choosing b_e to be sufficiently large, as in the previous paragraph.

Finally, assume that $1 \leq i \leq n$ and each element of D^* exceeds each element of F_i. It must be shown that any translate of $-F_i$ contained in $D(\hat{C})$ is contained in $D(C)$. Let $\{d_1, d_2, d_3\} \subseteq D(\hat{C})$ be a translate of $-F_i$. Note that $|d_j - d_k| \leq$

$m = \max F_i$ for $j, k \in \{1, 2, 3\}$. Let $d_j = a_j - c_j$, where $a_j, c_j \in \hat{C}$.

Case 1 *For some j, $1 \leq j \leq 3$, $d_j \in D(C)$.*

The b_d's may be chosen so that all elements of $D(\hat{C}) \setminus D(C)$ exceed $m + \max D(C)$ (just as it was argued above that these numbers may all be made to exceed s). Fix j with $d_j \in D(C)$ and assume for a contradiction that $d_k \notin D(C)$ holds for some $k \in \{1, 2, 3\}$. Then $|d_k - d_j| = d_k - d_j > (m + \max D(C)) - \max D(C) = m$ in contradiction to a remark in the previous paragraph. Hence $d_k \in D(C)$. It follows that d_1, d_2 and d_3 all belong to $D(C)$ as needed.

Case 2 *Assume that $a_1 = a_2 = a_3$.*

Then it is easily seen that $\{c_1, c_2, c_3\}$ is a translate of F_i contained in $\hat{C}$. However, $\hat{C}$ was chosen so that no such translate exists, so this case cannot arise.

Case 3 *Assume that $a_1 = a_2 \neq a_3$ and that Case 1 does not apply.*

Then $|c_1 - c_2| = |d_1 - d_2| \leq m$. It follows that $c_1, c_2 \in C_0$, since any two distinct elements of C differ by more than $m + t$ unless both are in C_0. (By choosing the b_d's sufficiently large and sufficiently far apart, we can arrange that any two distinct elements of C which are not both in C_0 differ by at least $\min D^*$. By hypothesis, all elements of D^* exceed $m + t$.)

Next, we claim that $c_3 \in C_0$. Suppose for a contradiction that $c_3 \notin C_0$. Roughly speaking, we now obtain a contradiction because this implies that $|d_1 - d_3|$ is approximately equal to $|b_d - b_e + b_f|$ for some $d, e, f \in D^*$ with an error which can be bounded in advance, but the values of b_d, b_e, and b_f may be chosen so that $|b_d - b_e + b_f|$ exceeds the sum of m and the error in the approximation so that $|d_1 - d_3| > m$, a contradiction. In more detail, let $a_1 \in \{b_d, b_d + d\}$, $a_3 \in \{b_e, b_e + e\}$, and $c_3 \in \{b_f, b_f + f\}$, where $d, e, f \in D^*$. Then $|(d_1 - d_3) - (b_d - b_e + b_f)| = |(a_1 - b_d) - c_1 - (a_3 - b_e) + (c_3 - b_f)| \leq d + t + e + f$. But the values of b_d, b_e and b_f may be chosen so that $|b_d - b_e - b_f| > d + t + e + f + m$. Hence $|d_1 - d_3| > m$, a contradiction. It follows that $c_3 \in C_0$.

Assume, as above, that $a_1 \in \{b_d, b_d + d\}$ and $a_3 \in \{b_e, b_e + e\}$. We know that c_1 and c_3 belong to C_0. Also, since a_1 and a_3 are distinct elements of $\hat{C} - C$, $|a_1 - a_3| \geq \min D^* > m + t$, where $m = \max F_i$. Hence $|d_1 - d_3| = |(a_1 - c_1) - (a_3 - c_3)| = |(a_1 - a_3) - (c_1 - c_3)| \geq |a_1 - a_3| - |c_1 - c_3| > (m + t) - t = m$, in contradiction to the fact that $|d_1 - d_3| \leq m$. Thus, this case cannot arise.

Case 4 *By symmetry, the only remaining case we need consider is where a_1, a_2, a_3 are distinct elements of $C_1 = \hat{C} \setminus C_0$, and Case 1 does not apply.*

Split up the elements of C_1 into those of the form b_d for some $d \in D^*$ and those of the form $b_d + d$ for some $d \in D^*$. By the pigeon-hole principle, there must be two elements of $\{a_1, a_2, a_3\}$ of the same form, say $b_d + d$. (The case where there are two of the form b_d is similar.) Say that $a_1 = b_d + d$ and $a_2 = b_e + e$, where $d, e \in D^*$. Then $e \neq d$ since $a_1 \neq a_2$, so $b_e \neq b_d$. By reindexing if necessary, we may assume that $b_d > b_e$. Since Case 1 does not apply, $c_1 \neq b_d$. Therefore $c_1, c_2 \in C_0 \cup \{b_p : p \in D^*, b_p < b_d\} \cup \{b_p + p : p \in D^*, b_p < b_d\}$. By making b_d much greater than t and all b_p with $b_p < b_d$, we can ensure that d_1 is much bigger than d_2 and in particular that $d_1 - d_2 > m$, a contradiction. We omit the routine but tedious details.

This completes the proof in the absence of the requirement that $|\hat{C}| > s$. This requirement may obviously be met by adding to $\hat{C}$ as defined above a sufficient number of large, far-apart elements. Specifically, any differences between these new elements or between these new elements and old elements should exceed s and $\max \cup_{i=1}^{n} F_i$.

$\square$

We now give the construction. Let A_s be the set of numbers enumerated in A before the beginning of stage s of the construction. At the beginning of stage s we will have a set C_s with $|C_s| \geq s$ which is disjoint from A_s and is our current approximation to $\overline{A}$. Then $D(C_s) \cap [0, s]$ is our current approximation to $D(\overline{A})$, and in fact we will have $D(\overline{A}) \cap [0, s] = D(C_s) \cap [0, s]$. Since the construction is effective, this implies that $D(\overline{A})$ is computable. Also at the beginning of stage s we will have a finite set L_s of 3-element sets such that C_s contains no translate of any set in L_s.

For each e and s with $e \leq s$, let $r(e, s)$ be the least number r such that $|C_s \cap [0, r]| \geq e$ and for each $d \in D(C_s) \cap [0, s]$ with $d \leq e$ there exist $u, v \in C_s \cap [0, r]$ with $d = u - v$. Such a number r must exist because $e \leq s \leq |C_s|$. For completeness, define $r(e, s) = s$ if $e > s$. The number $r(e, s)$ (for $e \leq s$) represents the "restraint" that the positive requirement P_e must respect at stage s, i.e. P_e should not cause any number $x \leq r(e, s)$ to enter A at stage s. The number $r(e, s)$ not only reflects the need to satisfy the negative requirements N_i for $i \leq e$ but also the need to ensure that each number $d \leq e$ in $D(C_s) \cap [0, s]$ for infinitely many s is in $D(\overline{A})$.

A requirement P_e *requires attention* at stage s if it has never previously received attention, $r(e, s) < s$, and there is a set F such that $|F| = 3$, $F \subseteq W_{e,s}$, and $C_s \cap [0, r(e, s)]$ contains no translate of F.

Stage 0. Initialize the construction by letting $A_0 = C_0 = L_0 = \emptyset$.

Stage $s, s > 0$. Let e be the least number such that $e \leq s$ and P_e requires attention at s, if there is such an e. Fix a finite set F which witnesses that P_e

requires attention, and let $L_{s+1} = L_s \cup \{F\}$. Apply Lemma 7 with $C = C_s$, s as in the construction, $\{F_1, \dots, F_n\} = L_{s+1}$ and $t = r(e, s)$. Let $C_{s+1} = \hat{C}$, where $\hat{C}$ is the set asserted to exist by Lemma 7 in this context. Let $A_{s+1} = A_s \cup \{z : z < s \quad \& \quad z \notin C_{s+1}\}$. Say that P_e *receives attention* at s. If there is no $e \leq s$ such that P_e requires attention at s, proceed in the same fashion, but let $L_{s+1} = L_s$ (rather than $L_s \cup \{F\}$ as above). This completes the construction.

We must now show that $A = \cup_s A_s$ has the desired properties. This is a straightforward "wait-and-see" argument. First, it is obvious that A is c.e. and each requirement P_e receives attention at most once. An easy induction on s shows that $A_s \cap C_s = \emptyset$ for each s. Also, it follows from the construction that if $u \in \overline{A}$, then $u \in C_{s+1}$ for all $s > u$. Given e, choose $s_0 \geq e$ so large that no requirement P_i with $i \leq e$ receives attention after stage s_0. Let r_0 be the least number r such that $|C_{s_0} \cap [0, r]| = e$. Then $r(e, s_0) \geq r_0$, and one may show by induction on s that $r(e, s) \geq r_0$ and that $C_s \cap [0, r_0] = C_{s_0} \cap [0, r_0]$ for all $s \geq s_0$. Hence $C_{s_0} \cap [0, r_0]$ is a set of size e which is disjoint from A. Since e was arbitrary, it follows that $\overline{A}$ is infinite.

It is easily seen that if $e \leq s$ and $r(e, s) \neq r(e, s + 1)$ then some requirement P_i with $i \leq e$ requires attention at stage $s + 1$. It follows that $\lim_s r(e, s)$ exists for each e.

Lemma 8 *$D(\overline{A})$ is computable.*

Proof. First note that if $x \in D(C_s)$ for infinitely many s, then $x \in D(\overline{A})$. To see this, let s_0 be a stage such that no P_e with $e < x$ receives attention after stage s_0. Pick $s \geq s_0$ such that $x \in D(C_s)$. Then there exist u and v such that $x = u - v$ and u and v are each in C_s and $\leq r(x, s)$. Then $r(x, s) = r(x, t)$ for all $t \geq s$, and it follows that $u, v \in \overline{A}$. Thus $x \in D(\overline{A})$ as needed.

Now we claim that $D(\overline{A}) \cap [0, s] = D(C_s) \cap [0, s]$ for all s. This clearly implies that $D(\overline{A})$ is computable. By induction on z and the construction, if $z \geq s$, then $D(C_z) \cap [0, s] = D(C_s) \cap [0, s]$. Hence, if $x \in D(C_s) \cap [0, s]$, then $x \in D(C_z)$ for all $z \geq s$. It follows that $x \in D(\overline{A})$ by the previous paragraph. This shows that $D(C_s) \cap [0, s] \subseteq D(\overline{A}) \cap [0, s]$. For the reverse inclusion, assume that $x \in D(\overline{A}) \cap [0, s]$. Let $x = u - v$, where $u, v \in \overline{A}$. Then, for sufficiently large z, we have $u, v \in C_z$, so $x \in D(C_z) \cap [0, s] = D(C_s) \cap [0, s]$.

□

It remains only to show that each positive requirement P_e is satisfied. Assume that W_e is infinite. Then W_e contains a 3-element subset F such that no translate of F is contained in $[0, r]$, where $r = \max_s r(e, s)$. Thus P_e eventually receives attention. (If not, it requires attention through F at all sufficiently large stages and thus must eventually receive attention.) If P_e receives attention at stage s_1 through F, then $F \in L_s$ for all $s > s_1$, and (by induction on s) C_s contains no translate of F for all $s > s_1$. Now choose $s_2 > s_1$ so that, for all $s > s_2$, every member of $D(\overline{A}) \cap [0, e]$ is in $D(C_s)$. Then, by Lemma 7, for all $s \geq s_2$, every translate of $-F$ in $D(C_{s+1})$ is in $D(C_s)$. Thus, there are only finitely many translates of $-F$ contained in $\cup_s D(C_s)$. But $\cup_s C_s \supseteq \overline{A}$, so there are only finitely many translates of $-F$ contained in $D(\overline{A})$. However, since $F \subseteq W_e$ and W_e is infinite, there are infinitely many translates of $-F$ contained in $D(W_e)$. This shows that $D(W_e) \neq D(\overline{A})$ and completes the proof of the theorem.

□

J. Schmerl has shown has shown that the "dual" of the preceding theorem holds, i.e. there is a computable set which is the difference set of a c.e. set but not of any co-c.e. set.

4 The difference operator and arithmetical sets

In this section we show that the family of arithmetical subsets of ω is generated from the computable subsets of ω by the difference operator and Boolean operations. This is not too surprising since the difference operator is analogous to the existential quantifier. However, it is unusual to generate the arithmetical subsets of ω directly, without also generating the arithmetical subsets of ω^k for all k.

Theorem 9 *The family of arithmetical subsets of ω is the smallest Boolean algebra of subsets of ω that contains every computable subset of ω and is closed under the difference operator D.*

Proof. Let $\mathcal{D}$ be the smallest Boolean algebra of subsets of ω containing all computable subsets of ω and closed under D. Obviously $\mathcal{D}$ is contained in the family of arithmetical subsets of ω. To obtain the reverse inclusion, it suffices to show for each n that if every Π_n set belongs to $\mathcal{D}$, then every Σ_{n+1} set belongs to $\mathcal{D}$. Let $A \in \Sigma_{n+1}$. Then

$$A = \{x : (\exists s)[(x, s) \in C]\} \tag{3}$$

for some Π_n set $C \subseteq \omega^2$. We will define two computable functions $k_1(x, s)$, $k_2(x, s)$ and set

$$C_i = \{k_i(x, s) : (x, s) \in C\} \cup \{k_i(x, s) + x : (x, s) \in C\} \tag{4}$$

for $i=1,2$. We will have that $k_i(x,s) \geq \max\{x,s\}$ for $i=1,2$ and all $x,s \in \omega$. Hence C_1, C_2 will each be Π_n, since, for all $u \in \omega$,

$$u \in C_i \iff (\exists x)_{\leq u}(\exists s)_{\leq u}[(u = k_i(x,s) \text{ or } u = k_i(x,s)+x) \ \& \ (x,s) \in C] \quad (5)$$

Finally, we ensure that

$$A = D(C_1) \cap D(C_2). \quad (6)$$

Since each C_i is Π_n and hence is in $\mathcal{D}$ by hypothesis, the above equation implies that $A \in \mathcal{D}$.

It remains to define k_1, k_2 with the properties specified above. Note that $A \subseteq D(C_1) \cap D(C_2)$ regardless of the choice of k_1, k_2, as may be seen by considering differences of the form $a-b$, where $a = k_i(x,s)+x$ and $b = k_i(x,s)$. Now, for $i=1,2$, let U_i be the set of potential elements of $D(C_i)$ which arise in other ways (i.e. the "unintended" potential elements of $D(C_i)$). More precisely, let U_i be the set of all numbers of the form $|a-b|$ such that there exist distinct pairs $(x,s),(x',s') \in \omega^2$ with $a \in \{k_i(x,s), k_i(x,s)+x\}$ and $b \in \{k_i(x',s'), k_i(x',s')+x'\}$. Since $D(C_i) \subseteq A \cup U_i$, to ensure that $D(C_1) \cap D(C_2) = A$ it suffices to ensure that $U_1 \cap U_2 = \emptyset$. This is done by making the functions k_1, k_2 grow sufficiently fast.

The functions k_1, k_2 are defined simultaneously by stages. Specifically, define $k_1(x,s)$ at stage $2\langle x,s\rangle$ and $k_2(x,s)$ at stage $2\langle x,s\rangle+1$, where $\langle .,. \rangle$ is a computable bijection from ω^2 to ω. When $k_i(x,s)$ is defined, finitely many new values are contributed to U_i, specifically all those generated by the pairs $(x,s),(x',s')$ with $\langle x',s'\rangle < \langle x,s\rangle$. All of these new elements may be made as large as desired by choosing $k_i(x,s)$ sufficiently large. Thus, let $k_i(x,s)$ be the least number which exceeds $\max\{x,s\}$ and is such that all elements it causes to enter U_i exceed all elements already in U_{3-i}. Then k_1, k_2 clearly have the desired properties, and the proof is complete.

□

We do not know whether every arithmetical subset of ω is computably isomorphic to one obtained from a computable set by repeated application of the difference operator D and complementation.

The following is a corollary to the proof of Theorem 9 obtained by omitting reference to the classifications of A, C_1, and C_2 in the arithmetical hierarchy.

Corollary 10 *Every set $A \subseteq \omega$ has the form $D(C_1) \cap D(C_2)$ for some $C_1, C_2 \subseteq \omega$.*

References

[1] P. Erdős, A. Sárközy, and V. T. Sós, On additive properties of general sequences, *Discrete Math.*, **134** (1994), 75–99.

[2] Z. Füredi, C. Jockusch, and L. A. Rubel, Difference sets and inverting the difference operator, *Combinatorica* **16** (1996), 87–106.

[3] I. Z. Ruzsa, On difference-sequences, *Acta Arithmetica* **25** (1974), 151–157.

[4] I. Z. Ruzsa, On difference sets, *Studia Scientiarum Mathematicarum Hungarica* **13** (1978), 319–326.

[5] I. Z. Ruzsa, Difference sets and the Bohr topology, I, preprint.

[6] J. H. Schmerl, What's the difference?, in this issue of *Annals of Pure and Applied Logic*

[7] R. I. Soare, Computability and recursion, to appear in *Bulletin of Symbolic Logic*, 1996.