RC 8184 (#35583) 4/1/80
Computer Science 11 pages

Research Report

ON RELATIVE DIAGONALS

Dexter Kozen
IBM Thomas J. Watson Research Center
Yorktown Heights, New York 10598

Michael Machtey
Purdue University
West Lafayette, Indiana 47907

LIMITED DISTRIBUTION NOTICE

This report has been submitted for publication outside of IBM and will probably be copyrighted if accepted for publication. It has been issued as a Research Report for early dissemination of its contents. In view of the transfer of copyright to the outside publisher, its distribution outside of IBM prior to publication should be limited to peer communications and specific requests. After outside publication, requests should be filled only by reprints or legally obtained copies of the article (e.g., payment of royalties).

IBM Research Division
San Jose · Yorktown · Zurich

RC 8184 (#35583) 4/1/80
Computer Science 11 pages

ON RELATIVE DIAGONALS

Dexter Kozen
IBM Thomas J. Watson Research Center
Yorktown Heights, New York 10598

Michael Machtey†
Purdue University
West Lafayette, Indiana 47907

Abstract. A diagonal that separates the complexity classes **C** and **D** is said to be *relative* if its relativized version with respect to an oracle A separates $\mathbf{C}^A$ and $\mathbf{D}^A$ whenever $\mathbf{C}^A \neq \mathbf{D}^A$. It is shown that (i) if **R** is complete for **D** then **R** is a relative diagonal, but (ii) unlike the unrelativized case, computable witness functions for $\mathbf{C} \neq \mathbf{D}$ do not always exist. In particular, there is no computable witness function for the relativized $\mathbf{P} =? \mathbf{NP}$ question. The proof of (ii) extracts the essence of a construction appearing in several papers in relativized complexity involving what Angluin calls *oracle properties*. We point out that the significance of oracle properties lies in their relation to the topological property of meagerness.

†This research was done during the author's tenure as visiting faculty, IBM T.J. Watson Research Center, Yorktown Heights, New York.

Introduction

The relativization results of Baker, Gill, and Solovay [BGS] have been taken to suggest that the technique of diagonalization cannot separate **P** and **NP**. In their words,

> It seems unlikely that ordinary diagonalization methods are adequate for producing an example of a language in NP but not in P; such diagonalizations, we would expect, would apply equally well to the relativized classes, implying a negative answer to all relativized P =? NP questions, a contradiction.

Let $C = \{ \phi_x \mid x \in N \}$ be an indexed class of recursive sets (for example, C might be **P**, the class of polynomial-time computable sets, indexed by Turing machines with polynomial time counters). In [K], a *diagonal* over C was defined to be a total recursive function $\mathbf{diag}_h$, defined with respect to a computable function h, by

$$\mathbf{diag}_h(x) = \neg\phi_{h(x)}(x) \tag{1}$$
$$= \textbf{if } \phi_{h(x)}(x) = 0 \textbf{ then } 1 \textbf{ else } 0$$

where h is *functionally onto*, i.e. for all i there exists an x such that $\phi_{h(x)} = \phi_i$. The definition was meant to model a simple form of the technique of diagonalization: on input x, compute the description h(x) of a program to simulate, simulate it on input x, then do something different. The restriction that h is functionally onto says that $\mathbf{diag}_h$ diagonalizes away from every set in C at some point, insuring that $\mathbf{diag}_h \notin C$.

It was shown in [K] that *every* recursive set R not in C is a diagonal. For example, if $\mathbf{P} \neq \mathbf{NP}$, then $\mathbf{sat} = \mathbf{diag}_h$ for some recursive function h, where **sat** is the NP-complete Boolean satisfiability problem. Thus, in a certain well-defined sense, if $\mathbf{P} \neq \mathbf{NP}$ is provable at all, then it is provable by diagonalization. This says that the technique of diagonalization cannot be discarded out of hand, as suggested by [BGS].

In this note we attempt to resolve these different views by taking a closer look at diagonalization relative to an oracle A. We wish to capture the notion of diagonalizations which "apply equally well to the relativized classes." We investigate three formal interpretations of this notion: *weak relative diagonals*, *strong relative diagonals*, and *uniform witness functions*. The three interpretations coincide in the unrelativized case.

A *weak relative diagonal* is the most direct generalization of (1). It models the following diagonalization method: on input x and oracle A, compute the description h(A,x) of a program to simulate, then simulate it on input x and oracle A, and do something different. Whenever

A is such that $C^A \neq D^A$, function h(A,) must be functionally onto the class C^A, so that the diagonalization successfully diagonalizes away from all functions in C^A.

A *strong relative diagonal* is exactly the same except that the oracle A is not allowed in the computation of h. This seems to be closer to the intent of [BGS].

The third interpretation involves *uniform witness functions*, the relativized analog of witness functions. Witness functions arise in connection with statements of the form

(2) $\forall x \exists y\, P(x,y)$.

One way to prove (2) is to give a recursive function f and demonstrate that P(x,f(x)) holds for all x. Such an f is called a *witness function* or *Skolem function*. The statement **P ≠ NP** is a statement of the form (2):

$$\forall x \exists y\, \mathbf{sat}(y) \neq \phi_x(y) .$$

Note, however, that if **P ≠ NP** then a computable witness function f exists, and can be constructed explicitly: on input x, f runs ϕ_x and **sat** in parallel on inputs 0,1,2,... and takes as its value the first input on which they differ; such an input must exist, otherwise **P = NP**. In general, if R is a total recursive function not in **C**, then there exists a computable witness function f attesting to this fact.

Thus in the unrelativized case, the situation is degenerate. Whenever $R \notin C$, a witness function f exists, and once this is known, a function h can be constructed as a functional inverse of f, making $R = \mathbf{diag}_h$. This construction is given in [K]. In the case of computation relative to an oracle A, the situation is more interesting. In this paper we show, for **C**, **D** classes of total recursive operators,

(i) Every recursive operator R complete for **D** is a strong relative diagonal. This says that if **P ≠ NP**, then the relativized **sat** problem is a strong relative diagonal separating the relativized classes $P^{(\,)}$ and $NP^{(\,)}$. The interesting part of this result is that weak and strong relative diagonals are equivalent in power, i.e. the oracle is not needed in the computation of the description of the machine to simulate.

(ii) Unlike the unrelativized case, uniform witness functions separating two operator classes do not necessarily exist. Specifically, they do not exist for any pair **C**, **D** such that **D – C** contains what Angluin calls an *oracle property* [A] and such that there exists an oracle A making $C^A = D^A$. In particular, there is no uniform witness function separating $P^{(\,)}$ and

$NP^{(\ )}$. The main lemma for this result extracts the essence of a construction appearing in several papers in relativized complexity [A,BG,BS] involving oracle properties. We point out that the significance of oracle properties lies in their relationship to the topological property of meagerness [Me].

These two results say that diagonals and witness functions are less closely related than suggested by [K]. Result (i) is for those who take the liberal view that diagonalization should admit all constructions of the form (1). Result (ii) on the other hand corroborates the intuition of [BGS], and is for those who take the more conservative view that diagonalization must involve the construction of a computable witness function.

Notation

A natural number $x \in N$ is identified with the x^{th} string in $\{0,1\}^*$ in lexicographic order. $|x|$ represents the length of string x. Sets and their characteristic functions are identified, so that $A(x) = 1$ iff $x \in A$. A *partial set* is a function $A:N \to \{0,1,\perp\}$. The *domain* of a partial set A is the set of x for which $A(x) \neq \perp$. A partial set is *total* if its domain is N. The empty set is not to be confused with the completely undefined characteristic function; the empty set is total. We say B is an *extension* of A and write $A \sqsubseteq B$ if the domain of A is a subset of the domain of B and A and B agree on the domain of A. 2^A denotes the power set of A.

An *oracle Turing machine* is denoted R or R(,). This notation is also used to denote the partial recursive operator computed by R. If A is a set, R(A,) denotes either the machine R equipped with oracle A or the partial recursive (in A) function computed by this machine. R(A,x) denotes the result of applying R(A,) to input x. R is *total* if $R(A,x) \neq \perp$ for all $A \in 2^N$ and $x \in N$.

C, D will be used to denote classes of total recursive functions or operators, and we will always assume C has a computable indexing $C = \{ \phi_x \mid x \in N \}$ satisfying certain fundamental effective closure properties. For one, we require that C be closed under (effective) finite table patching [A,BG,CM]. Other properties required of C, D will be made explicit as needed.

Let C, D be classes of operators, $C \subseteq D$. An operator S(,) is usually said to be *complete* for D with respect to an appropriate reducibility relation if $S \in D$ and every element in D can be reduced to S under that reducibility relation. The only property of completeness we shall need is that for any oracle A, $S(A,) \in C^A$ iff $D^A = C^A$, so in order to avoid discussing reducibilities we shall deviate from the standard and call S *complete* (for D with respect to C) if $S \in D$ and for all oracles A, if $S(A,) \in C^A$ then $D^A = C^A$.

Meagerness

Let A be a partial set with finite domain. The set of total extensions of A is called a *basic open set*. The basic open sets form a basis for a topology on 2^N; the resulting space is often called the *Cantor space*.

A set $N \subseteq 2^N$ is *nowhere dense* if, for any open set U, there is an open set $V \subseteq U$ disjoint from N. Equivalently, N is nowhere dense if for any partial set A with finite domain, there is a partial set B with finite domain extending A such that no total extension of B lies in N. Mehlhorn defines the set N to be *effectively nowhere dense* if the function $A \rightarrow B$ is computable. Subsets and finite unions of nowhere dense sets are again nowhere dense. A set is *meager* if it is a countable union of nowhere dense sets. Subsets and countable unions of meager sets are meager.

Intuitively, nowhere dense sets and meager sets are sparse. This is established in the following useful theorem:

Theorem (Baire Category Theorem). If M is meager, then any open set contains a point not in M.

This is proved in Mehlhorn's paper [Me] for the effective case; a proof of the noneffective version may be found in any introductory topology text.

Oracle properties and their relation to meagerness

The motivation for *oracle properties*, as expressed by Angluin [A], is that

> In several of the proofs concerning relativized complexity classes, it seems natural to view the oracle machines as attempting to recognize certain properties of the oracle set, where the particular input string serves only to select a certain portion of the oracle set.

A common example is the operator

$$R(A,x) = 1 \text{ iff } \exists y \in A \ \ |y| = |x| \ , \tag{3}$$

first used to make $P^A \neq NP^A$ [BGS]. To capture the idea formally, Angluin defined an *oracle property* to be a sequence Q_n, $n \in N$, where $Q_n \subseteq 2^{\Sigma^n}$, and a related recognition problem

$$R(A,) = \{ x \in \Sigma^* \mid A \cap \Sigma^{|x|} \in Q_{|x|} \}.$$

That is, the string x selects a family of distinguished subsets of $\Sigma^{|x|}$, namely $Q_{|x|}$; the input is accepted if the set of strings of A of length $|x|$ is one of these distinguised subsets. She then proved Corollary 6 below for the special case $C = \Pi_2^{p,(\ )}$ ([A], Lemma 3.1).

The key attribute of oracle properties, used in [A,BS,BG], is that *the value of* R(A,x) *does not depend on small elements of* A *for arbitrarily large* x. In other words, for each y there are only finitely many inputs x for which R(A,x) queries the oracle on y, and moreover the bound is independent of A. This observation leads to a more general definition of oracle properties.

Definition 4. An *oracle property* is a total recursive operator R for which there exists a total function $g:\mathbf{N} \to \mathbf{N}$ satisfying the two properties

(4.1) $\quad \liminf g(x) = \infty$

(4.2) $\quad$ if $A(y) = B(y)$ for all $y \geq g(x)$, then $R(A,x) = R(B,x)$.

Condition 4.1 says that g is unbounded from below. Together the conditions 4.1 and 4.2 say that R does not depend on small oracle elements for arbitrarily large inputs.

Any such R has a matching upper bound G such that if $A(y) = B(y)$ for all $y \leq G(x)$, then $R(A,x) = R(B,x)$. This is because the set $\{ y \mid \exists A\ R(A,x)$ queries A on $y \}$ has a maximum element, by König's Lemma. Thus g and G together give a "window" through which R is allowed to look at the oracle. Note that G is always computable, but g need not be.

The following result gives the significance of oracle properties in terms of meagerness.

Proposition 5. Let R be an oracle property, and let

$$A_i = \{ A \mid R(A,\ ) = \phi_i(A,\ ) \},$$
$$A = \{ A \mid R(A,\ ) \in C^A \} = \cup_i A_i.$$

The following conditions are equivalent:

(i) $R \notin C$

(ii) for all i, the set A_i is nowhere dense

(iii) the set A is meager.

Proof. (i) $\to$ (ii): If A_i were not nowhere dense, then there would exist a partial set A with finite domain such that every partial set B with finite domain extending A has a total extension in A_i. We show that this assumption contradicts $R \notin C$.

Let g and G be as in Definition 4. We describe the computation of an operator $\phi_j \in C$ on input (B,x) and show that $\phi_j = R$.

In case $g(x) > \sup(\text{domain}(A))$, $\phi_j(B,x)$ simulates $\phi_i(C,x)$, where

$$C(y) = A(y) \text{ if } y \text{ is in the domain of } A,$$
$$B(y) \text{ otherwise.}$$

In other words, when ϕ_i would query the oracle on some element outside the domain of A, ϕ_j consults B; on queries on which A is defined, ϕ_j consults a table in its finite control. Then

$$\phi_j(B,x) = \phi_i(C,x) = R(C,x);$$

but

$$R(C,x) = R(B,x)$$

since C(y) and B(y) agree on all $y \geq g(x)$.

In case $g(x) \leq \sup(\text{domain}(A))$, $\phi_j(B,x)$ immediately queries the oracle on all elements $\leq G(x)$ and computes R(B,x) directly.

ϕ_j need not compute g or G (recall g need not even be computable). A is fixed, so ϕ_j can keep in its finite control the least y such that $g(z) > \sup(\text{domain}(A))$ for all $z \geq y$ for comparison against its input x. Likewise, it can keep in its finite control the values of G(x) for all x such that $g(x) \leq \sup(\text{domain}(A))$. $\phi_j \in C$ by the assumption that C is closed under finite table patching.

(ii) $\rightarrow$ (iii) follows from the definition of meagerness.

(iii) $\rightarrow$ (i): If $R \in C$ then $\{ A \mid R(A,) \in C^A \} = 2^{\Sigma^*}$. But this contradicts the Baire Category Theorem. □

Corollary 6. $\forall A\, \exists i\, R(A,) = \phi_i(A,)$ iff $\exists i\, \forall A\, R(A,) = \phi_i(A,)$.

Almost exactly the same construction appears in the paper of Bennett and Gill [BG] in which it is proved that, relative to a random oracle, $P \neq NP$ with probability 1 (in symbols, $\Pr(\{ A \mid P^A \neq NP^A \}) = 1$). Their Condition 1 expresses the condition of being an oracle property, and their Lemma 1 can be restated:

Proposition 7 [BG]. Let R be an oracle property and let A_i and A be as in Proposition 5. The following conditions are equivalent:

(i) there exists an ε such that for all i, $\Pr(A_i) \leq 1 - \varepsilon$

(ii) for all i, $\Pr(A_i) = 0$

(iii) $\Pr(A) = 0$.

Relative diagonals and uniform witness functions

Let **C**, **D** be classes of total recursive operators, $\mathbf{C} \subseteq \mathbf{D}$, $\mathbf{C} \neq \mathbf{D}$, and let **C** have computable indexing $\mathbf{C} = \{ \phi_x \mid x \in N \}$. Recall that an operator S(,) is called *complete* (for **D** with respect to **C**) if $S \in \mathbf{D}$ and for all A, $S(A,) \in \mathbf{C}^A$ implies $\mathbf{C}^A = \mathbf{D}^A$. The operator (3) is complete for $\mathbf{NP}^{(\ )}$ with respect to $\mathbf{P}^{(\ )}$ [BGS].

Definition 8. A *weak relative diagonal* for **C** and **D** is a total recursive operator of the form

$$\mathbf{wrd}_h(A,x) = \neg \phi_{h(A,x)}(A,x)$$

where h is a total recursive operator such that whenever $\mathbf{C}^A \neq \mathbf{D}^A$, h(A,) is functionally onto the class $\mathbf{C}^A$, i.e.

$$\forall i \, \exists x \; \phi_{h(A,x)}(A,) = \phi_i(A,) \; . \; \square$$

A *strong relative diagonal* is the same, except that the oracle may not be used in the computation of h:

Definition 9. A *strong relative diagonal* for **C** and **D** is a total recursive operator of the form

$$\mathbf{srd}_h(A,x) = \neg \phi_{h(x)}(A,x)$$

where h is a total recursive function such that whenever $\mathbf{C}^A \neq \mathbf{D}^A$, h is functionally onto the class $\mathbf{C}^A$, i.e.

$$\forall i \, \exists x \; \phi_{h(x)}(A,) = \phi_i(A,) \; . \; \square$$

Let S(,) be complete for **D** with respect to **C**.

Definition 10. A *uniform witness function* for **C** and **D** is a total recursive operator f(,) such that for any oracle A, if $C^A \neq D^A$ then f(A,) bounds witnesses for the assertion that $S(A,) \notin C^A$; i.e.

$$\forall x\, \exists y \leq f(A,x)\ \phi_x(A,y) \neq S(A,y)\ .\ \square$$

Clearly, for any fixed A such that $C^A \neq D^A$, there exists an f such that f(A,) is a witness function for $S(A,) \notin C^A$. This is proved in exactly the same way as the unrelativized case. Definition 10 asks for an f that works *uniformly* in A.

Main results

Let **C**, **D** be as in Definitions 8-10.

Theorem 11. If R is complete for **D** with respect to **C**, then R is a strong relative diagonal.

Proof. Let R be complete. We wish to construct an h such that $R = \mathbf{srd}_h$ and such that h is functionally onto C^A whenever $R(A,) \notin C^A$.

First, let e be the function defined recursively by

$$e(x) = \mu i.(\exists A\ R(A,x) \neq \phi_i(A,x) \text{ and } \forall y < x\ e(y) \neq i)\ .$$

Here μi denotes "the least i such that". Now take $h(x) = r(e(x),x)$ where r(i,x) is the index of the recursive operator

$$\phi_{r(i,x)}(B,y) = \textbf{if } x = y \textbf{ then } \neg R(B,y) \textbf{ else } \phi_i(B,y)\ .$$

We claim that h is a total recursive function. Assume that e(y) is defined for all $y < x$. The predicate $\exists A\ R(A,x) \neq \phi_i(A,x)$ in the definition of e(x) is decidable, since by König's Lemma there is a bound, recursive in i and x and independent of A, on the set of oracle queries that R and ϕ_i make on input x. Further, there are infinitely many i such that $\exists A\ R(A,x) \neq \phi_i(A,x)$, since **C** is closed under finite table patching. Therefore e(x) exists and is computable. Under very reasonable restrictions on the indexing of **C**, the function r is total and computable, therefore h is.

Next we show that $R = \mathbf{srd}_h$. For any A, x,

$$\mathbf{srd}_h(A,x) = \neg\phi_{h(x)}(A,x), \quad \text{by definition of } \mathbf{srd}_h,$$

$= \neg\phi_{r(e(x),x)}(A,x)$, by definition of h,

$= \neg$(**if** x = x **then** $\neg$R(A,x) **else** $\phi_{e(x)}(A,x)$), by definition of r,

$= R(A,x)$.

Finally, we claim that h is functionally onto C^A whenever $R(A,\ ) \notin C^A$. This will establish the result. Suppose A is such that $R(A,\ ) \notin C^A$. Let $i \in N$ be arbitrary. For infinitely many x, $R(A,x) \neq \phi_i(A,x)$, for if R(A,x) were to differ from $\phi_i(A,x)$ for only finitely many x, then $R(A,\ ) \in C^A$ by finite table patching. Thus i satisfies the predicate $\exists A\ R(A,x) \neq \phi_i(A,x)$ for infinitely many x, so that eventually e(x) = i for some x. But then for any y,

$\phi_{h(x)}(A,y)$ = **if** x = y **then** $\neg$R(A,y) **else** $\phi_{e(x)}(A,y)$

= **if** x = y **then** $\phi_i(A,y)$ **else** $\phi_{e(x)}(A,y)$, since $R(A,x) \neq \phi_i(A,x)$,

= **if** x = y **then** $\phi_i(A,y)$ **else** $\phi_i(A,y)$, since e(x) = i,

$= \phi_i(A,y)$.

Thus $\phi_{h(x)}(A,\ ) = \phi_i(A,\ )$. Since i was arbitrary, h is functionally onto C^A. □

Theorem 12. If **D** – **C** contains an oracle property, and if there exists an A such that $C^A = D^A$, then no uniform witness function for $C \neq D$ exists.

Remark. The oracle property (2) is in $NP^{(\ )} - P^{(\ )}$ and there exists an A such that $P^A = NP^A$ [BGS], thus **P** and **NP** satisfy the premises of the theorem.

Proof. Let R be an oracle property, $R \in D - C$. Let S(,) be complete. The complexity of the set

$$A = \{ A \mid C^A = D^A \}$$

is at most Σ_2^P, since membership in *A* can be expressed

$$\exists x\ \forall y\ \ S(A,y) = \phi_x(A,y)\ .$$

We claim that S has a uniform witness function iff *A* is Σ_1^P.

($\rightarrow$) If f is a uniform witness function, then membership in A is equivalent to

$$\exists x\ \ \forall y \leq f(A,x)\ \ S(A,y) = \phi_x(A,y)\ .$$

This is a Σ_1^P predicate, since the second quantifier is bounded.

($\leftarrow$) If A is Σ^0_1 then it is equivalent to a predicate of the form

$$\exists y\ H(A,y)\ ,$$

where H is a total recursive operator. To compute f(A,x), enumerate y = 0,1,2,..., and for each such y, compute S(A,y) and $\phi_x(A,y)$ to determine if $S(A,y) \neq \phi_x(A,y)$. In parallel, compute H(A,y). Either $S(A,\ ) \in C^A$, in which case H(A,y) for some y, or not, in which case some y will eventually be found such that $S(A,y) \neq \phi_x(A,y)$. In the former case take f(A,x) = 0, and in the latter take f(A,x) to be the least y such that $S(A,y) \neq \phi_x(A,y)$. If A is such that $S(A,\ ) \notin C^A$, H(A,y) will never hold, thus f(A,x) will give a y such that $S(A,y) \neq \phi_x(A,y)$.

It is well known that every Σ^0_1 set is open. To see this, let $A = \{ A \mid \exists y\ H(A,y) \}$, where H is a total recursive operator, and let $A \in A$. Then there is a y such that H(A,y). Let B be the restriction of A to the set of elements of N queried by H(A,y). Then $B \sqsubseteq A$ and B has finite domain, and H(C,y) for all total extensions C of B, so the set of total extensions of B is a basic open neighborhood of A entirely contained in A.

Now suppose S has a uniform witness function. Since $R \in D$,

$$\{ A \mid C^A = D^A \} \subseteq \{ A \mid R(A,\ ) \in C^A \}\ .$$

But by the claims above, the former set is nonempty and open, and by Proposition 5, the latter set is meager. This contradicts the Baire Category Theorem. □

References

[A] Angluin, D., "On counting problems and the polynomial time hierarchy," *Theor. Comput. Sci.*, to appear.

[BG] Bennett, C.H. and J. Gill, "Relative to a random oracle, $P^A \neq NP^A \neq coNP^A$ with probability 1," manuscript, IBM Research, Yorktown Heights, New York, 1979.

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

[BS] Baker, T.P. and A.L. Selman, "A second step toward the polynomial time hierarchy," *Proc. 17th IEEE Symp. on Foundations of Comput. Sci.*, Oct. 1976, 71-75; also *Theor. Comput. Sci.*, to appear.

[CM] Chew, P. and M. Machtey, "A note of structure and looking back applied to the relative complexity of computable functions," manuscript, Dept. of Comp. Sci., Purdue Univ., July 1979.

[G] Gill, J.T., "Axiomatic independence of the question P=NP?", Elec. Eng. Dept., Stanford University, 1972.

[K] Kozen, D.C., "Indexings of subrecursive classes," *Proc. 10th ACM Symp. on Theory of Computing* (1978), 287-295; also *Theor. Comput. Sci.*, to appear.

[Ma] Machtey, M., "Remarks on recursion vs. diagonalization," manuscript, Dept. of Comp. Sci., Purdue Univ., Nov. 1977.

[Me] Mehlhorn, K., "On the size of sets of computable functions," *Proc. 14th Symposium on Switching and Automata Theory*, Oct. 1973, 190-196.