SOME REMARKS ON WITNESS FUNCTIONS FOR NON-POLYNOMIAL AND NON-COMPLETE SETS IN NP

by

Deborah Joseph
and
Paul Young

Computer Sciences Technical Report #533

February 1984

Some Remarks on Witness Functions for Non-Polynomial and Non-Complete Sets in NP[+]

Deborah Joseph[*]

Computer Science Department
University of Wisconsin
Madison, WI 53706

Paul Young[**]

Computer Science Department; FR 35
University of Washington
Seattle, WA 98195

We present two results about witness functions for sets in NP and $coNP$. First, any set that has a polynomially computable function which honestly witnesses that it is not in $coNP$ must be at least NP-hard. It follows from this result that any set in $NP-P$ that has a polynomially computable function that witnesses this fact must be complete for NP. Second, if A is any set for which there is a polynomially computable function which witnesses that it is not complete for NP, by merely witnessing that some fixed set in NP is not in P^A, then A must be in $NP \cap coNP$. Thus for two sets in $NP-coNP$, there are no polynomially computable functions which witness that one is not polynomially reducible to the other. In proving the first result we introduce the notion of a k*-creative* set and prove that all k-creative sets with honest productive functions are NP-complete. Since these sets seem not to be all polynomially isomorphic, we counter the conjecture of Berman and Hartmanis that all NP-complete sets are isomorphic with a conjecture that *not all* k-creative sets are isomorphic. The proofs we give are recursion-theoretic in style, but quite straightforward and easy.

[*] Supported by a University of Wisconsin Research Committee Grant.

[**] Supported by NSF Research Grant MCS 7609212A, University of Washington.

[+] The results contained in this paper were initially presented (unfortunately sometimes in incorrect form) by Paul Young at the 15th ACM SIGACT (Apr 1983) as part of an extended abstract entitled, *Some structural properties of polynomial reducibilities and sets in NP.*

Witness functions for $P \neq NP$ have been investigated by several previous authors, Kozen [Koz-80], Kozen and Machtey [K&M-80], O'Donnell [O'D-79], and Joseph [Jos-83]. In [Koz-80] Kozen refutes the suggestion of Baker, Gill and Solovay [BGS-75] that it will not be possible to prove that $P \neq NP$ by diagonalization, by showing that there exist witness functions for $P \neq NP$ if and only if there exist diagonals. However Kozen's work gives only limited insight about the possible complexity of witness functions for $P \neq NP$ should they exist - essentially he shows that if there is a polynomial witness function for $P \neq NP$, then a universal function for P must exist within NP. Some additional insight is given in O'Donnell's work, which shows that if $P \neq NP$ but this is not provable from Peano Arithmetic + T_{Π_1} (the true Π_1 sentences of arithmetic), then witness functions for $P \neq NP$ must grow faster than any provably recursive function. Similarly, in [Jos-83] it is shown that if it is consistent with a certain very weak arithmetic theory, $ET(Elem)$, to believe that $P = NP$, then there can be no monotone elementary function which witnesses that $P \neq NP$.

In this note we prove two simple facts about witness functions that are polynomially computable. We hope that these facts will be useful in explaining why proving $P \neq NP$ is so difficult. Among other things, our results show that in NP, sets that are complete and sets that are in $coNP$ cannot be separated by witness functions that are polynomially computable and honest.

It is commonly believed that the question of whether $P = NP$ has certain structural similarities to Post's problem - the problem in pure recursion theory of whether there are incomplete r.e. sets. In discussing why there are no constructive arguments in recursion theory for solving Post's problem and why the Friedberg-Muchnik priority arguments were required to solve it,[1] Rogers cites two theorems on the impossibility of constructive solutions to Post's problem:

[1] For references to subrecursive, including polynomial, versions of the Friedberg-Muchnik argument, see [Lad-75], [C&M-81] and [Sch-82].

Theorem I, [Rog-67,pp. 162]. If A is recursively enumerable and constructively nonrecursive, then A is creative. (And hence A is complete.)

Theorem II, [Rog-67,pp. 162]. If A and B are recursively enumerable, and if A is constructively nonrecursive in B, then B is recursive.

Since it is easily seen that any creative set is complete, Theorem I shows that if there is any computable witness function which shows that an r.e. set A is not recursive, then A must already be complete. On the other hand, Theorem II shows that if there is any computable function which witnesses that a set A is not complete, then A must actually be recursive. Thus notions of "complete" and of "decidable" cannot be "constructively" separated.

We show that if we restrict witness functions to be polynomial, then a version of Theorem I holds for NP. We also show that with the same restriction on our witness functions, a strong version of Theorem II holds for *NP vs NP∩coNP*. Our proofs essentially follow those in Rogers, [Rog-67].

Our notation follows that in [Rog-67] and [M&Y-78], except that we cannot use arbitrary complexity measures and programming systems. Our programming system uses both deterministic and nondeterministic programs which have a syntactically checkable condition that any nondeterministic computation is required to be single valued. (In fact for our purposes, nondeterministic programs may be permitted to output only 1.) $\varphi_i(x)$ is the output (if any) of program i on input x. In addition, Φ is a natural runtime complexity measure for such a programming system, i.e., it is one that is normally considered reasonable for investigations of P and NP. We define $W_i =_{def} \{ x : \varphi_i(x)\downarrow \}$ and define:

$$P^{(k)} =_{def} \{ W_i : \textit{program } i \textit{ is deterministic and } \varphi_i(x)\downarrow \textit{ implies } \Phi_i(x) < |i|\cdot|x|^k + |i| \},$$

$$NP^{(k)} =_{def} \{ W_i : \varphi_i(x)\downarrow \textit{ implies } \Phi_i(x) < |i|\cdot|x|^k + |i| \}.$$

Thus $P = \bigcup_k P^{(k)}$ and $NP = \bigcup_k NP^{(k)}$.

We begin with a weak definition of polynomial creativity[2].

Definition. Let k_0 be any fixed integer. A set $C \in NP$ is k_0*-creative* if there is a polynomially computable function f (a *productive* function) such that for all i which witness that $W_i \in NP^{(k_0)}$,

$$f(i) \in C \cap W_i \text{ or } f(i) \in \bar{C} - W_i.$$

The idea behind this definition is that a set C is creative if f is a polynomial witness, not fully to the fact that $\bar{C}$ is not in NP, but merely to the fact that $\bar{C}$ is not in $NP^{(k_0)}$. Thus a very strong analogue to Theorem I above would be that every k_0 creative set is complete. Unfortunately we are unable to prove such a theorem. Recall however that a function f is *polynomially honest* if its running time is bounded by some polynomial in its value. For example, every polynomially computable function whose arguments are within a polynomial of the outputs is polynomially honest -- polynomially computable functions that are *not* honest must have *very small* outputs for some inputs. If a set C is not in *coNP*, then for every infinite W_i in NP there is a value $f_0(i)$ that is greater than i and such that $f_0(i) \in C \cap W_i$ or $f_0(i) \in \bar{C} - W_i$. Thus it seems not unreasonable to restrict our attention to witness functions that are greater than the identity function, or, what is an even weaker restriction for polynomially computable functions, those that are polynomially honest.[3] Our first result is a polynomial analogue to Theorem I.

[2] Ko and Moore, [K&M-81], have given another natural definition of polynomial creative sets. However, using their definition they have shown that there can be no polynomially creative sets even in DTIME(2^{poly}).

[3] A similar argument for restricting one's attention to witness functions at least as big as the identity is made in [Jos-83]. There however one is considering elementary functions as witness functions. Since an elementarily bounded search over an elementarily computable function still leaves one with an elementary time-bound, the restriction in [Jos-83] is more reasonable than the corresponding restriction in this paper, since we are here concerned with polynomial computations.

Theorem 1. Every k_0-creative set with a polynomially honest productive function is NP-complete. (In fact, complete with respect to Karp reducibility.)

Proof. To simplify notation we first give the proof under the assumption that the productive function f is not just honest, but that it grows at least as rapidly as the identity. Let C be a k_0 creative set with productive function f and let A be any set in NP. In particular let A be in $NP^{(k)}$ for some fixed k. We must show that A is Karp reducible to C. Define a polynomially computable function g such that

$$\varphi_{g(y)}(z) = \begin{cases} 0 \text{ if } |z|^{k_0} > |y|^k \ \mathit{and}\ y \in A \\ \uparrow \ \mathit{otherwise} \end{cases}.$$

Here, given that A is nondeterministic, $\varphi_{g(y)}$ is to be computed in the most obvious nondeterministic fashion. First test whether $|z|^{k_0} > |y|^k$; this takes time proportional to $|z|^{k_0}$. Next test whether $y \in A$ using the nondeterministic algorithm for A; this takes time proportional to $|y|^k$ which is less than $|z|^{k_0}$. If both of these are true then output 1 and otherwise diverge. By suitably "padding" the instructions for $g(y)$, we can also make $|g(y)|^{k_0} > |y|^k$. Clearly, $g(y)$ can be computed in time approximately $|y|^{k_0-k}$.

But we now have that $y \in A$ iff $W_{g(y)} = \{ z\colon\ |z|^{k_0} > |y|^k \}$ iff $g(y) \in W_{g(y)}$. But by construction $W_{g(y)} \in NP^{(k_0)}$ and C is k_0-creative with productive function f. Thus, since $f(g(y)) > g(y)$, $y \in A$ iff $f(g(y)) \in W_{g(y)}$; and because f is a productive function for C, $f(g(y)) \in W_{g(y)}$ iff $f(g(y)) \in C$. Thus $y \in A$ iff $f(g(y)) \in C$, so C is Karp complete.

In the event that f is not greater than the identity but is instead merely polynomially honest, one simply replaces the condition $|g(y)|^{k_0} > |y|^k$ by a condition that makes $g(y)$ not only this big, but also big enough to guarantee that $|f(g(y))|^{k_0} > |y|^k$. ■

Theorem 1 leaves open the question of whether k-creative sets exist. Fortunately, they do, and Theorem 2 provides an interesting class of k-creative sets:

Theorem 2. Let f by any polynomially computable, polynomially honest, one-one function. Define

$$K_f^k = \{ f(i) : \Phi_i(f(i)) \leq |i| \cdot |f(i)|^k + |i| \},$$

then K_f^k is k-creative, with f as an honest productive function.

Proof. One easily verifies that K_f^k is in NP by observing that since f is polynomially computable and polynomially honest, given y one can guess a value x and verify that $f(x) = y$ in polynomial time. Once this is done, checking that $\Phi_x(y) \leq |x| \cdot |y|^k + |x|$ can easily be done in nondeterministic polynomial time. f itself is the required productive function for $\overline{K_f^k}$ since given any $W_i \in NP^k$,

$$\begin{aligned} f(i) \in W_i &\Leftrightarrow \varphi_i(f(i)) \downarrow \\ &\Leftrightarrow \Phi_i(f(i)) \leq |i| \cdot |f(i)|^k + |i| \\ &\Leftrightarrow f(i) \in K_f^k. \quad \blacksquare \end{aligned}$$

Simple as they are Theorems 1 and 2 give a whole new class of *structurally* defined sets in NP. Before proceeding, we would like to look at this class more carefully.

A Momentary Diversion

In studying "natural" NP-complete sets, Berman and Hartmanis, [B&H-77], observed that all of the "natural" NP-complete sets have polynomially computable padding functions. This fact, together with the fact that in recursive function theory all "complete" sets are recursively isomorphic, is apparently the basis for their conjecture that all NP-complete sets are polynomially isomorphic. We would like to address the question of whether the sets defined by Theorems 1 and 2 are all polynomially isomorphic. To do so, first recall the classical proof from recursion theory that all "complete" sets are recursively isomorphic.

The proof breaks into three parts. First one defines creative sets and proves that all "complete" sets are creative. Second one proves that all creative sets are cylinders[4]. And finally one easily proves that all sets of the same many-one degree that are cylinders are in fact isomorphic. How much of this proof can be carried out in a polynomial setting? Clearly, the last step can be since it is just the basis of Berman and Hartmanis' observation that all "natural" NP-complete sets are polynomially isomorphic. However, to the extent that the remainder of the proof cannot be carried out, it is evidence that the Berman Hartmanis conjecture fails, since, knowing the existence of k-creative sets, all k-creative sets must be cylinders if their conjecture were to hold.

Thus, since the sets defined by Theorems 1 and 2 are already creative, it seems reasonable to ask whether they are cylinders in a polynomial sense.

Definition. A set C is a *polynomial cylinder* if there exists a polynomially computable and polynomially invertible function p, a *padding* function, such that for all x and y, $x \in C \ iff \ p(x,y) \in C$.

With this definition we can try to adapt the recursion theoretic proof to show that all creative sets are cylinders and hence polynomially isomorphic.

Although the standard technique from [Rog-67] does not adapt in a polynomial setting unless the productive function f is both one-one and polynomially invertible, a similar problem in quite a different setting was faced by Schnorr in [Sch-75] where he used a new technique credited to an anonymous referee. This technique has been used again in [MWY-78] on problems similar to Schnorr's, in [M&Y-78] in a different setting, and again in [Dow-78] in a setting similar to that of this paper. The technique does not allow us to produce a polynomial padding function, but it does go part way: If C is a k-creative set for which there is a productive function $f \in P^{(k-1)}$, then we can construct

[4] A set C is a cylinder if it is recursively isomorphic to B x N, for some set B. Therefore a set that is a cylinder has a padding function.

a *pseudo polynomial padding function* p. However, p, lacks polynomial invertibility and is one-one only on the complement of the set:

Theorem 3. Let C be any k-creative set for which there is a productive function $f \in P^{(k-1)}$. Then the set C has a polynomially computable function p such that for all x and y, $x \in C$ iff $p(x,y) \in C$. Furthermore, p is one-one on $\overline{C}$.

Proof. Let S be a standard S_1^2 function; that is, for all e, y, k and x, $\varphi_e(y,k,x) = \varphi_{S(e,y,k)}(x)$. What's more recall that S can be selected such that

$$\Phi_{S(e,y,k)}(x) \leq l(\Phi_e(y,k,x))$$

for a linear function l, which is independent of e, y and k. (See [M&Y-78] for details.)

Suppose that C is any k-creative set and $f \in P^{(k)}$ is a polynomially computable productive function for $\overline{C}$. We can use the recursion theorem to find an index e such that

$$\varphi_e(y,k,x) = \begin{cases} \downarrow & \text{if } (\exists <z,j> < <y,k>)[f(S(e,z,j)) = f(S(e,y,k))] \text{ or } y \in C \\ \uparrow & \textit{otherwise.} \end{cases}$$

Standard facts about well-behaved nondeterministic time measures and about the complexity behavior of the recursion theorem and of S_m^n functions in linearly bounded measures ([M&Y-78]), imply that for all e, y, and k, $W_{S(e,y,k)} \in NP^{(k)}$, provided that the fixed point e is chosen sufficiently large. We claim, in addition, that $f(S(e, ,))$ is the desired padding function. Two things need to be shown,

(i) $(\forall y,k)\ y \in C \ \textit{iff}\ f(S(e,y,k)) \in C$, and

(ii) $f(S(e, ,))$ is one-one on $\overline{C}$.

We begin by showing that $f(S(e, ,))$ is one-one on $\overline{C}$. For the sake of contradiction suppose that $y, z \not\in C$ but $f(S(e,y,k)) = f(S(e,z,j))$ for some k and j. What's more choose z and j to be minimal in the sense that there do not exist z_0 and j_0 such that $<z_0,j_0> < <z,j>$ and $f(S(e,y,k)) = f(S(e,z_0,j_0))$. Now consider $W_{S(e,z,j)}$. We claim that $W_{S(e,z,j)} = \phi$. If not, then there exists x_0 such that $\varphi_e(z,j,x_0)\downarrow$, which implies that there exist $<z_0,j_0> < <z,j>$ and

$$f(S(e,z_0,j_0)) \; = \; f(S(e,z,j)) \; = \; f(S(e,y,k)).$$

But this contradicts the minimality of $<z,j>$. Therefore, $W_{S(e,z,j)} = \phi$ and $S(e,z,j) \notin W_{S(e,z,j)}$. However since f is a productive function for C, we must also have $f(S(e,z,j)) \notin C$.

Now consider $W_{S(e,y,k)}$. By construction $W_{S(e,y,k)} = N$. Therefore, $S(e,y,k) \in W_{S(e,y,k)}$ and thus, $f(S(e,y,k)) \in C$. But our original assumption was that $f(S(e,y,k)) = f(S(e,z,j))$, so we have a contradiction since one can not be an element of C while the other is an element of $\overline{C}$. Therefore $f(S(e,y,k))$ is one-one on $\overline{C}$.

We now need to show that for all y and k,

$$y \in C \;\; iff \;\; f(S(e,y,k)) \in C.$$

Suppose that $y \notin C$. Then $\lambda k.f(S(e,y,k))$ is one-one and thus for all k, $W_{S(e,y,k)} = \phi$. Therefore $S(e,y,k) \notin W_{S(e,y,k)}$ and since f is a productive function for C, $f(S(e,y,k)) \notin C$.

Similarly, suppose that $y \in C$. Then for all k, $W_{S(e,y,k)} = N$. Therefore, $S(e,y,k) \in W_{S(e,y,k)}$ and since f is a productive function for C, $f(S(e,y,k)) \in C$. Thus $f(S(e,\,,\,))$ satisfies the requirements of the theorem. ■

It is now important to notice first, that had f been one-one, p would also be one-one, but, second, that even in this case p would not quite be a padding function that makes C a polynomial cylinder. The problem is that p is not necessarily polynomially *invertible*, and the only obvious way to make p polynomially invertible is for the productive function f itself to be polynomially invertible. But f could have been *any* one-one, polynomially honest, polynomially computable function. The only way for all such f's to be polynomially invertible is for there to be no polynomially computable "one-way" functions, a supposition that is widely believed to be false by cryptographers.

In spite of some effort, we have been unable to show that k-creative sets have polynomially invertible padding functions unless we know *a priori* that the productive functions are not only of low complexity but are also polynomially invertible. Since Theorem 2 guarantees that *every* honest, one-one, polynomially computable function, *invertible or not*, is a productive function we are led to the following conjectures:

Conjecture 1. The k-creative sets are polynomially isomorphic only if polynomial "one-way" functions do not exist.

Since we conjecture that "one-way" functions do exist, we also have

Conjecture 2. The k-creative sets are not all polynomially isomorphic, and hence not all NP-complete sets are polynomially isomorphic - a direct contradiction of the Berman and Hartmanis conjecture.

In any case, the k-creative sets give a new class of NP-complete sets for which the Berman-Hartmanis conjecture seems to fail. (Assuming that not all NP-complete sets are polynomially isomorphic, the "density" of NP-complete isomorphism types is explored in [M&Y-84].)

The difficulty of improving Theorem 3 to make all k-creative sets paddable suggests that not only are not all NP-complete sets isomorphic, but that they are not even all complete under one-one polynomial time reducibilities. On the other hand, the only k-creative sets we know to exist do have one-one productive functions, thus they all admit polynomial padding, and hence they are all complete under one-one polynomial time reductions. This suggests:

Question 1. Do all k-creative sets have one-one productive functions? Are all NP-complete sets complete under one-one polynomial time reductions?

The above results and conjectures suggest many additional questions, at least some of which should be solvable without resolving P *vs* NP. We list a few, the interested reader should have little trouble finding more:

Question 2. In classical recursion theory, all "many-one complete" sets are creative. With our notion of k-creative, the polynomial analogue seems unlikely for NP-complete sets. We would conjecture that not all NP-complete sets are k-creative. In fact, we do not even know whether *any* "natural" NP-complete set is k-creative. Additionally, it would be interesting to know whether there is some other "structurally" defined class of NP-complete sets which are *not* k-creative.

Question 3. What is the *logical* connection between Conjectures 1 and 2? For example, is it possible to prove that NP-complete sets are all isomorphic *iff* "one-way" functions do not exist?

Question 4. The construction of existing k-creative sets (Theorem 2 above) required that the productive functions all be one-one and polynomially honest. Does every k-creative set have a productive function which is one-one and honest?

Question 5. In order to even begin the construction of a pseudo-padding function given in the proof of Theorem 3, we had to assume that the k-creative had a productive function of low complexity (in $P^{(k-1)}$). Does every k-creative set have a productive function in $P^{(k-1)}$? We suspect not.

Question 6. Theorem 3 enables us to show that for many k-creative sets C, $\overline{C}$ can not be *weakly polynomially immune* in the sense of *not* having a subset which is the range of a one-one polynomially computable function, p. On the other hand, the range of this function p need not by polynomially decidable. Thus we ask whether k-creative sets or their complements are *almost polynomially immune* in the sense of not having subsets which are the range of polynomially computable one-one functions with polynomially decidable ranges. A positive answer would imply that such sets are *not* all polynomially isomorphic. In any case, the observation that for many k-creative sets, C, $\overline{C}$ can not be weakly immune shows that proving that every NP-complete set is k-creative is too hard: an affirmative answer implies $P \neq NP$. Finally, we do not know what degree of polynomial immunity, if any, is possible for k-creative sets.

We now return to our discussion of the polynomial analogs of Theorems I and II.

A Second Result on Witness Functions for P $\neq$ NP

Our second result on witness functions is analogous to Theorem II above. It will follow as a corollary to this result that any set that can be polynomially witnessed to be incomplete for NP must be in $NP \cap coNP$.

Theorem 4. Let B be any set and suppose that there is a polynomial witness to the fact that B is not hard for NP. I.e., suppose that there is a set A in NP and a polynomially computable function h which witnesses that A is not polynomially reducible to B. Then B is in $NP \cap coNP$.

In fact, h need only witness that $\bar{A}$ is not in $P^{(1)}$ relative to B. That is, $\bar{A} \not\in P^{(1),B}$.

Proof. Suppose that B is any recursive set for which there is a polynomially computable witness function, h, to the fact that B is not hard for NP. Then the function h must satisfy:

$$\varphi_i^B(h(i)) = 1 \ iff \ \ h(i) \in A$$

for any program i which witnesses that $W_i^B \in P^{(1),B}$. Observe that for *any* set B we can construct a polynomially computable function g such that:

$$\varphi_{g(i)}^B(z) = \begin{cases} 1 & \text{if } i \in B \\ \uparrow & otherwise. \end{cases}$$

For any reasonable choice of g, $g(i)$ is a program which witnesses that $W_{g(i)}^B \in P^{(1),B}$. However, we now have that

$$i \in B \ iff \ \ W_{g(i)}^B = \{0, 1, 2, \cdots \} \ iff \ \ h(g(i)) \in W_{g(i)}^B \ iff \ \ h(g(i)) \in A.$$

Thus $i \in B$ if and only if $h(g(i)) \in A$, showing that B is in NP.

To complete the proof, we must show that under the same conditions $\bar{B}$ is in NP. But the proof is exactly the same: in the above proof simply take every occurence of B that is not as superscript, and replace it with $\bar{B}$. ∎

It is worth noting in the above proof we did not need that h is a function. It was enough to have h be any nondeterministic polynomial process such that any value, $h(i)$, that it produces satisfies,

$$W_i^B \in P^{(1),B} \quad implies \quad [\varphi_i^B(h(i)) = 1 \ iff \ \ h(i) \in A].$$

REFERENCES

[BGS-75] Baker, T., J. Gill and R. Solovay, "Relativization of the P = NP question," *SIAM J. Comput.* 4 (1975), pp. 431-444.

[B&H-77] L. Berman and J. Hartmanis, "On isomorphisms and density of NP and other complete sets," *SIAM J. Comp.* **1** (1977), pp. 305-322.

[C&M-81] P. Chew and M. Machtey, "A note on structure and looking back applied to the relative complexity of computable functions," *J. Comput. Systems Sci.* **22** (1981), pp. 53-59.

[Dow-78] M. Dowd, "On isomorphism," unpublished manuscript, 1978.

[Jos-83] D. Joseph, "Polynomial time computations in models of ET," *J. Comput. Systems Sci.* **26** (1983), pp. 311-338.

[Koz-80] Kozen, D., "Indexings of subrecursive classes," *Theor Comput Sci* **11** (1980), pp. 277-301.

[K&M-81] K. Ko and D. Moore, "Completeness, approximation and density," *SIAM J Comput* **10** (1981), pp. 787-796.

[K&M-80] D. Kozen and M. Machtey, "On relative diagonals," *Technical Report*, IBM T J Watson Research Center, Yorktown Heights, NY, (1980).

[Lad-75] R. Ladner, "On the structure of polynomial time reducibility," *J. ACM*, **2** (1975), pp. 135-171.

[MWY-78] M. Machtey, K. Winklmann, and P. Young, "Simple Godel numberings, isomorphisms, and programming properties," *SIAM J. Comp.*, **7** (1978), pp. 39-60.

[M&Y-78] M. Machtey and P. Young, *An Introduction to the General Theory of Algorithms*, Elsevier-North Holland, 1978.

[O'D-79] M. O'Donnell, "A programming language theorem that is independent of Peano arithmetic," *Proc. of the 11th Symp. on the Theory of Comput.* (1979), pp. 176-188.

[Rog-67] H. Rogers, *Recursive Functions and Effective Computability*, McGraw-Hill, 1967.

[Sch-75] C. Schnorr, "Optimal enumerations and optimal Godel numberings," *Math Systems Theory* **8** (1975), pp. 182-191.

[Sch-82] U. Schoning, "A uniform approach to obtain diagonal sets in complexity classes," *Theor Comput Sci* **18** (1982), pp. 95-103.