Witness-Isomorphic Reductions and Local Search

Sophie Fischer*    Lane Hemaspaandra†    Leen Torenvliet‡

May 6, 1996

Abstract

We study witness-isomorphic reductions, a type of structure-preserving reduction between $NP$ decision problems. We completely determine the relative power of the different models of witness-isomorphic reduction, and we show that witness-isomorphic reductions can be used in a uniform approach to the local search problem.

1 Introduction

The “natural” $NP$ complete decision problems are very much alike. They not only are of the same complexity, but also are in the same polynomial-time isomorphism degree [BH77], and the reductions/isomorphisms between many of these problems are parsimonious [Sim75]. One would expect that such a tight connection between $NP$-complete problems “of interest” would lead to an integrated approach when dealing with the closely related optimization problems. This however is not common practice in operations research. Indeed, typically, for each individual $NP$ optimization problem new techniques and heuristics are invented. It seems that though existing reductions show a tight connection between solutions to the problem, the connection is not strong enough still to allow translation of search techniques from one problem to another.

*IBM, Watsonweg 2, 1423 ND Uithoorn, The Netherlands. Supported in part by grant NWO/SION 612316801.
†Department of Computer Science, University of Rochester, Rochester, NY 14627. Supported in part by grants NSF-CCR-8957604, NSF-INT-9116781/JSPS-ENGR-207, NSF-CCR-9322513, and NSF-INT-9513368/DAAD.315\PRO\fo-ab. Work done in part while visiting the Tokyo Institute of Technology, the University of Electro-Communications—Tokyo, the University of Amsterdam, and Friedrich-Schiller-Universität Jena.
‡Department of Computer Science, University of Amsterdam, 1018 TV Amsterdam, The Netherlands. Supported in part by HC&M grant ERB4050PL93-0516.
A first step towards tightening the relation between problems further than parsimonious reductions can, was taken by Lynch and Lipton [LL78] who defined “structure-preserving reductions.” This notion was later applied to optimization problems by Ausiello, D’Atri and Protasi [ADP80]. A structure-preserving reduction $f$ is accompanied by a polynomial-time computable function $g$ that computes from each witness for a given $x$ a witness for $f(x)$. More recently, Agrawal and Biswas [AB92] studied the complementary approach. They stated a problem $A$ to have a “universal relation” if for any problem $B$ reduced to $A$ a witness for $x \in B$ can be computed from a witness for $f(x) \in A$.

In this paper we further study the existence of reductions that preserve the properties of the witness spaces. Instead of just asking that the reduction preserves the number of solutions, we require an isomorphism between the witnesses. We will see that even this extremely demanding reducibility notion can indeed often link the relations (witness schemes) that define $NP$-complete problems. Yet, surprisingly, there exist very natural witness schemes for problems in the isomorphism degree of $Sat$ for which it is unlikely that such a tight connection between these problems and $Sat$ exists.

Such witness-isomorphic reductions (for short, wi-reductions) can be used to obtain insight into the structural properties of local search problems. Local search is a technique for optimization problems introduced by Johnson, et al. [JPY88]. Instead of searching for a globally optimal solution, local search techniques try to improve a given initial solution until a local optimum is reached. Fischer [Fis95a] defines a class of decision problems related to local search and shows these problems $NP$-complete. In Section 4 we show that witness-isomorphic reductions exists between standardized witnessing relations for some (yet not all, as we see in Section 5) of these problems. We infer from this that a local search strategy for one problem can be polynomially translated into a local search strategy for others.

Many different witnessing schemes can define an $NP$ decision problem and the witness-isomorphic reductions in this paper are defined in terms of these relations rather than in terms of the problem. Our classification of problems through the tool of witness-isomorphic reductions might be more satisfying if we could frame witness-isomorphic reductions as a property of problems rather than a property of the relations. One way of achieving such a goal would be to “quantify out” the relation. For problems $A$ and $B$ one might be able to show that witness-isomorphic reductions exist regardless of which witness schemes are chosen to define $A$ and/or $B$. In Section 3 we study possible approaches along this line, and determine their computational power. We conclude that some are trivial and that amongst the remaining
ones there is no compelling reason to prefer one over the other. This section also provides some new observations on the question of \( \#P \) completeness of \( NP \) counting problems. In particular, \( \#P \) is often thought of as the counting version of \( NP \). However Valiant \cite{Val79} has shown that not only \( NP \)-complete problems have \( \#P \) hard counting versions. We look at the flip question: Do all \( NP \)-complete problems have (only) \( \#P \)-complete counting versions? We give a structural condition sufficient to ensure that the answer to this question is “no.”

2 Definitions and Notation

Sets are denoted by capital letters and are subsets of \( \Gamma^* \), where \( \Gamma = \{0, 1\} \). The cardinality of a set \( A \) is denoted as \( |A| \). Strings are denoted as small letters \( x, y, u, v, \ldots \) and are elements of \( \Gamma^* \). \( NP \) is the class of all sets that can be recognized by nondeterministic Turing machines running in polynomial time. We will use the following standard equivalent definition of \( NP \). A set \( A \) is in \( NP \) if and only if there exists a polynomial-time relation \( R_A \) and a polynomial \( p_A \) such that \( x \in A \iff \exists y \cdot p_A(|x|) \land R_A(x, y) \).

The relation \( R_A \) is called a witness scheme for \( A \), and a string \( y \) for which \( R_A(x, y) \) is called a witness for \( x \in A \). Via padding, each set in \( NP \) has a countably infinite number of witness schemes. We will often assume that the polynomial \( p_A \) is given and not mention it separately.

2.1 Witness-Isomorphic Reductions

**Definition 2.1** Let \( A \) and \( B \) be languages in \( NP \) and let \( R_A \) be a witness scheme for \( A \) and let \( R_B \) be a witness scheme for \( B \). We will say that \((A, R_A) \) reduces (polynomial-time) witness-isomorphically to \((B, R_B) \) \( (A, R_A) \leq_{wi} (B, R_B) \) if and only if there exist polynomial-time computable and polynomial-time invertible functions \( f \) and \( g \) such that:

1. \( (\forall x)[x \in A \iff f(x) \in B] \). That is, \( A \leq^P_m B \) via \( f \).
2. \( \forall x, y : \) if \( R_A(x, y) \) then \( (\exists z)[g(\langle x, y \rangle) = \langle f(x), z \rangle \land R_B(f(x), z)] \).
3. \( \forall x, y_1 \neq y_2 : \) if \( R_A(x, y_1) \) and \( R_A(x, y_2) \) then \( g(\langle x, y_1 \rangle) \neq g(\langle x, y_2 \rangle) \).
4. \( \forall x, w, z : \) if \( f(x) = w \) and \( R_B(w, z) \), then \( (\exists y)[R_A(x, y) \land g(\langle x, y \rangle) = \langle w, z \rangle] \).

We say, in the above situation, that \((A, R_A) \leq_{wi} (B, R_B) \) via \( f \) and \( g \).
Let us explain what the above definition intuitively means. Informally (as we will here speak of witnesses when we in fact should speak of witness-string pairs), we are merely speaking of an invertible many-one polynomial-time reduction \( f(x) \) from \( A \) to \( B \) that has an additional property. The additional property is that there is an invertible polynomial-time function \( g \) that, individually for each \( x \in A \), creates a bijection between the set of witnesses under \( R_A \) for \( x \in A \) and the set of witnesses under \( R_B \) for \( f(x) \in B \). The reason we emphasize the word “set” is that what we are speaking of here is more related to what is often referred to as a “set isomorphism” rather than to what is often referred to as a “language isomorphism.” The distinction is as follows: We do not require that \( g \) establish a tight correspondence between the non-witnesses of \( x \) and the non-witnesses of \( f(x) \)—in fact we do not require any particular behavior at all from \( g \) in terms of where it maps non-witnesses (except that the behavior must not destroy invertibility). To make our notion as clear as possible, as this is the central concept of the paper, we give an alternate definition that, it is not hard to see, is equivalent to the above definition.

**Definition 2.2** For a binary relation \( R \) and a set \( D \) let \( R[D] \) denote \( R \cap (D \times \text{range}(R)) \) (see, e.g., [Sup72]). Let \( A \) and \( B \) be languages in \( \text{NP} \) and let \( R_A \) be a witness scheme for \( A \) and let \( R_B \) be a witness scheme for \( B \). We will say that \( (A, R_A) \) reduces (polynomial-time) witness-isomorphically to \( (B, R_B) \) if and only if there exist polynomial-time computable and polynomial-time invertible functions \( f \) and \( g \) such that:

1. \( (\forall x)[x \in A \iff f(x) \in B] \). That is, \( A \leq_w^p B \) via \( f \).
2. \( (\forall x)[|R_A|(|x|) = |R_B|(|f(x)|) \land g(R_A(|x|)) = R_B(|f(x)|)] \).

We say, in the above situation, that \( (A, R_A) \leq_w^i (B, R_B) \) via \( f \) and \( g \).

Based on wi-reductions, a notion of witness-isomorphic isomorphism can be defined. Just as in the case of many-one reductions and p-isomorphism, we can find sufficient conditions for two pairs of sets with associated witness schemes to be wi-isomorphic. A function is *length increasing* if the length of its output is greater than the length of its input. A function is called *1-invertible* if it is 1-1, and its inverse can be computed in polynomial time.

**Definition 2.3** Let \( A \) and \( B \) be two sets in \( \text{NP} \) and let \( R_A \) be a witness scheme for \( A \) and let \( R_B \) be a witness scheme for \( B \). The pair \((A, R_A)\) is wi-isomorphic to \((B, R_B)\), notated \( (A, R_A) \equiv_{wi} (B, R_B) \), if and only if there are functions \( f \) and \( g \) such that \( (A, R_A) \leq_w (B, R_B) \) via \( f \) and \( g \) (in the sense of Definition 2.1) and \((B, R_B) \leq_w (A, R_A) \) via \( f^{-1} \) and \( g^{-1} \).
Theorem 2.4 Let $A$ and $B$ be two sets in $NP$ and let $R_A$ be a witness scheme for $A$ and let $R_B$ be a witness scheme for $B$. Suppose that $(A, R_A) \preceq_{wi} (B, R_B)$ via $f_1$ and $g_1$ and $(B, R_B) \preceq_{wi} (A, R_A)$ via $f_2$ and $g_2$. Suppose that both $f_1$ and $f_2$ are length increasing and 1-invertible. Then $(A, R_A) \equiv_{wi} (B, R_B)$.

Using a polynomial-time version of the Schröder-Bernstein theorem, Berman and Hartmanis [BH77] showed that all paddable $NP$-complete problems are polynomial-time isomorphic. Since all currently known natural $NP$-complete sets are paddable, this implies that these sets belong to a single p-isomorphism degree of $NP$, namely that of $Sat$. In this paper we will show for three well-known natural $NP$-complete problems that they are wi-isomorphic to each other, and that there exist natural $NP$-complete problems that are highly unlikely to be wi-isomorphic to these problems. Thus, using wi-isomorphism, we are able to nontrivially refine the p-isomorphism degree of $Sat$.

We finish this subsection by giving a necessary condition for the existence of a witness-isomorphic reduction. We also note a set of sufficient conditions.

Theorem 2.5 Let $R_1$ and $R_2$ be relations (implicitly representing two problems). For each $b \in \{1, 2\}$ and each $i \in \{0, 1, \ldots\}$, define $Y_{b, i} = \{x | [R_b provides exactly $i$ witnesses for $x]\}$. Define two conditions as follows:

(D1) $P = P^\#P$.

(D2) There exists a polynomial $q$ such that, for each $z \in \Sigma^*$ and each $i$, it holds that: if $z \in Y_{1, i}$, then $(\exists y \in Y_{2, i}) [q(|z|) \geq |y|]$ and $q(|y|) \geq |z|].$

Then the following two claims hold: (1) If (D1) and (D2) hold, then $R_1$ witness-isomorphically reduces to $R_2$, and (2) If (D2) fails to hold, then $R_1$ does not witness-isomorphically reduce to $R_2$.

2.2 Local Search

Definition 2.6 [JPY88] A Polynomial Local Search (PLS) problem $A$ is a five tuple $(I_A, F_{S_A}, f_A, opt_A, N_A)$, where $I_A$ is the set of instances of $A$, for each $I \in I_A$ the set $F_{S_A}(I)$ is the set of feasible solutions of $I$, $f_A(I, S)$ assigns to every instance and feasible solution an integer value, its cost. The value of $opt_A$ is either min or max depending on the optimization nature of the problem, and for each $I \in I_A, s \in F_{S_A}(I), N_A(I, s)$ is a set of feasible solutions (known as the set of neighbors of $s$). Furthermore, $I_A \in P$, for each $I \in I_A$ an initial solution in $F_{S_A}(I)$ can be computed in polynomial time.
and for given \( s \in \mathcal{FS}_A(I) \) we can either decide in polynomial time whether \( s \) is locally optimal or compute an \( s' \in N_A(I,s) \) with a better cost, where "better" is smaller in the case where \( \text{opt}_A = \min \) and larger otherwise. The class of all PLS problems is called PLS.

The set of feasible solutions of a local search problem, together with a neighborhood structure, can be interpreted as a directed graph. The nodes of this graph are feasible solutions and edges point from feasible solutions to other feasible solutions with better cost. A path in this graph, such that each solution on this path has a cost better than the previous one, is called an augmenting path. A local search algorithm can be viewed as walking along an augmenting path in the graph from an arbitrary node (initial solution) to a sink (local optimum).

For a problem \( A \in \text{PLS} \), one can define a decision variant \( A^* \) as follows.

**Definition 2.7** [Fis95a] Let \( A \in \text{PLS} \). Define decision problem \( A^* \) as

- **Given** \( I \in I_A, s \in \mathcal{FS}_A(I), 0^d \).
- **Question** Is there a path \( p \) and a locally optimal solution \( s' \), such that \( p \) is an augmenting path between \( s \) and \( s' \) and \( p \) has length at most \( d \)?

Solution \( s \) is called the initial solution and value \( d \) is called the distance. The problem \( A^* \) is called the starred version of problem \( A \).

For \( A \in \text{PLS} \), the set \( A^* \) belongs to \( NP \), and so it is characterized by polynomial-time computable relations. We consider in this paper one such relation, the relation \( R_{A^*} \). Relation \( R_{A^*}(\langle I, s, 0^d \rangle, lsp) \) evaluates to true if and only if \( lsp \) is an augmenting path of length at most \( d \) from \( s \) to a locally optimal solution. Such an augmenting path is called a short augmenting path. Relation \( R_{A^*} \) is called the natural witness scheme of \( A^* \).

In Sections 4 and 5, we will consider the following three PLS problems.

**1:** The instance set of the problem \( \text{MaxSat} \) consists of Boolean formulas in CNF, where each clause has a weight. The set of feasible solutions of such a formula \( \phi \) is formed by all assignments \( \tau \) to the variables of \( \phi \). The cost of \( \tau \) equals the sum of the weights of the clauses satisfied by \( \tau \). An assignment \( \tau' \) is a neighbor of \( \tau \) if we can obtain \( \tau' \) from \( \tau \) by flipping the value of one variable in \( \tau \). This neighborhood is called the flip neighborhood.

**2:** The instance set of the problem \( \text{MinPartition} \) consists of multisets \( A \) of integers. The set of feasible solutions of \( A \) is formed by all partitions of the multiset \( A \) into two disjoint multisets. The cost of a partition is the absolute value of the difference of the sums of the values of the two sets. We wish to
minimize this cost. A partition \((A', B')\) is a neighbor of partition of \((A, B)\), if we can obtain \((A', B')\) from \((A, B)\) by either moving an element from \(A\) to \(B\) or moving an element from \(B\) to \(A\). This neighborhood is called the swap neighborhood.

3: The instance set of the problem \(MinVC\) consists of graphs \(G\). The set of feasible solutions of \(G\) is formed by all vertex covers of \(G\). The cost of a vertex cover of \(G\) equals the number of vertices in the vertex cover. A vertex cover \(VC'\) is a neighbor of a vertex cover \(VC\) if we can obtain \(VC'\) from \(VC\) by deleting one vertex from \(VC\). This neighborhood is called the remove neighborhood.

3 Models of Witness-Isomorphic Reduction

3.1 Witness-Isomorphic Reduction Definitions

We will define several variants of the wi-reduction. These variations arise from different possible quantifications in the definition. There are six possible combinations of existential and universal quantification, and Definition 3.1 presents each of them. We will consider all these types of reductions. Our results completely order the strengths of these six notions of witness-isomorphic reduction. We will also address the incidental, but interesting, issue of whether all counting versions of \(NP\)-complete sets are \#\(P\)-complete.

**Definition 3.1** For each \(A, B \in NP\),

1. \(A \preceq_{\text{wi} \exists}^P B\) if and only if there exists a witness scheme \(R_A\) for \(A\) and a witness scheme \(R_B\) for \(B\) such that \((A, R_A) \preceq_{\text{wi}} (B, R_B)\).
2. \(A \preceq_{\text{wi} \forall}^P B\) if and only if for each witness scheme \(R_A\) for \(A\) and for each witness scheme \(R_B\) for \(B\), \((A, R_A) \preceq_{\text{wi}} (B, R_B)\).
3. \(A \preceq_{\text{wi} \exists \forall}^P B\) if and only if for each witness scheme \(R_B\) for \(B\) there exists a witness scheme \(R_A\) for \(A\) such that \((A, R_A) \preceq_{\text{wi}} (B, R_B)\).
4. \(A \preceq_{\text{wi} \forall \exists}^P B\) if and only if for each witness scheme \(R_A\) for \(A\) there exists a witness scheme \(R_B\) for \(B\) such that \((A, R_A) \preceq_{\text{wi}} (B, R_B)\).
5. \(A \preceq_{\text{wi} \forall \forall}^P B\) if and only if there exists a witness scheme \(R_B\) for \(B\) such that for each witness scheme \(R_A\) for \(A\), \((A, R_A) \preceq_{\text{wi}} (B, R_B)\).
6. \(A \preceq_{\text{wi} \exists \forall}^P B\) if and only if there exists a witness scheme \(R_A\) for \(A\) such that for each witness scheme \(R_B\) for \(B\), \((A, R_A) \preceq_{\text{wi}} (B, R_B)\).
The mnemonic is that the "wi" subscript gives the order of the quantifiers and which set ("l" for left or "r" for right) the quantifier belongs to in cases where this is ambiguous. Some of the relations between these reductions are immediate from the definitions. The remaining ones (viewing the reductions as shorthands for the subset of $NP \times NP$ for which they hold), are stated in the following theorem.

**Theorem 3.2** The relations of the various reductions of Definition 3.1 on $NP$ is $\leq^P_{wi3\forall r} = \leq^P_{wi\forall r} \leq^P_{wi\forall l} \leq^P_{wi\exists l} \leq^P_{wi\exists r} \leq^P_{wi\exists 3} = \leq^P_{m}$. We prove this theorem by considering the properties of these reductions.

Since $Sat$ is a lodestar in the study of $NP$, we note, in contrast to some of the other reduction types soon to be discussed, that we trivially have here broad equivalence to $Sat$. (We adopt the standard notational shorthand $E_{p}^P(B) = \{A \mid [A \leq^P_{p} B$ and $B \leq^P_{p} A]\}$)

**Corollary 3.3** $E^P_{wi\exists 3}(Sat) = E^P_{wi\forall l}(Sat) = NP - \leq^P_{m}$-complete.

**3.2 The Reductions** $\leq^P_{wi\exists 3} \leq^P_{wi\forall l} \leq^P_{wi\forall r}$ and $\leq^P_{wi\exists r}$

In the next theorem we see that $\leq^P_{wi\exists 3}$ and $\leq^P_{wi\forall l}$ are, on $NP$, just new names for $\leq^P_{m}$. The proof is based on the fact that we can use as a witness scheme for set $A$ (the set reduced from) any witness scheme of set $B$ (the set reduced to). We essentially steal for $A$ the witness scheme of $B$.

**Theorem 3.4** 1. $(\forall A, B \in NP)[A \leq^P_{wi\exists 3} B$ if and only if $A \leq^P_{m} B]$.

2. $(\forall A, B \in NP)[A \leq^P_{wi\forall l} B$ if and only if $A \leq^P_{m} B]$.

Proof. The first part follows from the second part. Suppose that $A \leq^P_{m} B$. For each witness scheme for $B$, $R_{B}$ (we will often, as here, leave the polynomial implicit), define

$$R_{A}(x, y) = R_{B}(h(x), y).$$

It should be clear that $A$ and $B$ have the same witnesses under the witness schemes $R_{A}$ and $R_{B}$. Thus $A \leq^P_{wi\forall l}$. The reductions $\leq^P_{wi\forall r}$ and $\leq^P_{wi\exists l}$ are pathological. They relate only the empty set to itself.

**Theorem 3.5** For any sets $A, B \in NP : A \leq^P_{wi\forall r} B \iff A \leq^P_{wi\exists l} B \iff A = B = \emptyset$. 

8
Proof. Suppose $A \leq^P_{wi\exists^\forall \forall} B$. Let $(R_A, p_A)$ be a relation and polynomial satisfying the definition of $A \leq^P_{wi\exists^\forall \forall} B$, i.e., with the polynomials suppressed and implicit as usual, $R_A$ is such that for each witness scheme $R_B$ for $B$ it holds that $(A, R_A) \leq_{wi} (B, R_B)$. If $A \neq \emptyset$, let $m$ denote the minimum over all strings $z$ in $A$ of the number of witnesses (under $(R_A, p_A)$) certifying $z \in A$. If we change the $B$ relation to be as before, except now to have $m + 1$ certificates replacing each previous certificate, this proves that $A$ in fact does not $\leq^P_{wi\exists^\forall \forall}$-reduce to $B$.

The above observation is inspired by a paper of Edwards and Welsh [EW] that used a similar observation to “disprove,” in a certain nonstandard sense, the Berman-Hartmanis Isomorphism Conjecture.

3.3 The $\leq^P_{wi\exists^\forall_\forall}$-reduction

Note how strong the claim $A \leq^P_{wi\exists^\forall_\forall} B$ is. It says that there is some relationship for $B$ so flexible that any relation for $A$ yields a witness-isomorphic reduction to $B$ with respect to the flexible relation. Nonetheless, such tremendous flexibility can and does exist. In fact, any sufficiently careful proof of Cook’s Theorem yields the following claim.

**Theorem 3.6** ($\forall A \in \text{NP})[A \leq^P_{wi\exists^\forall_\forall} \text{Sat}]$. Furthermore, the existentially quantified relation for Sat is uniform over all sets $A \in \text{NP}$; that is, not only does it hold that for each $A \in \text{NP}$ there exists a witness scheme $R_{\text{Sat}}$ for Sat such that for each witness scheme $R_A$ for $A$, $(A, R_A) \leq_{wi} (\text{Sat}, R_{\text{Sat}})$, but in fact it even holds that there exists a witness scheme $R_{\text{Sat}}$ for Sat such that for each set $A \in \text{NP}$ and for each witness scheme $R_A$ for $A$, $(A, R_A) \leq_{wi} (\text{Sat}, R_{\text{Sat}})$.

The good behavior of $\leq^P_{wi\exists^\forall_\forall}$ is further certified by its transitivity. However, it is not in general reflexive.

**Proposition 3.7**

1. $(\forall A, B, C \in \text{NP})(A \leq^P_{wi\exists^\forall_\forall} B \text{ and } B \leq^P_{wi\exists^\forall_\forall} C) \implies A \leq^P_{wi\exists^\forall_\forall} C$.

2. For each nonempty finite set $A$, $A \not\leq^P_{wi\exists^\forall_\forall} A$. If $P \neq \text{NP}$, then there is a set $A$ in $\text{NP} – P$ such that $A \not\leq^P_{wi\exists^\forall_\forall} A$.

Proof. The first part is immediate from the definition. The second part is immediate for the case of nonempty finite sets. For the case of $\text{NP} – P$, it is easy to see that Ladner’s construction yields the desired result as follows.
Let $A$ be the $NP$ set yielded by a Ladner-type construction. Let the set $A$
be such that it consists of a segment of $SAT$, followed by a segment of the
empty set, and so on, such that each segment is exponentially longer than the
segment before it (Ladner’s [Lad75] construction can easily be implemented
so as to satisfy this). Consider the set $A$ along with any witnessing relation
for it. Consider the set $A$ along with the same witnessing relation trivially
altered to have, for any string $x$, two witnesses for each witness in the original
relation. There are two cases. If there is some constant $k$ such that for each
$x \in A$, $A$ has at most $k$ witnesses with respect to the first relation, then
any string in $A$ (with respect to the second relation) that has the maximum
number of witnesses has no string in $A$ (with respect to the first relation)
to map to in a $\leq_P^{w_i \exists_r \forall_f}$ reduction. On the other hand, consider the case in
which there is no constant $k$ such that for each $x \in A$, $A$ has at most $k$
witnesses with respect to the first relation. Consider an arbitrary potential
polynomial-time $\leq_P^{w_i \exists_r \forall_f}$ reduction from $A$ to $A$. Note that any polynomial
reduction will, for all but a finite number of $A$’s segments of $SAT$, fail to be
able map them to the next of $A$’s segments of $SAT$, due to the exponential
spacing. Note that, after this point, the first time an ambiguity level occurs
that is higher than any that previously occurred (as must happen due to the
assumption that there is no constant bound on the ambiguity), that string
in $A$ (with the second relation) will not be able to $\leq_P^{w_i \exists_r \forall_f}$ reduce via the
candidate reduction to an appropriate string in $A$ (with respect to the first
relation). \hfill $\square$

It is instructive to compare our $\leq_P^{w_i \exists_r \forall_f}$ reductions to the “universal
relation” notion proposed by Agrawal and Biswas [AB92]. Our notion is
more demanding than theirs in that it requires witness isomorphism, rather
than allowing mere equivalence as filtered through their elaborate “masking”
mechanism. On the other hand, our notion is less demanding than theirs
in that our definition applies to arbitrary $NP$ sets, rather than forcing $NP$-
completeness and applying with all $NP$ sets as the potential left-hand side
of the reduction.

### 3.4 $\leq_P^{w_i \exists_r \forall_f}$-Reducibility

Note that $\leq_P^{w_i \exists_r \forall_f}$ is a rather unusual reduction, as it requires that structure
be projected “forward.” As already noted, it is a more general reduction
than $\leq_P^{w_i \exists \forall_f}$, and a less general reduction than $\leq_P^{w_i \exists_r \forall_f}$. First note that the first
inclusion is strict. Consider for instance reducing a set with one element
to another set with one element. We will first give necessary conditions
for \( \leq_{wNP} \)-reducibility. Then we show that the second inclusion is strict. Finally, we show that on a subclass of NP that \( \leq^L_{wNP} \)-reducibility equals many-one reducibility.

**Definition 3.8** Let \( C \) and \( D \) be two disjoint sets. Set \( C \) is NP-separable from \( D \) if and only if there exists a set \( E \in NP \), such that \( C \subseteq E \) and \( E \) and \( D \) are disjoint.

**Theorem 3.9** Let \( A, B \in NP \). Suppose that \( A \leq^P_{1,1-honest} B \) via a reduction \( f \) such that \( f(A) \cap B \) is NP-separable from \( f(A) \). Then \( A \leq^P_{wNP} B \).

**Proof.** Let witness scheme \( R_A \) be given. Let witness scheme \( R_B \) be any witness scheme for \( B \). Let \( C \in NP \) be a set such that \( f(A) \cap B \subseteq C \) and \( C \) and \( f(A) \) are disjoint. Let \( R_C \) be a witness scheme for \( C \). Construct a witness scheme \( R \) for \( B \) as follows.

\[
R(f(x), x \# y) = R_A(x, y), \\
R(x, y_1 \# y_2) = R_B(x, y_1) \land R_C(x, y_2).
\]

It is easy to see that \( R \) is polynomial-time computable. It also holds that \( (A, R_A) \leq^P_{wi} (B, R) \) via \( f \), since elements in \( A \) and \( f(A) \) have the same witnesses.

What is the relationship between \( \leq^P_{wNP} \) and \( \leq^P_{m} \)? Clearly, for any finite sets \( S \) and \( T \) such that \( |S| > |T| \), we have \( S \leq^P_{m} T \) yet \( S \nleq^P_{wNP} T \). This pigeon-hole trick can be easily also used on infinite sets (e.g., on \( S = \{0^{2^k} | k \geq 1\} \cup \{1^{2^k} | k \geq 1\} \) and \( T = \{0^{2^k} | k \geq 1\} \). This is indeed just a trick based on the lack of enough strings to which to map. That is, it does not hold that

\[
(\forall n) \left( \exists \text{ polynomial } f \right) \left( |S|, |T| \leq^P_f(n) \right).
\]

However, there are relativized worlds where there are sets \( A \) and \( B \) such that \( A \leq^P_{m} B \) and there are enough strings to map to, yet \( A \) does not \( \leq^P_{wNP} \) reduce to \( B \).\(^1\) There are also relativized worlds (e.g., via collapsing classes

\(^1\)We briefly outline the proof. Let \( S^A = \{y \mid (\exists k)\ |y| = 2^k \} \) and \( <0, y> \in A \) and \( (\exists z)\ |z| = |y| \) and \( <1, y, z> \in A \}. \) The construction will ensure that \( (\forall y)\ |z| = |y| \) and \( <1, y, z> \in A \}. \) Thus, \( S^A \) will be in \( U^P_A \). We will also ensure in the construction that \( (\forall w)\ |S^A| \leq 2 \) and that \( if \ |w| = |y| \) and \( <0, w> \in A \) and \( <0, y> \in A \), then \( w \in S^A \) if and only if \( y \in S^A \). \( U^P_A \) is the class of sets accepted by
dramatically) such that all \(NP\) sets related by a many-one reduction and satisfying (**) in fact are related by the \(\leq_{w^1\mathcal{V}_3}^P\) reduction.

So, we have given necessary conditions for \(\leq_{w^1\mathcal{V}_3}^P\)-reducibility. Furthermore we have shown that the \(\leq_{w^1\mathcal{V}_3}^P\) reduction does not equal the many-one reduction. However, there is a subclass of \(NP\) on which these two kinds of reductions coincide.

**Theorem 3.10** Let \(A\) and \(B\) be two \(NP\)-complete sets. Suppose that \(A\) and \(B\) are both 1-invertibly paddable. Then \(A \leq_{m}^P B\) if and only if \(A \leq_{w^1\mathcal{V}_3}^P B\).

**Proof.** We know by their paddability that \(A\) and \(B\) are polynomial-time isomorphic. So there exists a polynomial-time computable function \(f\), such that \(f\) is a reduction from \(A\) to \(B\) and \(f^{-1}\) is a reduction from \(B\) to \(A\). Furthermore, since \(f\) is onto, \(f(A) \cap B = \emptyset\). Thus \(f(A)\) and \(f(A) \cap B\) are \(NP\)-separable. From Theorem 3.9, this theorem follows. \(\Box\)

### 3.5 \#P-completeness

In the penumbra of these notions lies an interesting question about \#P-completeness. Many people, quite informally, think of \#P as the counting version of \(NP\). However, Valiant [Val79] has noted that some \(P\) problems have \#P-complete counting versions. We investigate a flip side of the issue: Are all \(NP\)-complete sets \#P-complete in their counting versions? In particular, are there \(NP\)-complete sets that with respect to some witness scheme are not \#P-complete?

We use \#P-completeness in its most natural form, namely, with respect to 1-T reductions (see [Zan91], and also [Val79], for some discussion of the issues involved in completeness types for \#P). That is, \(f\) is \#P-complete if and only if \(f \in \#P\) and for each \(g \in \#P\), it holds that \(g \in FP_{1-T}\).

We first prove the following theorem concerning sets in \(NP\) having a witness scheme such that the counting version of the set is not \#P-complete with respect to this witness scheme.

---

a nondeterministic polynomial-time Turing machine that, with \(A\) as its oracle, has the property that for no input does the machine have more than two accepting paths (see [Wat88]). Let \(T^A = \{0^n \mid (3y)[|y| = n \text{ and } y \in S^A]\} \in UP_{\mathcal{V}_3}^A \subseteq NP^A\). Now, using the standard type of oracle argument as to how hard it is for a Turing machine to maintain unambiguity (see, e.g., [HH90]), we can easily choose \(A\) to satisfy these conditions and yet also ensure that \(S^A \not\leq_{w^1\mathcal{V}_3}^P T^A\) (via ensuring through a stage construction that each potential reducer either fails to appropriately reduce or reduces a string having one witness to one having two witnesses).
Theorem 3.11

1. If there is a \( \text{NP}\)-complete set \( L \) that with respect to some witnessing relation \( R_L \), is not \( \#P \)-complete, then \( P \neq P^{\#P} \).

2. If \( P \neq P^{\#P} \) and \( \text{NP} = \text{FewP} \), then each \( \text{NP}\)-complete set has some witnessing scheme with respect to which it fails to be \( \#P\)-complete.

Proof. The first part is immediate. As to the second part, assume \( P \neq P^{\#P} \) and \( \text{NP} = \text{FewP} \). Let \( L \) be any \( \text{NP}\)-complete problem. Since \( \text{NP} = \text{FewP} \), \( L \) has some witnessing relation having at most a polynomial number of witnesses for each input. We claim that \( L \) with respect to this relation cannot be \( \#P\)-complete. Why? If it were, consider the 1-Turing reduction from \( \#\text{SAT} \) to this. Since this has only a polynomial number of potential values, we can now consider all possible ones as answers to the 1-Turing reduction, and can thus generate a polynomial set of values one of which is the correct number of solutions for the given \( \#\text{SAT} \) formula. This is what is known as an enumerative approximation scheme [CH89] for \( \#\text{SAT} \). However, Cai and Hemaspaandra [CH91], and, independently, Toda ([Tod90], cited in [ABG90]) have shown that \( \#\text{SAT} \) has an enumerative approximation scheme only if \( P = P^{\#P} \). This contradicts our assumption that \( P \neq P^{\#P} \). \qed

Let \( \text{NP}-\leq_r\)-complete be the set of decision problems that are complete for \( \text{NP} \) with respect to the \( \leq_r \)-reduction. One might hope to sidestep Theorem 3.11 by asking whether every \( \text{NP}\)-complete set has some witness scheme with respect to which it is \( \#P\)-complete. For \( \#P \)-\( \leq_{1-r} \)-completeness this is an interesting open question. However, there are nontrivial relativized worlds (i.e., worlds in which \( P \) and \( \text{NP} \) differ) in which there are \( \text{NP}\)-complete sets that are not (in the natural sense) \( \#P \)-\( \leq_{m} \)-complete sets with respect to any legal witness relation. For example, the pathological relativized \( \text{NP}\)-complete sets constructed in [HH91] are not even (in that relativized world) \( \leq_{m} \)-hard for the \( P \) function \( f(n) = n \). Nonetheless, we give below a condition sufficient to imply that every \( \text{NP}\)-complete set has a witness scheme such that the set is \( \#P\)-complete with respect to this witness scheme.

Theorem 3.12 If \( \text{NP}-\leq_{m}\)-complete = \( \text{NP}-\leq_{1-1, \text{onto, honest}} \)-complete, then every \( \text{NP}\)-complete set \( L \) has a witness scheme \( R_L \), such that the counting version of \( L \) is \( \#P\)-complete with respect to \( R_L \).
4Witness-Isomorphic Reductions

We now turn from the more abstract discussion of Section 3 to the discussion of specific witness-isomorphic reductions between specific problems with respect to specific witness relations. That is, henceforward we will focus on Definition 2.1 and its application to natural problems. For problems whose globally optimal solutions are beyond the reach of feasible computation, one may turn to the local search approach in hope of finding a locally optimal solution in reasonable time. Note that a witness-isomorphic reduction between two (starred versions) of local search problems establishes a tight connection between search paths that translates these search paths back and forth. Thus, such a reduction makes a strategy concocted for one problem usable for the other. We give two examples of witness-isomorphic reductions from standard NP problems to the starred versions of local search problems. From this we conclude that there is a “wi-connection” between the two starred versions. Let Sat be the set of satisfiable Boolean formulas. Let R Sat be the witness scheme for Sat that on input ϕ and τ decides whether τ is a satisfying assignment for φ. Let Partition be the set of multi-sets containing positive integers. Let R Par be the witness scheme for Partition that on input A and (A0, B0) decides whether (A0, B0) is a partition of the elements of A, i.e., whether the elements in A0 sum up to the same value as the elements of B0.

Lemma 4.1[Fis95a] MaxSat* is NP-complete.

Proof. We prove the NP-completeness of MaxSat* by reduction from SAT. Let φ be a Boolean formula in CNF on n variables, x1, . . . , xn, and let ϕ have m clauses, C1, . . . , Cm. Construct ψ = ∧i=1n (xi ∨ bi)m+1 ∧ (C1 ∨ α) ∧ . . . ∧ (Cm ∨ α). By (x ∨ y)p we mean that the clause (x ∨ y) appears p times in ψ. Clause (Cj ∨ α) is a clause that contains all literals in Cj and α. Let τ0 be the all-zero assignment for the variables in ψ. We reduce ϕ to (ψ, τ0, 0n).

It is easy to see that every locally optimal solution for ψ assigns to bi or xi the value one, 1 ≤ i ≤ n, and satisfies ψ. Furthermore, a locally optimal solution that assigns to all literals in a clause Cj the value 0, assigns to α the value 1.

Let τ be a satisfying assignment of φ. Let ⃗τ be an assignment for ψ depending on ϕ in the following way. For 1 ≤ i ≤ n, τ and ⃗τ assign the same value to xi. Assignment ⃗τ assigns to bi the complement of the value it assigns to xi and it assigns to α the value 0. It is easy to see that ⃗τ is reachable from τ0 within n flips and that ⃗τ is a satisfying assignment of ψ.
Now let $\tilde{\tau}$ be any locally optimal solution reachable from $\tau_0$ within $n$ flips. We can associate with $\tilde{\tau}$ an assignment $\tau$ for the variables in $\phi$ that assigns to $x_i$ the value $\tilde{\tau}$ assigns to $x_i$, $1 \leq i \leq n$. Assignment $\tau$ must be a satisfying assignment of $\phi$, since otherwise $\tau$ assigns to all literals of at least one clause in $\phi$ the value 0. This means that $\tilde{\tau}$ assigns to $\alpha$ the value 1. This contradicts the fact that $\tilde{\tau}$ is reachable from $\tau_0$ within $n$ flips. $\square$

Consider the many-one reduction from $\text{SAT}$ to $\text{MaxSat}^*$ in Lemma 4.1. In this reduction, to every satisfying assignment $\tau$ for $\phi$ a unique near locally optimal assignment $\tilde{\tau}$ for $\psi$ is associated. This assignment $\tilde{\tau}$ can be reached from $\tau_0$ by many short augmenting paths. These many short augmenting paths occur due to the fact that the values of $x_i$ or $b_i$ can be flipped in any order. In the proof of the following theorem we extend $\psi$ by a subformula $\xi$ that takes care that the order in which the variables $x_i$ and $b_i$ are flipped is fixed.

**Theorem 4.2** There exists a witness-isomorphic reduction from $(\text{Sat},R_{\text{Sat}})$ to $(\text{MaxSat}^*,R_{\text{MaxSat}^*})$.

**Proof.** Let $\phi$ be a Boolean formula in CNF on the variables $x_1, x_2, \ldots, x_n$ and let $\phi$ have clauses $C_1, \ldots, C_m$. Construct

$$\psi = \bigwedge_{i=1}^{n} (x_i \lor b_i)^{m+1} \land \bigwedge_{j=1}^{m} (C_j \lor \alpha)$$

and

$$\xi = \bigwedge_{j=1}^{n-1} \bigwedge_{i=j+1}^{n} ((x_j \lor b_j \lor x_i)^{3m} \land (x_j \lor b_j \lor b_i)^{3m}).$$

Let $\Psi = \psi \land \xi$. The notation $C^\mu$, $C$ a clause in $\Psi$, means that $C$ appears $\mu$ times in $\Psi$. Furthermore, $(C_j \lor \alpha)$ is the clause that contains the literals of $C_j$ and $\alpha$. Let $\tau_0 = 0^{2n+1}$, i.e., initial solution $\tau_0$ assigns to all variables of $\psi$ the value 0. We claim that the function that maps $\phi$ to $<\Psi, \tau_0, 0^n>$ is a witness-isomorphic reduction from $\text{SAT}$ to $\text{MaxSat}^*$. Note that $\psi$ is the same formula defined in the proof of Lemma 4.1. Note also that by the structure of $\xi$, on any augmenting path leaving $\tau_0$, first $x_1$ or $b_1$ is flipped, then $x_2$ or $b_2$, and so on. Lemma 4.1 proved that the function that maps $\phi$ to $<\psi, \tau_0, 0^n>$ is a many-one reduction from $\text{SAT}$ to $\text{MaxSat}^*$. So if $\phi$ is not satisfiable, no locally optimal assignment for $\Psi$ can be reached after at most $n$ flips. To see this, notice that any assignment reachable from $\tau_0$ after at most $n$ flips does not satisfy $\psi$. 

15
Suppose that $\phi$ is satisfiable. Let $\tau$ be a satisfying assignment for $\phi$ that assigns to $x_i$ the value $\tau_i$. Consider the assignment $\hat{\tau}$ for $\Psi$ that assigns to $x_i$ the value $\hat{\tau}_i$, to $b_i$ the value $\tau_i$, and to $\alpha$ the value $0$. Assignment $\hat{\tau}$ satisfies $\Psi$. So for every assignment $\tau$ for $\phi$ there is a unique locally optimal assignment $\hat{\tau}$ reachable from $\tau_0$ after at most $n$ flips by a unique augmenting path.

Let $\hat{\tau}$ be a locally optimal solution reachable from $\tau_0$ after at most $n$ flips. Since $\hat{\tau}$ is locally optimal, $\hat{\tau}$ satisfies $\phi$ and thus $\hat{\tau}$ satisfies $\psi$. From the distance between $\tau_0$ and $\hat{\tau}$ and the local optimality from $\hat{\tau}$, we know that $\hat{\tau}$ assigns either to $x_i$ or to $b_i$ the value $1$, $1 \leq i \leq n$. Notice that there is exactly one augmenting path from $\tau_0$ to $\hat{\tau}$. Assignment $\tau$ that assigns to $x_i$ the same value $\hat{\tau}$ assigns to $x_i$ satisfies $\phi$, since $\hat{\tau}$ satisfies $\psi$ and $\hat{\tau}$ assigns to $\alpha$ the value $0$.

Similarly, one can show (the full, tedious details can be found in [Fis95b]²) that $(\text{Sat}, \text{R}_{\text{Sat}})$ reduces witness-isomorphically to $(\text{Partition}, \text{R}_{\text{Partition}})$ (in fact, this is implicit in the literature, via using a reduction of Savelsberg and Van Eerde Boas [SvEB84]) and that $(\text{Partition}, \text{R}_{\text{Partition}})$ reduces witness-isomorphically to $(\text{MinPartition}^*, \text{R}_{\text{MinPartition}^*})$. In light of these reductions, Theorem 4.2, Theorem 2.4, and Theorem 3.6, we can conclude that $(\text{MaxSat}^*, \text{R}_{\text{MaxSat}^*}) \equiv_{\text{wi}}^{\text{iso}} (\text{MinPartition}^*, \text{R}_{\text{MinPartition}^*})$.

5 A Non Wi-Isomorphism

In the previous section we gave witness-isomorphic reductions from $(\text{Sat}, \text{R}_{\text{Sat}})$ to starred versions of local search problems (always with the “short path witness scheme”). By Theorem 3.6 we can use these reductions to obtain tight relations between the (starred versions of) these local search problems. It would be very nice if such reductions could be found between all (starred versions of) local search problems with their short path witness schemes. This could motivate the search for a uniform search strategy, applicable via translation, to any problem in PLS. We note however that witness-isomorphic reductions are not always possible.

²Briefly, the idea of the latter reduction is as follows: From a given instance of partition $A = \{a_1, a_2, \ldots, a_n\}$, we construct an instance of $\text{MinPartition}^*$, $\langle A', (A'_0, B'_0), \theta^{2n} \rangle$, in which each integer $a_i$ is represented by the elements $a^1_i$, $a^2_i$, $\beta^1_i$ and $\beta^2_i$. These elements ensure that a path from $(A'_0, B'_0)$ to a local optimum (which is a partition of the original problem) is indeed unique. Let $(A'_0, B'_0)$ be a partition of $A'$ reachable after at most $2n$ swaps. By inserting enough elements of weight 1, we ensure that $(A_x, B_x)$ is locally optimal if and only if $A_x = B_x$. 

16
A very simple example shows this. Define for instance a variant of MaxSat, the problem VMS, that has the same instance as MaxSat. Suppose that the set of solutions belonging to a Boolean formula \( \phi \) contains tuples \( (\tau, l) \), where \( \tau \) is an assignment to the variables in \( \phi \) and \( l \in \{0, 1\} \). Two tuples \( (\tau, l) \) and \( (\tau', l') \) are neighbors if \( \tau' \) is a neighbor of \( \tau \) according to the flip neighborhood. Like MaxSat, the problem VMS belongs to PLS. Define for VMS its starred version \( VMS^* \) as we did before, and let \( R_{VMS^*} \) be its natural witness scheme. Since there are Boolean formulas that have exactly one satisfying assignment, \( (\text{Sat}, R_{\text{Sat}}) \not\leq_{wi} (VMS^*, R_{VMS^*}) \).

Note that we have broken condition \((D2)\) of Theorem 2.5 in a particularly simple way: by ensuring that there are no instances of \( VMaxSat\) having an odd number of witnesses. In fact, the counterexample just given is exactly the type of mismatch that was of interest to Edwards and Welsh [EW].

We now turn our attention to an optimization problem with a well-known neighborhood structure. Consider the MinVC problem with the remove neighborhood. We will show now that if \( R \neq NP \) then there is a structural difference between MaxSat and MinVC in terms of their short local search paths. Furthermore, separation of these two problems seems to resist simple combinatorial arguments as used above.

**Theorem 5.1** MinVC* is NP-complete.

**Proof.** To prove that MinVC* is NP-complete, we will construct a polynomial-time reduction from 3Sat to MinVC*. Let \( \phi = C_1 \land C_2 \land \ldots \land C_m \) be a Boolean formula on the variables \( x_1, \ldots, x_n \). From \( \phi \) we construct a graph \( G \) that contains a part for every variable \( x_i \) and every clause \( C_j \). For every variable \( x_i \), graph \( G \) contains the vertices \( v_i, \overline{v_i}, \zeta_i^1 \) and \( \zeta_i^2 \). Furthermore, graph \( G \) contains the edges \( (v_i, \overline{v_i}) \) and \( (\overline{v_i}, \zeta_i^2) \), \( 1 \leq j \leq 2 \).

For each clause the graph has a part that consists of the nine vertices \( \lambda_i^j \), \( 1 \leq i, j \leq 3 \). This part contains three edges \( (\lambda_i^1, \lambda_i^2), (\lambda_i^2, \lambda_i^3), \) and \( (\lambda_i^3, \lambda_i^1) \) and three pairs of edges \( (\lambda_i^1, \lambda_i^2), (\lambda_i^1, \lambda_i^3), \) \( 1 \leq j \leq 3 \). Graph \( G \) also contains edges between vertices in the variable part and vertices in the clause part. Suppose that clause \( C_j \) contains an occurrence \( l_k \) of the variable \( x_i \). If \( l_k = x_i \), then edge \( (v_i, \lambda_i^j) \) is in \( G \). Otherwise edge \( (\overline{v_i}, \lambda_i^j) \) is an edge in \( G \). Figure 1 shows an example graph \( G \).

The reduction maps \( \phi \) to \( (G, V_0, 0^{n+5m}) \), where \( V_0 \) contains all the vertices in \( G \). A locally optimal vertex cover \( V^* \) reachable from \( V_0 \) has the following properties.

1. Either \( v_i \) or \( \overline{v_i} \) or both \( \zeta_i^1 \) and \( \zeta_i^2 \) are removed from \( V_0 \).
2. For every clause part, at least for 2 literals \( l_i, l_j \) the vertices \( \lambda_i^2, \lambda_i^3, \lambda_j^2, \) and \( \lambda_j^3 \) have been removed from \( V_0 \).

3. Finally, either \( \lambda_k^i, i, j \neq k \), or both \( \lambda_k^2 \) and \( \lambda_k^3 \) have been removed.

(Property 1 is immediate. Property 2 follows from the fact that at least two of \( \lambda_k^i \) must remain in the vertex cover. Property 3 follows from Property 2.) So at least \( n + 5m \) vertices must be removed from \( V_0 \) before a locally optimal vertex cover can be reached.

Let \( \tau \) be an assignment that satisfies \( \phi \). We define a vertex cover \( V \) for \( G \) obtained from \( V_0 \) as follows. If \( \tau \) assigns to \( x_i \) the value 0, vertex \( v_i \) is removed from \( V_0 \). Otherwise, vertex \( v_i \) is removed from \( V_0 \). For the minimal \( k \) such that \( \tau \) makes \( l_k \) true in a clause, the vertex \( \lambda_k^i \) is removed from \( V_0 \). For the remaining two literals \( l_{k'} \) and \( l_{k''} \) in such a clause, the vertices \( \lambda_{k'}^2, \lambda_{k'}^3, \lambda_{k''}^2 \) and \( \lambda_{k''}^3 \) are removed from \( V_0 \). Vertex cover \( V \) is locally optimal and is reachable by removing \( n + 5m \) vertices.

If \( \tau \) is an assignment that does not satisfy \( \phi \), there is at least one clause having only false literals. This means that either all of \( \lambda_k^j \) remain in the vertex cover or there is some variable part where both \( v_i \) and \( \bar{v}_i \) remain in the vertex cover. In both these cases at least \( n + 5m + 1 \) vertices will be removed before reaching a locally optimal solution. \( \square \)
Lemma 5.2 Let $G$ be an instance of $\text{MinVC}$, let $VC_0$ be any feasible solution in $\mathcal{F}_{\text{MinVC}}$. Let $VC$ be a locally optimal solution reachable from $VC_0$ after $k$ local search steps. Then there are $k!$ augmenting paths from $VC_0$ to $VC$.

Proof. Let

$$VC_0, VC_1, \ldots, VC_k = VC$$

be any augmenting path from $VC_0$ to $VC$. At least one such path exists. Suppose that $VC_i$ is obtained from $VC_{i-1}$ by deleting a vertex $v_i$. Notice that once a vertex is deleted, it will never be introduced again. Let $\pi$ be a permutation on $\{1, 2, \ldots, k\}$ and consider the sequence of solutions

$$VC_0, VC_{\pi(1)}, \ldots, VC_{\pi(k)}$$

where $VC_{\pi(i)}$ is obtained from $VC_{\pi(i-1)}$ by deleting the vertex $v_{\pi(i)}$. We will show that this sequence is an augmenting path from $VC_0$ to $VC$. Notice that $VC_{\pi(k)} = VC_k$, since to reach $VC_{\pi(k)}$ from $VC_0$ the same vertices have been deleted as to reach $VC_k$ from $VC_0$, only in another order. So $VC_{\pi(k)}$ is vertex cover of $G$ and thus $VC_{\pi(h)}$ is also a vertex cover of $G$. Since $VC_{\pi(i)}$ contains fewer solutions than $VC_{\pi(i-1)}$, the sequence is an augmenting path.

$\Box$

Theorem 5.3 If there exists a wi-reduction from $(\text{Sat}, R_{\text{Sat}})$ to $(\text{MinVC*}, R_{\text{MinVC*}})$ then $R = NP$.

Proof. Suppose that such a reduction exists. On an input formula, $F$, we use the Valiant-Vazirani [VV85] construction to obtain a new formula (different coin flips may yield different formulas). The Valiant-Vazirani construction has the following properties. If $F$ is not satisfiable, then for all coin flips the new formula obtained is not satisfiable. There is a polynomial $h$ (independent of $F$) such that if $F$ is satisfiable, then with probability at least $1/h(|F|)$ the formula obtained has exactly one satisfying assignment. Apply the assumed wi-reduction on the new formula obtained as above. We obtain a graph with an initial vertex cover and (with probability $1/h(|F|)$ if $F$ is satisfiable but with probability zero if $f$ is not satisfiable) a unique optimal vertex cover at distance 1. We search the distance-1 neighborhood of the initial solution to retrieve this vertex cover, and accept (on the current probabilistic computation path) if we find it. If $F$ is satisfiable (respectively, is not satisfiable), this algorithm accepts with probability $1/h(|F|)$ (respectively, 0), thus $R = NP$. $\Box$
Acknowledgments: We thank M. Ogiwara for helpful discussions, and H. Buhrman for suggesting the proof of Theorem 5.3. We thank Marius Zimand for a careful, helpful proofreading.

References


