A UNIFORM REDUCTION THEOREM
extending a result of J. Grollmann and A. Selman

Kenneth W. Regan
Merton College
Oxford, OX1 4JD England

Abstract: We derive a recursion-theoretic result telling when a family of reductions to a class \( \mathcal{A} \subseteq \mathcal{P}(\Sigma^*) \) can be replaced by a single oracle Turing machine. The theorem is a close analogue of the Uniform Boundedness Theorem of functional analysis, specializing it to the Cantor-set topology on \( \mathcal{P}(\Sigma^*) \). This generalizes one of the main theorems of J. Grollmann and A. Selman [FOCS '84], namely that \( \mathcal{NP} \)-hardness implies uniform \( \mathcal{NP} \)-hardness for 'promise problems'. We investigate other consequences and problems arising from the theorem.

1. Promise problems

Let \( Y \) and \( N \) be disjoint subsets of \( \Sigma^* \), where \( \Sigma = \{0,1\} \). Define \( \mathcal{J}(Y,N) \) to be the class \( \{ B \subseteq \Sigma^* \mid Y \subseteq B \land N \subseteq (\Sigma^* \setminus B) \} \) of languages which "separate" \( Y \) from \( N \). This is the solution space of the following conditional decision problem \( \Pi(Y,N) \):

\[
\begin{align*}
\text{Promise:} & \quad \text{The input string } x \text{ is in } Y \cup N. \\
\text{Query:} & \quad \text{Is } x \text{ in } Y?
\end{align*}
\]

Problems about inverting easy-to-compute functions, and more specifically cracking public-key cryptosystems, fall naturally into this category. See [EY80], [SY82], and [GS84] for the original formulation of promise problems and more-detailed examples.

Some basic definitions: If \( M \) is an oracle Turing machine (OTM), then we write \( L(M^A) \) for the language accepted by \( M \) with oracle set \( A \subseteq \Sigma^* \). An OTM is \( p \)-bounded if its running time is bounded by a fixed polynomial of the length of its input for all oracle sets. By attaching polynomial "clocks" one can generate a comprehensive recursive enumeration \( \{ P_j \}_{j=1}^\infty \) of \( p \)-bounded OTM's, so that \( A \leq^p \mathcal{B} \iff (\exists j)[A = L(P_j^B)] \) for all \( A,B \subseteq \Sigma^* \). SAT is taken as a representative \( \mathcal{NP} \)-complete language.

Definition 1 [SY82]: The promise problem \( \Pi(Y,N) \) is

1. in \( \mathcal{P} \) if \( \mathcal{J}(Y,N) \cap \mathcal{P} \neq \emptyset 
2. \( \mathcal{NP} \)-hard if every language in \( \mathcal{J}(Y,N) \) is \( \mathcal{NP} \)-hard.
3. uniformly \( \mathcal{NP} \)-hard if there exists a single \( p \)-bounded oracle Turing machine \( M \) such that \( L(M^B) = \text{SAT} \) for all \( B \in \mathcal{J}(Y,N) \).
The above-mentioned papers implicitly restrict attention to recursive languages in $\mathcal{J}(Y,N)$ in (2) and (3). We shall touch on this in §4.

What J. Grollmann and A. Selman prove in [GS84] is that $\mathcal{NP}$-hardness and uniform $\mathcal{NP}$-hardness are actually equivalent for promise problems. That is,

$$\forall \mathcal{J}(Y,N) (\exists Y) : L(P^B_Y) = \text{SAT}$$

$$\iff$$

$$\exists Y (\forall \mathcal{J}(Y,N)) : L(P^B_Y) = \text{SAT}.$$  \hspace{1cm}(1.1)

[Gr84] and [GS85] extend this to Turing reductions from one promise problem to another. We say $\Pi(S,T) \leq^P \Pi(Y,N)$ if for every $A \in \mathcal{J}(Y,N)$ there exists a $p$-bounded OTM $P$ such that $L(P^A) \in \mathcal{J}(S,T)$. The reduction is uniform if for some fixed $j$, $L(P^A_j) \in \mathcal{J}(S,T)$ for all $A \in \mathcal{J}(Y,N)$. The extended theorem replaces 'L($P^B_Y$) = SAT' with 'L($P^B_Y$) \in \mathcal{J}(S,T)' above. The uniformity result for $\mathcal{NP}$-hard promise problems follows by taking $S := \text{SAT}$, $T := \Sigma^* \setminus \text{SAT}$.

Their proof proceeds by diagonalization over the effective enumeration $[P_j]_{j=1}^\infty$. We remove some of their assumptions, and present the result as a consequence of the phenomenon known in classical analysis as the "uniform boundedness principle".

2. Topological background

Order $\Sigma^*$ lexicographically as $\lambda, 0, 1, 00, 01, 10, 11, 000, \ldots$ (where $\lambda$ is the null string). For each $x \in \Sigma^*$, define $\text{bin}(x)$ to be the positive natural number having binary representation $1x$. Then every $A \in \Sigma^*$ corresponds uniquely to an infinite 0-1 "characteristic vector" $\chi_A$, so that e.g. the set of primes goes to '0110101001\ldots'. (We use lowercase Greek letters $\alpha, \beta, \gamma$, and $\chi$ for finite or infinite 0-1 strings intended as characteristic vectors, to reduce confusion with strings $x, y, z, w, \ldots \in \Sigma^*$ intended as members of languages.) We write $\alpha \subseteq \beta$ to mean that $\alpha$ is an initial segment of $\beta$ (possibly null or all of $\beta$), and $\alpha \subseteq A$ if $A \subseteq \Sigma^*$ and $\alpha \subseteq \chi_A$.

For $A, B \subseteq \Sigma^*$ define $p(A,B)$ to be $2^{-n}$, where $n$ is the length $|\alpha|$ of the longest string $\alpha$ such that $\alpha \subseteq A$ and $\alpha \subseteq B$. If $A = B$, then $p(A,B) = 0$. This is a metric on the power set $\mathcal{P}(\Sigma^*)$, and defines the Cantor-set topology $\mathcal{T}$, akin to the positive information topology of [Cu80]. The open sets of $\mathcal{T}$ are precisely those classes $\mathcal{O} \subseteq \mathcal{P}(\Sigma^*)$ where membership of $A \in \mathcal{O}$ can be verified from a finite initial segment of $\chi_A$, i.e.

$$(\forall A \in \mathcal{O}) (\exists x \in \Sigma^*)(\forall e \in \Sigma^*) [\alpha \subseteq A \wedge (\forall e \in \Sigma^*) : \alpha \subseteq B \iff B \in \mathcal{O}]$$  \hspace{1cm}(2.1)

Correspondingly, classes $\mathcal{C}$ closed in $\mathcal{T}$ are precisely those characterizable by lists of "forbidden initial segments", namely those $\alpha$ satisfying (2.1) for some given $A$ and $\mathcal{C} := \mathcal{P}(\Sigma^*) \setminus \mathcal{C}$. (Where complements are understood to be in $\Sigma^*$ or in $\mathcal{P}(\Sigma^*)$ we prefix a tilde $\sim$. Thus $\sim\text{SAT}$ stands for $\Sigma^* \setminus \text{SAT}$, and $\sim\mathcal{C}$, for $\mathcal{P}(\Sigma^*) \setminus \mathcal{C}$. For future reference, we also let $\langle \cdot, \cdot \rangle$ be a (wlog. polynomial-time) computable bijection from $\Sigma^* \times \Sigma^*$ to $\Sigma^*$.)