SPARSE reduces conjunctively to TALLY

Harry Buhrman* Edith Hemaspaandra† Luc Longpré‡

Abstract

Polynomials over finite fields are used to show that any sparse set can conjunctively reduce to a tally set. This leads to new results and to simple proofs of known results about various classes that lie between P and P/poly.

1 Introduction

Sparse sets and tally sets have been the subject of much research recently in structural complexity theory. A nice survey of results on this topic can be found in [HOW92].

Sparse sets are closely linked to non-uniform complexity classes and circuit complexity. It is well known that sets Turing reducible to sparse sets is exactly the class of sets having polynomial size circuits, and is also the same as the advice class P/poly, the class of sets solvable with polynomial size advice. Since sparse sets can be encoded easily as tally sets, this is also the same as the class of sets Turing reducible to tally sets.

For a reduction $\leq_r^p$ and a class of sets $\mathcal{C}$, let $R_r(\mathcal{C})$ be the class of all sets that are $\leq_r^p$-reducible to a set in $\mathcal{C}$. In this terminology, P/poly $= R_T(\text{SPARSE}) = R_T(\text{TALLY})$. There is an interesting structure of sets lying between P and P/poly that can be defined by changing the Turing reductions to weaker reductions, and/or by considering tally sets instead of sparse sets.

The study of the $R_r(\text{SPARSE})$ and $R_r(\text{TALLY})$ classes, for various reductions r, was initiated by Book and Ko in [BK88]. A more extensive study of these classes can be found in

*CWI, Kruislaan 413, 1098 SJ Amsterdam, the Netherlands. Work done in part while at the University of Amsterdam and while visiting Boston University with the support of NSF Grant CCR-8814339 and NWO Grant SIR 13-603.

†Department of Computer Science, Le Moyne College, Syracuse, NY 13214. Work done in part while at the University of Amsterdam.

‡College of Computer Science, Northeastern University, Boston, MA 02115. Supported in part by NSF Grant CCR-9211174.

[Ko89], [AHOW92] and [AHH$^+$92]. Our main result refutes one of Ko's conjectures [Ko89] by showing that every sparse set is conjunctive truth-table reducible to a tally set:

$$\mathrm{SPARSE} \subseteq R_{ctt}(\mathrm{TALLY}).$$

$$R_{ctt}(\mathrm{SPARSE}) = R_{ctt}(\mathrm{TALLY}).$$

The reduction uses polynomials over finite fields to encode any sparse set into a tally set in such a way that a polynomial time algorithm can compute membership in the sparse set using a conjunctive truth table query. This encoding method itself found more applications. Recently, it has been used to show an upward separation for FewP [RRW94]. The more classic encoding method did not seem to work there. It has also been used to handle bottlenecks in neural networks [Wat].

Our result is surprising since it is false for disjunctive truth table reductions [Ko89]: SPARSE $\not\subseteq R_{dtt}(\mathrm{TALLY})$, and since it was believed to be false by those who looked at the problem. One way to interpret the result is as follows. It is easy to see that one can encode a sparse set into a tally set. But can it be encoded in such a way that all the information about the sparse set can be retrieved with a conjunctive truth-table? With a disjunctive truth-table? The answers are yes and no, respectively.

The result allows us to derive corollaries that either settle other open problems or provide simple proofs of previously known results. For example, as a derived result, we refute another conjecture of Ko by showing:

$$R_{bdtt}(\mathrm{SPARSE}) \subseteq R_{ctt}(\mathrm{SPARSE}).$$

These two results and the following result by Gavaldà and Watanabe settle all the remaining open problems from [Ko89]. We end this section by looking at *positive* truth-table reductions [Sel82] ($\leq^p_{ptt}$) to sparse and tally sets. In particular, we show that *ptt* reductions to tally sets capture the class $R_{tt}(\mathrm{TALLY})$:

$$R_{ptt}(\mathrm{TALLY}) = R_{tt}(\mathrm{TALLY}).$$

and thus:

$$R_{ptt}(\mathrm{SPARSE}) = R_{tt}(\mathrm{SPARSE}).$$

In [GW], Gavaldà and Watanabe use a technique based on Kolmogorov complexity to prove the conjecture of Ko that $R_{ctt}(\mathrm{SPARSE}) \not\subseteq R_{dtt}(\mathrm{SPARSE})$. Their construction actually provides something stronger. If $f(n)$ is an unbounded function from integers to integers, such that $f(n)$ is computable in time polynomial in n, then their construction provides a set that is not $\leq^p_{dtt}$-reducible to any sparse set, but $\leq^p_{ctt}$-reducible to a sparse set using only $f(n)$ queries on inputs of length n: $R_{f(n)\text{-}ctt}(\text{SPARSE}) \not\subseteq R_{dtt}(\text{SPARSE})$, for any polynomial time computable unbounded function f. By improving their technique, we are able to make the set reducible to a *tally* set. For any polynomial time computable unbounded function f:

$$R_{f(n)\text{-}ctt}(\text{TALLY}) \not\subseteq R_{dtt}(\text{SPARSE}).$$

Combining this with our main result, we can strengthen one of Ko's results and show that for any polynomial time computable unbounded function f:

$$R_{f(n)\text{-}dtt}(\text{TALLY}) \not\subseteq R_{ctt}(\text{SPARSE}).$$

This is optimal in some sense and reveals the following picture: $R_{bdtt}(\text{SPARSE})$ is included in $R_{ctt}(\text{SPARSE})$ (this paper) and $R_{bctt}(\text{SPARSE})$ is included in $R_{dtt}(\text{SPARSE})$ [Ko89]. On the other hand for any unbounded f, the classes $R_{f(n)\text{-}dtt}(\text{SPARSE})$ and $R_{f(n)\text{-}ctt}(\text{SPARSE})$ are incomparable.

From our main result, we can easily obtain further new results. For example, we show that various classes are not closed under complementation. We also obtain results that were previously known, almost directly from our main result. A typical line of reasoning is as follows: if a set is $\leq^p_{ctt}$-reducible to a sparse set, then it is $\leq^p_{ctt}$-reducible to a tally set by our result, and thus its complement is $\leq^p_{dtt}$-reducible to a tally set. This complementation argument can be applied only for tally sets.

2 Preliminaries

2.1 Notations

Let $\Sigma = \{0, 1\}$. Strings are elements of Σ^*, and are denoted by lower case letters $x, y, u, v, \cdots$. For any string x the length of a string is denoted by $|x|$. Subsets of $\Sigma^*$are denoted by capital letters $A, B, C, S, \cdots$. The set $\Sigma^* - A$ is denoted by $\overline{A}$. For a set A we use $A^{=n}(A^{\leq n})$ to denote the subset of A consisting of all strings of length $n(\leq n)$. For any set A the cardinality of A is denoted by $\|A\|$. If for all n, $\|A^{=n}\| \leq d(n)$, we say that A is of *density* $d(n)$. We call a set S is *sparse* if there exists a polynomial p such that for all n, $\|S^{\leq n}\| \leq p(n)$. A set T is called *tally* if $T \subseteq \{0\}^*$. We fix a pairing function $\lambda xy.\langle x, y\rangle$ computable in polynomial time from $\Sigma^* \times \Sigma^*$ to Σ^*. Without loss of generality we assume that for all $x, y : |x| + |y| \leq |\langle x, y\rangle| \leq 2(|x| + |y|)$. We assume that the reader is familiar with the standard Turing machine model.

2.2 Truth tables

The ordered pair $\langle\langle a_1, \cdots, a_k\rangle, \alpha\rangle$, for $k > 0$, is called a *truth-table condition of norm k* if $\langle a_1, \cdots, a_k\rangle$ is a k-tuple of strings, and α is a k-ary Boolean function [LLS75]. The set $\{a_1, \cdots, a_k\}$ is called the *associated set* of the tt-condition. A function f is a *truth-table function* if f is total and $f(x)$ is a truth-table condition for every x in Σ^*. We denote the associated set of $f(x)$ by $\mathrm{Ass}(f(x))$. If, for all x, $f(x)$ has norm less than or equal to k, then f is called a k-truth-table (ktt) function. We say that a tt-function f is a *disjunctive* (*conjunctive)* truth-table (dtt (ctt)) function if f is a truth-table condition whose Boolean function is always a disjunction (conjunction) of its arguments.

2.3 Reductions, reducibilities

Let $A_1, A_2 \subseteq \Sigma^*$. In this paper, all reductions are polynomial time computable. We say that:

1. A_1 is truth-table reducible to A_2 ($\leq^p_{tt}$-reducible) iff there exists a polynomial time computable tt-function f such that $x \in A_1$ iff $\alpha(\chi_{A_2}(a_1), \ldots, \chi_{A_2}(a_k)) = \mathbf{true}$, where $f(x)$ is $\langle\langle a_1, \ldots, a_k\rangle, \alpha\rangle$ and χ_{A_2} is the characteristic function of the set A_2.

2. A_1 is k-truth-table reducible to A_2 ($\leq^p_{k\text{-}tt}$-reducible) iff $A_1 \leq^p_{tt} A_2$ by some ktt function. A_1 is bounded-truth-table reducible to A_2 ($\leq^p_{btt}$-reducible) iff $A_1 \leq^p_{k\text{-}tt} A_2$ for some integer k.

3. A_1 is disjunctive (conjunctive) truth-table reducible ($\leq^p_{dtt}(\leq^p_{ctt})$-reducible) to A_2, iff $A_1 \leq^p_{tt} A_2$ by some dtt (ctt)-function. For $k \geq 0$, A_1 is k-disjunctive (conjunctive) truth-table reducible ($\leq^p_{k\text{-}dtt}$ ($\leq^p_{k\text{-}ctt}$)) to A_2, if $A_1 \leq^p_{tt} A_2$ by some dtt (ctt)-function of norm k.

4. A_1 is disjunctive (conjunctive) truth-table reducible ($\leq^p_{bdtt}$ ($\leq^p_{bctt}$)-reducible) to A_2, iff $A_1 \leq^p_{k\text{-}dtt}(\leq^p_{k\text{-}ctt}) A_2$ for some integer k.

5. A_1 is positive truth-table reducible to A_2 ($\leq^p_{ptt}$-reducible) [Sel82] iff $A_1 \leq^p_{tt} A_2$ by some tt function f such that for all sets X_1, X_2, Y_1 and Y_2: if $X_1 \leq^p_{tt} X_2$ via f, $X_2 \subseteq Y_2$ and $Y_1 \leq^p_{tt} Y_2$ via f, then $X_1 \subseteq Y_1$.

We will consider languages that are reducible to sparse and tally sets. Let r be any of the above reductions. Then,

$$\mathrm{SPARSE} = \{S \mid S \text{ is a sparse set}\}.$$

$$\text{co-SPARSE} = \{S \mid \overline{S} \text{ is a sparse set}\}.$$

$$\text{TALLY} = \{T \mid T \text{ is a tally set}\}.$$

$$R_r(\text{SPARSE}) = \{A \mid A \leq_r^p S \text{ for some } S \in \text{SPARSE}\}.$$

$$R_r(\text{TALLY}) = \{A \mid A \leq_r^p T \text{ for some } T \in \text{TALLY}\}.$$

2.4 Kolmogorov complexity

The *Kolmogorov complexity* of a string x, $K(x)$, is the size of the smallest index of a Turing machine that generates x and halts. A *Kolmogorov random* string is a string x such that $K(x) \geq |x|$. For a more detailed description see for example [LV93].

3 Conjunctive Reductions to Tally Sets

Theorem 1 SPARSE $\subseteq R_{ctt}(\text{TALLY})$.

Proof: Let S be a sparse set and let $d(n)$ a polynomial upper bound on its density, where d is a polynomial time computable function. Such a function d exists for every sparse set. We show that $S \in R_{ctt}(\text{TALLY})$.

We have to build a $\leq_{ctt}^p$ reduction g from S to a tally set T. We can insure that $\text{Ass}(g(x)) \cap \text{Ass}(g(y)) = \emptyset$ for $|x| \neq |y|$ by building g such that every element of $\text{Ass}(g(x))$ is of the form $0^{\langle n,j \rangle}$, where n is the length of x. In the following, let $x_1, \cdots, x_{2^n}$ be the 2^n strings of length n. Note that if g is a reduction from S to T, then $x_i \in S \Leftrightarrow \text{Ass}(g(x_i)) \subseteq T$. Since this property holds for all x_i, a $\leq_{ctt}^p$ reduction generates a family of 2^n tally sets such that for all $x_i \notin S$: $\text{Ass}(g(x_i)) \not\subseteq \bigcup_{x_j \in S} \text{Ass}(g(x_j))$. Whether the reduction is possible depends on whether we can efficiently construct such a family of sets. The existence of these kinds of families have been studied in [EFF82, EFF85, NW88]. We will construct a family of sets $\mathcal{F} = \{Q_1, \cdots, Q_{2^n}\}$, with the following properties:

1. $Q_i \in \text{TALLY}$,
2. Q_i can be generated in polynomial time (in n),
3. For any $d(n)+1$ sets $Q_{i_1}, \cdots, Q_{i_{d(n)}}, Q_k \in \mathcal{F}$ such that $k \notin \{i_1, \cdots, i_{d(n)}\}$, $Q_k \not\subseteq \bigcup_{j=1}^{d(n)} Q_{i_j}$.

If we set the tally set $T = \bigcup_{x_i \in S} Q_i$, then $x_i \in S$ if and only if $Q_i \subseteq T$, since S is of density $d(n)$. If we are able to generate Q_i in polynomial time (in n), then we can define the $\leq^p_{ctt}$reduction f from $S^{=n}$ to T by $\mathrm{Ass}(f(x_i)) = Q_i$. First we show by the next lemma that property 3 above follows from the following stronger property which is easier to verify.

Lemma 1.1 *Let $\mathcal{F} = \{Q_1, \cdots, Q_{2^n}\}$ be a family of sets such that for some $r > 0$, $\|Q_i\| > r{\cdot}d(n)$ and $\|Q_i \bigcap Q_j\| \leq r$, for $i \neq j$. Then, for any $d(n)+1$ sets $Q_{i_1}, \cdots, Q_{i_{d(n)}}, Q_k \in \mathcal{F}$ such that $k \notin \{i_1, \cdots, i_{d(n)}\}$, $Q_k \not\subseteq \bigcup_{j=1}^{d(n)} Q_{i_j}$.*

Proof: Suppose this is not true i.e. there exist $d(n)+1$ sets $Q_{i_1}, \cdots, Q_{i_{d(n)}}, Q_k \in \mathcal{F}$ such that $k \notin \{i_1, \cdots, i_{d(n)}\}$, and $Q_k \subseteq \bigcup_{j=1}^{d(n)} Q_{i_j}$. Since $\|Q_k\| > r{\cdot}d(n)$, there must exist a j such that $1 \leq j \leq d(n)$ and $\|Q_k \bigcap Q_{i_j}\| > r$. But this contradicts the fact that the size of the intersection of any two different sets is at most r. $\Box$

One way to construct these families is as follows. Let $GF(p)$ be a finite field with a prime number of elements. Note here that we can always find a prime between x and $2x$ [Che52].

We consider polynomials over $GF(p)$, for p prime. We need an easy fact about roots of polynomials over finite fields. For more detail see section 6.6 in [Coh74].

FACT 1.1 *Two different polynomials of degree $\leq r$ can not intersect on more than r points in $GF(p)$.*

We represent a polynomial of degree $\leq r$ by its $r+1$ coefficients. We view each polynomial as a $(r+1)$-digit number in base p. With the i^{th} polynomial, denoted by q_i, we mean the polynomial whose representation is the number base p that represents i. Consider the following family of sets: $Q_i = \{0^{\langle n, a, q_i(a) \rangle} \mid a \in GF(p)\}$. We will choose r and p such that the conditions of lemma 1.1 are fulfilled. Observe that Q_i is a tally set of size p, and that for two different polynomials, q_i and q_j, $\|Q_i \bigcap Q_j\| \leq r$. It remains to force the following requirements:

1. $p^{r+1} \geq 2^n$ (We need 2^n different sets)

2. $r{\cdot}d(n) < p$ (to fulfill the requirements of lemma 1.1)

It is easy to verify that taking $r = \lceil \frac{2n}{\log n} \rceil$, and p the first prime larger than $r{\cdot}d(n)$ fulfills these two requirements.

The only thing remaining is to show that we can generate the i^{th} set Q_i in polynomial time (in n). First we have to compute the prime number p. Since the length of the binary representation of $r{\cdot}d(n)$ is in $O(\log(n))$ and because there is a prime between $r{\cdot}d(n)$ and $2r{\cdot}d(n)$, we can do a brute force search (or do a more sophisticated sieve method [Pri83]) in polynomial time. Next we have to pick the i^{th} polynomial over $GF(p)$ (can easily be done in polynomial time), and compute Q_i. Since p is a prime number, the operations in $GF(p)$ are simply multiplication and addition modulo p, which also can be done in polynomial time. $\Box$

Recall that the $\leq_{ctt}^{p}$reduction f from $S^{=n}$ to $\bigcup_{x_i \in S} Q_i$ is defined by $\mathrm{Ass}(f(x_i)) = Q_i$. Since $\|Q_i\| = p \leq 2r \cdot d(n) \leq \frac{4nd(n)}{\log n}$, we have in fact shown that $S \in R_{O(\frac{nd(n)}{\log n})-ctt}(\text{TALLY})$. As recently shown by Saluja [Sal93], this bound is optimal.

Notice that if we consider probabilistic reductions, we can randomly choose exactly one of the strings from $\mathrm{Ass}(f(x))$ and get a many-one reduction with a one-sided error. This observation is due to Schöning in [Sch93], where he shows that every sparse set many-one reduces to a tally set by a polynomial time, randomized procedure.

Corollary 1 $R_{ctt}(\text{SPARSE}) = R_{ctt}(\text{TALLY})$.

Corollary 2 co-SPARSE $\subseteq R_{dtt}(\text{TALLY})$.

Proof: If A is $\leq_{ctt}^{p}$-reducible to a tally set, then $\overline{A}$ is $\leq_{dtt}^{p}$-reducible to a tally set. $\Box$

The following Theorem can be derived using Theorem 1. It refutes another of the conjectures from [Ko89]. (The conjecture was that $R_{bdtt}(\text{SPARSE}) \not\subseteq R_{ctt}(\text{SPARSE})$.)

Theorem 2 $R_{bdtt}(\text{SPARSE}) \subseteq R_{ctt}(\text{TALLY})$.

Proof: Let A be $\leq_{k\text{-}dtt}^{p}$-reducible to some sparse set S via f. Using Theorem 1 we get that S is $\leq_{ctt}^{p}$-reducible to some tally set T_S via g. We will construct a tally set T and a reduction h such that $A \leq_{ctt}^{p} T$ via h. Define

$$T = \{0^{\langle n_1, \cdots, n_k \rangle} \mid n_j \in I\!N \text{ and } \exists i : 0^{n_i} \in T_S\}.$$

In the following it is convenient to view T as a Cartesian product. For $A_1, \cdots, A_k$ tally sets, let

$$A_1 \times \cdots \times A_k = \{0^{\langle n_1, \cdots, n_k \rangle} \mid 0^{n_i} \in A_i\}.$$

Define the $\leq_{ctt}^{p}$ reduction h as follows: if $f(x) = \langle \langle y_1, \cdots, y_k \rangle, \alpha \rangle$, then let $\mathrm{Ass}(h(x)) = \mathrm{Ass}(g(y_1)) \times \cdots \times \mathrm{Ass}(g(y_k))$. Note that h is polynomial time computable, since both f and g are. It remains to show that h reduces A conjunctively to T.

$$x \in A \quad \Rightarrow \quad \exists i : y_i \in S$$

$$
\begin{aligned}
&\Rightarrow \quad \exists i : \mathrm{Ass}(g(y_i)) \subseteq T_S \\
&\Rightarrow \quad \mathrm{Ass}(g(y_1)) \times \cdots \times \mathrm{Ass}(g(y_k)) \subseteq T. \\
x \notin A \quad &\Rightarrow \quad \forall i : y_i \notin S \\
&\Rightarrow \quad \forall i \exists 0^{n_i} : 0^{n_i} \in \mathrm{Ass}(g(y_i)) \text{ and } 0^{n_i} \notin T_S \\
&\Rightarrow \quad 0^{\langle n_1, \cdots, n_k \rangle} \notin T \\
&\Rightarrow \quad \mathrm{Ass}(g(y_1)) \times \cdots \times \mathrm{Ass}(g(y_k)) \not\subseteq T.
\end{aligned}
$$

□

Theorem 1 offers a new understanding of the class R_{ctt}(SPARSE) and as such, it has been used in [AKM92] to prove various results.

To understand the relationship between sparse and tally sets, it is important to know which reductions are able to differentiate between tally and sparse sets, and which aren't. It is well-known that R_{tt}(SPARSE)= R_{tt}(TALLY) [HIS85] and our corollary 1 gives the analog for $\leq^p_{ctt}$ reductions. On the other hand, there *do* exist reductions that are more powerful with sparse oracles than with tally oracles: This holds for instance for many-one reductions and for disjunctive truth-table reductions [Ko89].

As the next Theorem shows, *positive* truth-table reductions on sparse and tally sets behave like $\leq^p_{ctt}$ reductions and not like $\leq^p_{dtt}$ reductions:

Theorem 3 *R_{ptt}(SPARSE)= R_{ptt}(TALLY).*

The result follows immediately from the following Theorem that claims that $\leq^p_{ptt}$ reductions to tally sets capture the class R_{tt}(TALLY).

Theorem 4 *R_{tt}(TALLY)= R_{ptt}(TALLY).*

Proof: Let A be a set in R_{tt}(TALLY), and suppose T is a tally set such that $A \leq^p_{tt} T$ by a tt-function f that is computable in time $p(n)$ where p is a polynomial. We have to show that $A \in R_{ptt}$(TALLY). We define the tally set T', that will witness the fact that $A \in R_{ptt}$(TALLY), as follows:

$$T' = \{0^{\langle n, 0 \rangle} \mid 0^n \in T\} \cup \{0^{\langle n, 1 \rangle} \mid 0^n \notin T\}.$$

We claim that $A \leq^p_{ptt} T'$ by the following reduction:

On input x of length n do the following:

1. If there exists an $m \leq p(n)$ such that $0^{\langle m, 0\rangle}$ and $0^{\langle m, 1\rangle}$ are both *not* in the oracle set, then reject;

2. else, if there exists an $m \leq p(n)$ such that $0^{\langle m, 0\rangle}$ and $0^{\langle m, 1\rangle}$ are both *in* the oracle set, then accept;

3. otherwise, simulate the old tt-function f on input x, replacing each query 0^m by $0^{\langle m, 0\rangle}$.

It is immediate that this reduction reduces A to T', since by definition of T' we are always in case 3, which implies that we just simulate f. It remains to show that the reduction is positive. Suppose for a contradiction that it isn't. Then there exist a string x of length n and two oracle sets $X \subset Y$ such that x is accepted with oracle X and rejected with oracle Y. Since x is accepted with oracle X, we cannot be in case 1, that is, it must be the case that for all $m \leq p(n)$ either $0^{\langle m, 0\rangle} \in X$, or $0^{\langle m, 1\rangle} \in X$. Now look at Y. If $Y \setminus X$ does not contain strings of the form $0^{\langle m, i\rangle}$ for $m \leq p(n), i \in \{0, 1\}$, then $f(x)$ with oracle Y behaves in exactly the same way as $f(x)$ with oracle X. In particular, x is accepted, which contradicts our assumption. Therefore, suppose that for some $m \leq p(n)$ and $i \in \{0, 1\}$ it is the case that $0^{\langle m, i\rangle}$ occurs in Y but not in X. Then it must be the case that $0^{\langle m, |1-i|\rangle} \in X$, and therefore, since $X \subseteq Y$, both $0^{\langle m, 0\rangle}$ and $0^{\langle m, 1\rangle}$ are in Y. This implies that we are in case 2, and thus, x is accepted contrary to the assumption. □

Note that by the construction, it is immediate that T' is 1-tt reducible to T.

4 Conjunctive and Disjunctive Reductions

Gavaldà and Watanabe [GW] showed that $R_{ctt}(\text{SPARSE}) \not\subseteq R_{dtt}(\text{SPARSE})$. Combining this result with Theorem 1, we can quickly derive the following Theorem of Ko:

Theorem 5 ([Ko89]) $R_{dtt}(\text{SPARSE}) \not\subseteq R_{ctt}(\text{SPARSE})$.

Proof: Let A be a set in $R_{ctt}(\text{SPARSE})$, that is not in $R_{dtt}(\text{SPARSE})$. Consider the set $\overline{A}$. Since $A \in R_{ctt}(\text{SPARSE})$ and $R_{ctt}(\text{SPARSE}) = R_{ctt}(\text{TALLY})$ by Theorem 1, we have that $A \in R_{ctt}(\text{TALLY})$. By simple complementation, it follows that $\overline{A} \in R_{dtt}(\text{TALLY})$ and therefore, $\overline{A} \in R_{dtt}(\text{SPARSE})$. Now, we see that $\overline{A}$ can not be in $R_{ctt}(\text{SPARSE})$. For suppose $\overline{A} \in R_{ctt}(\text{SPARSE})$. Then, again using Theorem 1, $\overline{A} \in R_{ctt}(\text{TALLY})$, so $A \in R_{dtt}(\text{TALLY}) \subseteq R_{dtt}(\text{SPARSE})$, contradicting our choice of A. □

Gavaldà and Watanabe's proof actually provides something stronger. They show that

$$R_{f(n)\text{-}ctt}(\text{SPARSE}) \not\subseteq R_{dtt}(\text{SPARSE})$$

for any polynomial time computable unbounded function f. Ko's proof of Theorem 5 does not seem to provide this generalization, and the above proof does not generalize directly, because when we go conjunctively from a sparse set to a tally set, we need a polynomial number of queries. To be able to use the previous argument, while keeping the number of queries small, we need a strengthening of Gavaldá and Watanabe's Theorem to tally sets:

Theorem 6 *For any polynomial time computable unbounded function f, $R_{f(n)\text{-}ctt}(\text{TALLY}) \not\subseteq R_{dtt}(\text{SPARSE})$.*

Proof: If we can prove the theorem for small functions f, it is immediately true for larger functions, so we may assume $f(n) \le \log n$. For every n, let x_n be a Kolmogorov random string of length n. Define

$$\begin{aligned} A = \{ \quad & \langle 0^n, \langle i_1, b_1\rangle, \cdots, \langle i_{f(n)}, b_{f(n)}\rangle\rangle \text{ such that} \\ & 1 \le i_1 < i_2 < \cdots < i_{f(n)} \le n \text{ and} \\ & \text{for every } j, \text{ the } i_j\text{-th bit of } x_n \text{ is } b_j\}. \end{aligned}$$

It is immediate that $A \le^p_{f(n)\text{-}ctt} T$, where

$$T = \{0^{\langle n,i,b\rangle} | \text{ the } i\text{-th bit of } x_n \text{ is } b\}.$$

To show that A is not $\le^p_{dtt}$-reducible to any sparse set, leading to a contradiction, assume $A \le^p_{dtt} S$, via reduction h, where h is n^c time computable and $\|S^{\le n}\| \le n^c$.

Let A_n be the set of all strings of A of the form $\langle 0^n, \cdots\rangle$. We will show that there is a string y_n in S that is queried by many strings from A_n (Lemma 6.1). Suppose that a string $\langle 0^n, \langle i_1, b_1\rangle, \cdots, \langle i_{f(n)}, b_{f(n)}\rangle\rangle$ queries the string y_n. Since h is a $\le^p_{dtt}$reduction from A to S and $y_n \in S$, this provides us with the $f(n)$ bits $i_1, i_2, \cdots, i_{f(n)}$ of x_n. By a careful counting argument, we show below that, for n large enough, we get enough bits of x_n from y_n to contradict the randomness of x_n.

Lemma 6.1 *There exist a constant d and for every n a string y_n in S such that:*

$$\|\{z \in A_n | \; y_n \in Ass(h(z))\}\| \ge n^{\frac{1}{2}f(n)-d}.$$

Proof: The number of strings in A_n is $\begin{pmatrix} n \\ f(n) \end{pmatrix} \geq \left(\frac{n}{f(n)}\right)^{f(n)}$. Thus, for $f(n) \leq n^{\frac{1}{2}}$, $\|A_n\| \geq n^{\frac{1}{2}f(n)}$. For each string z in A_n, there is a string in $S \cap \mathrm{Ass}(h(z))$. Since strings in A_n are certainly of length less than $2n$, the queried strings are of length at most $(2n)^c$. Thus, there are at most $((2n)^c)^c = (2n)^{c^2}$ strings of S in $\cup_{z \in A_n} \mathrm{Ass}(h(z))$. There must be a string y_n in that set that is in $\mathrm{Ass}(h(z))$ for at least $\|A_n\|/(2n)^{c^2}$ many z's. Since $\|A_n\| \geq n^{\frac{1}{2}f(n)}$, $\|A_n\|/(2n)^{c^2} \geq n^{\frac{1}{2}f(n)-d}$ for a suitable d. □

Given a set $Y \subseteq A_n$, let I_Y be the set of indices i_j that are mentioned in the strings from Y.

Lemma 6.2 *Let $Y \subseteq A_n$, then $\|Y\| \leq \|I_Y\|^{f(n)}$.*

Proof: Each string in Y mentions exactly $f(n)$ bits of I_Y. There are exactly $\begin{pmatrix} \|I_Y\| \\ f(n) \end{pmatrix}$ ways to select $f(n)$ bits from the set of indices I_Y, so

$$\|Y\| \leq \begin{pmatrix} \|I_Y\| \\ f(n) \end{pmatrix} \leq \|I_Y\|^{f(n)}.$$

□

Lemma 6.3 *There exists a string $y_n \in S$ such that for the set Y of strings in A_n that query y_n: $\|I_Y\| \geq n^{\frac{1}{2}-d/f(n)}$.*

Proof: Let y_n be given by Lemma 6.1, and let Y be the set of strings z in A_n such that $y_n \in \mathrm{Ass}(h(z))$. Then, by Lemma 6.2,

$$n^{\frac{1}{2}f(n)-d} \leq \|I_Y\|^{f(n)}.$$

$$\|I_Y\| \geq n^{(\frac{1}{2}f(n)-d)/f(n)} = n^{\frac{1}{2}-d/f(n)}.$$

□

Now, to derive a contradiction, we show how to describe x_n with fewer than n bits. To describe x_n, use the string y_n from Lemma 6.3. To compute y_n, we need one of the strings $z \in A_n$ that query y_n, and the index of y_n in the set of queries. The string z can be described using $O(f(n)\log n)$ bits and the index can be described in $O(\log n)$ bits. It follows that y_n can be described using $O(f(n)\log n)$ bits. Given y_n, we can compute all the bits of x_n that are mentioned in strings from the set Y of strings in A_n that query y_n.

Now look at the sequence containing all the bits of x_n that are not mentioned by Y. This requires $n - \|I_Y\| \leq n - n^{\frac{1}{2}-d/f(n)}$ bits. Since the bits described by Y all contain their index, they can be inserted into their respective position. The total number of bits to describe x_n is $n - n^{\frac{1}{2}-d/f(n)} + O(f(n)\log n)$, which is strictly less than n if $f(n)$ is unbounded and $\leq \log n$. □

Now we can derive the wanted Theorem.

Theorem 7 *For any polynomial time computable unbounded function f, $R_{f(n)\text{-}dtt}(\text{TALLY}) \not\subseteq R_{ctt}(\text{SPARSE})$.*

Proof: Using Theorem 6, we can use the same reasoning as in the proof of Theorem 5. Since we start from a tally set, we don't have the problem associated with the blow up in number of queries. □

The following corollaries can all be obtained from Theorem 6 and Theorem 7.

Corollary 3 *For any polynomial time computable unbounded function f, $R_{f(n)\text{-}ctt}(\text{SPARSE})$ and $R_{f(n)\text{-}dtt}(\text{SPARSE})$ are not closed under complementation.*

Corollary 4 *For any polynomial time computable unbounded function f, $R_{f(n)\text{-}ctt}(\text{SPARSE})$ and $R_{f(n)\text{-}dtt}(\text{SPARSE})$ are incomparable.*

Corollary 5 *For any polynomial time computable unbounded function f, $R_{f(n)\text{-}dtt}(\text{SPARSE})$ and $R_{f(n)\text{-}ctt}(\text{SPARSE})$ are strictly included in $R_{f(n)\text{-}tt}(\text{SPARSE})$.*

These results hold for the corresponding $R_r(\text{TALLY})$ classes as well. For bounded conjunctive and disjunctive reductions to sparse sets, we get the following analog:

Theorem 8 *For all $k \geq 1$, $R_{k\text{-}ctt}(\text{SPARSE})$, $R_{k\text{-}dtt}(\text{SPARSE})$, $R_{bdtt}(\text{SPARSE})$ and $R_{bctt}(\text{SPARSE})$ are not closed under complementation, and therefore strictly included in $R_{btt}(\text{SPARSE})$.*

Proof:

It is not hard to see that if $R_{bdtt}(\text{SPARSE})$ is closed under complementation, then $R_{1\text{-}tt}(\text{SPARSE}) \subseteq R_{bdtt}(\text{SPARSE})$. By Theorem 2, it follows that $R_{1\text{-}tt}(\text{SPARSE}) \subseteq R_{ctt}(\text{SPARSE})$, contradicting [Ko89]. For the bounded conjunctive case we can argue in a similar way.

□

Note that this Theorem does not hold for the corresponding R_r(TALLY) classes: It follows from [Ko89] that $R_m(\text{TALLY}) = R_{k\text{-}ctt}(\text{TALLY}) = R_{k\text{-}dtt}(\text{TALLY}) = R_{btt}(\text{TALLY})$, and thus all these classes are closed under complementation.

Acknowledgements

We would like to thank Lance Fortnow for pointing out the relevance of [NW88], and Peter Erdös for giving us a copy of [EFF85]. We also thank Ricard Gavaldà for providing us with a preliminary version of one of the proofs in [GW] before it was available for general distribution, Peter van Emde Boas for discussing algebra with us, and two anonymous referees for helpful comments.

References

[AHH+92] V. Arvind, Y. Han, L. Hemachandra, J. Köbler, A. Lozano, M. Mundhenk, M. Ogiwara, U. Schöning, R. Silvestri, and T. Thierauf. Reductions to sets of low information content. In *Proceedings of the 19th International Colloquium on Automata, Languages, and Programming*, 1992.

[AHOW92] E. Allender, L. Hemachandra, M. Ogiwara, and O. Watanabe. Relating equivalence and reducibility to sparse sets. *SIAM J. Comput.*, 21(3):521–539, 1992.

[AKM92] V. Arvind, J. Köbler, and M. Mundhenk. On bounded truth-table, conjunctive, and randomized reductions to sparse sets. In *Proceedings 12th Conference on the Foundations of Software Technology & Theoretical Computer Science*, 1992.

[BK88] R. Book and K. Ko. On sets truth-table reducible to sparse sets. *SIAM J. Comput.*, 17:903–919, 1988.

[Che52] L. Chebyshev. Mémoire sur les nombres premiers. *Journal de Math.*, 17:366–390, 1852.

[Coh74] P.M. Cohn. *Algebra Volume 1.* John Wiley & Sons, 1974.

[EFF82] P. Erdös, P. Frankl, and Z. Füredi. Families of finite sets in which no set is covered by the union of two others. *Journal of Combinatorial Theory, Series A*, 33:158–166, 1982.

[EFF85] P. Erdös, P. Frankl, and Z. Füredi. Families of finite sets in which no set is covered by the union of r others. *Israel Journal of Mathematics*, 51:79–89, 1985.

[GW] R. Gavaldà and O. Watanabe. On the computational complexity of small descriptions. To appear in SIAM J. Comput. Appeared in preliminary version in [GW91].

[GW91] R. Gavaldà and O. Watanabe. On the computational complexity of small descriptions. In *Proc. Structure in Complexity Theory sixth annual conference*, pages 89–101. IEEE Computer Society Press, 1991.

[HIS85] J. Hartmanis, N. Immerman, and V. Sewelson. Sparse sets in NP-P: EXPTIME versus NEXPTIME. *Inf. Control*, 65:158–181, 1985.

[HOW92] L. Hemachandra, M. Ogiwara, and O. Watanabe. How hard are sparse sets? In *Proc. Structure in Complexity Theory, seventh annual conference*, pages 222–238. IEEE Computer Society Press, 1992.

[Ko89] K. Ko. Distinguishing conjunctive and disjunctive reducibilities by sparse sets. *Information and Computation*, 81:62–87, 1989.

[LLS75] R. Ladner, N. Lynch, and A. Selman. A comparison of polynomial time reducibilities. *Theor. Comput. Sci.*, 1:103–123, 1975.

[LV93] M. Li and Paul Vitányi. *An Introduction to Kolmogorov Complexity and its Applications.* Texts and Monographs in Computer Science. Springer-Verlag, 1993.

[NW88] N. Nisan and A. Wigderson. Hardness vs. randomness. In *Proc. 29th IEEE Symposium on Foundations of Computer Science*, pages 2–11, 1988.

[Pri83] P. Pritchard. Prime number sieves. *J. of Algorithms*, 4:332–344, 1983.

[RRW94] Rao, Rothe, and Watanabe. Upward separation for FewP and related classes. Technical Report TR 488, University of Rochester, Feb 1994. To appear in *Info. Proc. Letters.*

[Sal93] S. Saluja. Relativized limitations of left set technique and closure classes of sparse sets. In *Proc. Structure in Complexity Theory eighth annual conference.* IEEE Computer Society Press, 1993.

[Sch93] U. Schöning. On random reductions from sparse sets to tally sets. *Info. Proc. Letters*, 46:239–241, 1993.

[Sel82] A. Selman. Analogues of semirecursive sets and effecitve reducibilities to the study of NP complexity. *Information and Control*, 52(1):36–51, 1982.

[Wat] O. Watanabe. Private communication.