Weak Cardinality Theorems for First-Order Logic (Extended Abstract)

Till Tantau
Technische Universität Berlin
Fakultät für Elektrotechnik und Informatik
10587 Berlin, Germany
Fax +49-30-314-73500
tantau@cs.tu-berlin.de

February 25, 2003

Abstract

Kummer's cardinality theorem states that a language is recursive if a Turing machine can exclude for any n words one of the $n + 1$ possibilities for the number of words in the language. It is known that this theorem does not hold for polynomial-time computations, but there is evidence that it holds for finite automata: at least weak cardinality theorems hold for finite automata. This paper shows that some of the recursion-theoretic and automata-theoretic weak cardinality theorems are instantiations of purely logical theorems. Apart from unifying previous results in a single framework, the logical approach allows us to prove new theorems for other computational models. For example, weak cardinality theorems hold for Presburger arithmetic.

1 Introduction

Given a language A and n input words, we often wish to know which of these words are in the language. For languages like the satisfiability problem this problem is presumably difficult to solve, for languages like the halting problem it is impossible to solve. To tackle such problems, Gasarch [7] has proposed to study a simpler problem instead: we just *count how many* of the input words are elements of A. To make things even easier, we do not require this number to be computed exactly, but only approximately. Indeed, let us just try to *exclude* one possibility for the number of input words in A.

In recursion theory, Kummer's cardinality theorem [17] states that, using a Turing machine, excluding one possibility for the number of input words in A is just as hard as deciding A. It is not known whether this statement carries over to automata theory, that is, it is not known whether a language A must be regular if a finite automaton can always exclude one possibility for the number of input words in A. However, several *weak* forms of this theorem are known in automata theory. For example, for $n = 2$ the cardinality theorem is known to hold also for finite automata [26].

These parallels between recursion and automata theory are surprising insofar as computational models 'in between' exhibit a different behaviour: there are languages A outside the class P of problems decidable in polynomial time for which we *can* always exclude, in polynomial time, for any n words one possibility for their number in A.

The present paper explains (at least partly) *why* the parallels between recursion and automata theory exist and why they are not shared by the models in between. Basically, the weak cardinality theorems for Turing machines and finite automata are just different instantiations of the same logical theorems. These logical theorems cannot be instantiated for polynomial time since polynomial time lacks a logical characterisation in terms of elementary definitions.

Using logic for the formulation and proof of the weak cardinality theorems has another advantage, apart from unifying previous results. Theorems formulated for arbitrary logical structures can be applied to new fields: the weak cardinality theorems all hold for Presburger arithmetic and the nonspeedup theorem also holds for ordinal number arithmetic.

In the logical setting, 'computational models' are replaced by 'logical structures' and 'computation' is replaced by 'elementary definition'. For example, the cardinality theorem for $n = 2$ now becomes the following statement: Let $\mathcal{S}$ be a logical structure with universe U that satisfies certain requirements. If for some set A and some number n we can elementarily define a function $f\colon U \times U \to \{0, 1, 2\}$ in $\mathcal{S}$ such that $f(x, y) \neq |\{x, y\} \cap A|$ for all x and y, then A is elementarily definable in $\mathcal{S}$.

One of the applications of cardinality computations is in the study of separability. As argued in [27], 'cardinality theorems are separability results in disguise'. In recursion theory and in automata theory one can rephrase the weak cardinality theorems as separability results. Such a rephrasing is also possible for first-order logic and we can formulate purely logical separability theorems that are interesting in their own right. An example of such a theorem is the following statement: Let $\mathcal{S}$ be a logical structure satisfying certain requirements and let A be a subset of $\mathcal{S}$'s universe. If there exist elementarily definable supersets of $A \times A$, $A \times \bar{A}$, and $\bar{A} \times \bar{A}$ whose intersection is empty, then A is elementarily definable in $\mathcal{S}$.

This paper is organised as follows. In section 2 the history of the cardinality theorem is retraced and the weak cardinality theorems are formulated rigorously. Section 3 prepares the logical formulation of the weak cardinality theorems. It is shown how the class of regular languages and the class of recursively enumerable languages can be characterised in terms of appropriate elementary definitions. In section 4 the weak cardinality theorems for first-order logic are formulated. In section 5 applications of the theorems to separability are discussed.

In this extended abstract all proofs are given in the technical appendix.

2 History of the Cardinality Theorem

2.1 The Cardinality Theorem for Recursion Theory

For a set A, the *cardinality function* $\#_A^n$ takes n words as input and yields the number of words in A as output, that is, $\#_A^n(w_1, \ldots, w_n) = |\{w_1, \ldots, w_n\} \cap A|$. The cardinality function and the idea of 'counting input words', due to Gasarch [7] in its general form, play an important role in a variety of proofs both in complexity theory [19, 13, 24, 9, 15] and recursion theory [17, 18, 4]. For example, the core idea of the Immerman–Szelepcsényi theorem is to *count* the number of reachable vertices in a graph in order to *decide* the reachability problem.

One way of quantifying the complexity of $\#_A^n$ is to consider its *enumeration complexity*, which is the smallest number m such that $\#_A^n$ is m-enumerable. Enumerability, which was first defined by Cai and Hemaspaandra [6] in the context of polynomial-time computations and which was later transfered to recursive computations, can be regarded as 'generalised approximation'. It is defined as follows: a function f, taking n tuples of words as input, is *m-Turing-enumerable* if there exists a Turing machine that on input w_1, ... , w_n starts a possibly infinite computation during which it prints words onto an output tape. At most m different words may be printed and one of them must be $f(w_1, \ldots, w_n)$.

Intuitively, the larger m, the easier it should be to m-Turing-enumerate $\#_A^n$. *This intuition is wrong.* Kummer's cardinality theorem, see below, states that even n-Turing-enumerating $\#_A^n$ is just as hard as deciding A. In other words, excluding just one possibility for $\#_A^n(w_1, \ldots, w_n)$ is just as hard as deciding A. Intriguingly, the intuition *is* correct for polynomial-time computations since the work of Gasarch, Hoene, and Nickelsen [7, 12, 21] shows that a polynomial-time version of the cardinality theorem does not hold.

Theorem 2.1 (Cardinality theorem [17]). *If $\#_A^n$ is n-Turing-enumerable, then A is recursive.*

The cardinality theorem has applications for instance in the study of semirecursive sets [14], which play a key role in the solution of Post's problem [23]. The proof of the cardinality theorem is difficult. Several less general results had already been proved when Kummer wrote his paper 'A Proof of Beigel's Cardinality Conjecture' [17]. The title of Kummer's paper refers to the fact that Richard Beigel was the first to conjecture the cardinality theorem as a generalisation of his so-called 'nonspeedup theorem' [3]. In the following formulation of the nonspeedup theorem χ_A^n denotes the n-fold characteristic function of A. The nonspeedup theorem is a simple consequence of the cardinality theorem.

Theorem 2.2 (Nonspeedup theorem [3]). *If χ_A^n is n-Turing-enumerable, then A is recursive.*

Owings [22] succeeded in proving the cardinality theorem for $n = 2$. For larger n he could only show that if $\#_A^n$ is n-Turing-enumerable, then A is recursive in the halting problem. Harizanov et al. [8] have formulated a restricted cardinality theorem, whose proof is somewhat simpler than the proof of the full cardinality theorem.

Theorem 2.3 (Restricted cardinality theorem [8]). *If $\#_A^n$ is n-Turing-enumerable via a Turing machine that never enumerates both 0 and n simultaneously, then A is recursive.*

2.2 Weak Cardinality Theorems for Automata Theory

If we restrict the computational power of Turing machines, the cardinality theorem no longer holds [7, 12, 21]: there are languages $A \notin \mathrm{P}$ for which we can always exclude one possibility for $\#_A^n(w_1, \dots, w_n)$ in polynomial time. However, if we restrict the computational power even further, namely if we consider finite automata, there is strong evidence that the cardinality theorem holds once more, see the following conjecture:

Conjecture 2.4 ([26]). *If $\#_A^n$ is n-fa-enumerable, then A is regular.*

The conjecture refers to the notion of *m-enumerability by finite automata.* This notion was introduced in [25] and is defined as follows: A function f is *m-fa-enumerable* if there exists a finite automaton for which for every input tuple $(w_1, \dots, w_n)$ the output attached to the last state reached is a set of at most m values that contains $f(w_1, \dots, w_n)$. The different components of the tuple are put onto n different tapes, shorter words padded with blanks, and the automaton scans the tapes synchronously, which means that all heads advance exactly one symbol in each step. The same method of feeding multiple words to a finite automaton has been used in [16, 2, 1].

In a line of research [16, 2, 1, 25, 26, 27], the following three theorems were established. They support the above conjecture by showing that all of the historically earlier, weak forms of the recursion-theoretic cardinality theorem hold for finite automata.

Theorem 2.5 ([25]). *If χ_A^n is n-fa-enumerable, then A is regular.*

Theorem 2.6 ([26]). *If $\#_A^2$ is 2-fa-enumerable, then A is regular.*

Theorem 2.7 ([26, 2]). *If $\#_A^n$ is n-fa-enumerable via a finite automaton that never enumerates both 0 and n simultaneously, then A is regular.*

3 Computational Models as Logical Structures

The aim of formulating purely logical versions of the weak cardinality theorems is to abstract from concrete computational models. The present section explains which logical abstraction is used in later sections.

3.1 Presburger Arithmetic

Let us start with an easy example: Presburger arithmetic. This notion is easily transfered to a logical setting—it is defined in terms of first-order logic in the first place: A set A of natural numbers is called *definable in Presburger arithmetic* if there exists a first-order formula $\phi(x)$ over the signature $\{+^2\}$ such that $a \in A$ iff $\phi(x)$ holds if we interpret x as a and the symbol $+$ as the normal addition of natural numbers. For example, the set of even natural numbers is definable in Presburger arithmetic using the formula $\phi(x) = \exists y\,(y + y = x)$.

In the abstract logical setting used in the next sections, the 'computational model Presburger arithmetic' is represented by the logical structure $(\mathbb{N}, +)$. The class of languages the are 'computable in Presburger arithmetic' is given by the class of languages that are elementarily definable in $(\mathbb{N}, +)$. Recall that a relation R is called *elementarily definable in a logical structure $\mathcal{S}$* if there exists a first-order formula $\phi(x_1, \dots, x_n)$ such that $(a_1, \dots, a_n) \in R$ iff $\phi(x_1, \dots, x_n)$ holds in $\mathcal{S}$ if we interpret each x_i as a_i.

3.2 Finite Automata

In order to make finite automata and regular languages accessible to a logical setting, for a given alphabet Σ we need to find a logical structure $\mathcal{S}_{\mathrm{REG}|\Sigma^*}$ with the following property: a language $A \subseteq \Sigma^*$ is regular iff it is elementarily definable in $\mathcal{S}_{\mathrm{REG}|\Sigma^*}$.

It is known that such a structure $\mathcal{S}_{\mathrm{REG}|\Sigma^*}$ exists: Büchi has proposed one [5], though a small correction is necessary as pointed out by McNaughton [20]. However, the elements of Büchi's structure are natural numbers, not words, and thus a reencoding is necessary. A more directly applicable structure is discussed in [27], where it is shown that the structure $(\Sigma^*, I_{\sigma_1}, \dots, I_{\sigma_{|\Sigma|}})$ has the desired properties. The relations I_{σ_i}, one for each symbol $\sigma_i \in \Sigma$, are binary relations that hold for a pair (u, v) of words if the $|v|$-th letter of u is σ_i.

3.3 Polynomial-Time Computations

There is no logical structure $\mathcal{S}$ such that the class of languages that are elementarily definable in $\mathcal{S}$ is exactly the class P of languages decidable in polynomial time. To see this, consider the relation $R = \{(M, t) \mid M \text{ halts on input } M \text{ after } t \text{ steps}\}$. This relation is in P, but the language defined by the first-order formula $\phi(M) = \exists t\, R(M, t)$ is exactly the halting problem. Thus in any logical structure in which we can elementarily define R we can also elementarily define the halting problem.

3.4 Turing Machines

On the one hand, the class of recursive languages cannot be defined elementarily: the argument for polynomial-time machines also applies here. On the other hand, the arithmetical hierarchy contains exactly the sets the are elementarily definable in $(\mathbb{N}, +, \cdot)$.

The most interesting case, the class of recursively enumerable languages, is more subtle. Since the class is not closed under complement, it cannot be characterised by elementary definitions. However, it can be characterised by *positive* elementary definitions, which are elementary definitions that do not contain negations: For every alphabet Σ there is a structure $\mathcal{S}_{\mathrm{RE}|\Sigma^*}$ such that a language $A \subseteq \Sigma^*$ is recursively enumerable iff it is positively elementarily definable in $\mathcal{S}_\Sigma$. An example of such a structure $\mathcal{S}_{\mathrm{RE}|\Sigma^*}$ is the following: its universe is Σ^* and it contains all recursively enumerable relations over the alphabet Σ^*.

4 Logical Versions of the Weak Cardinality Theorems

In this section the weak cardinality theorems for first-order logic are presented. The theorems are first formulated in terms of elementary definitions. This allows us to apply them to all computational models that can be characterised in terms of elementary definitions. As argued in the previous section, this includes Presburger arithmetic, finite automata, and the arithmetical hierarchy, but misses the recursively enumerable languages. This is remedied later in this section, where positive elementary definitions are discussed. It is shown that at least the nonspeedup theorem can be formulated in a 'positive' way. At the end of the section higher-order logics are briefly touched.

We are still missing one crucial definition for the formulation of the weak cardinality theorems: What does it mean that a function is m-enumerable in a logical structure?

Definition 4.1. Let $\mathcal{S}$ be a logical structure with universe U and m a positive integer. A function $f\colon U \to U$ is *elementarily m-enumerable in $\mathcal{S}$* if there exists a relation $R \subseteq U \times U$ with the following properties:

1. R is elementarily definable in $\mathcal{S}$,
2. the graph of f is contained in R,
3. R is m-bounded, that is, for every $x \in U$ there exist at most m different y with $(x, y) \in R$.

The definition is easily adapted to functions f that take more than one input or yield more than one output. This definition does, indeed, reflect the notion of enumerability: A function with finite range is m-fa-enumerable iff it is elementarily m-enumerable in $\mathcal{S}_{\mathrm{REG}|\Sigma^*}$; a function is m-Turing-enumerable iff it is positively elementarily m-enumerable in $\mathcal{S}_{\mathrm{RE}|\Sigma^*}$.

4.1 The Non-Positive First-Order Case

We are now ready to formulate the weak cardinality theorems for first-order logic. In the following theorems, a logical structure is called *well-orderable* if a well-ordering of its universe can be defined elementarily. For example $(\mathbb{N}, +)$ is well-orderable using the formula $\phi_{\leq}(x, y) = \exists z\, (x + z = y)$. The *cross product* of two function f and g is defined in the usual way by $(f \times g)(u, v) = \big(f(u), g(v)\big)$.

The first of the weak cardinality theorems, the nonspeedup theorem, is actually just a corollary of a more general theorem that is formulated first: the cross product theorem.

Theorem 4.2 (Cross product theorem). *Let $\mathcal{S}$ be a well-orderable logical structure with universe U. Let $f, g \colon U \to U$ be functions. If $f \times g$ is elementarily $(n + m)$-enumerable in $\mathcal{S}$, then f is elementarily n-enumerable in $\mathcal{S}$ or g is elementarily m-enumerable in $\mathcal{S}$.*

Theorem 4.3 (Nonspeedup theorem). *Let $\mathcal{S}$ be a well-orderable logical structure with universe U. Let $A \subseteq U$. If χ^n_A is elementarily n-enumerable in $\mathcal{S}$, then A is elementarily definable in $\mathcal{S}$.*

Theorem 4.4 (Cardinality theorem for two words). *Let $\mathcal{S}$ be a well-orderable logical structure with universe U. Let every finite relation on U be elementarily definable in $\mathcal{S}$. Let $A \subseteq U$. If $\#^2_A$ is elementarily 2-enumerable in $\mathcal{S}$, then A is elementarily definable in $\mathcal{S}$.*

Theorem 4.5 (Restricted cardinality theorem). *Let $\mathcal{S}$ be a well-orderable logical structure with universe U. Let every finite relation on U be elementarily definable in $\mathcal{S}$. Let $A \subseteq U$. If $\#^n_A$ is elementarily n-enumerable in $\mathcal{S}$ via a relation R that never 'enumerates' 0 and n simultaneously, then A is elementarily definable in $\mathcal{S}$.*

The proofs of these theorems are given in the technical appendix.

The premises of the first two and the last two of the above theorems differ in the following way: for the last two theorems we require that every finite relation on S is elementarily definable in $\mathcal{S}$. An example of a logical structure where this is not the case is $(\omega_1, +, \cdot)$, where ω_1 is the first uncountable ordinal number and $+$ and $\cdot$ denote ordinal number addition and multiplication. Since this structure is uncountable, there exist a singleton set $A = \{\alpha\}$ with $\alpha \in \omega_1$ that is not elementarily definable in $(\omega_1, +, \cdot)$. For such structures theorems 4.4 and 4.5 do not hold: $\#^2_A$ *is* elementarily 2-enumerable since $\#^2_A(x, y) \in \{0, 1\}$ for all $x, y \in \omega_1$, but A is not elementarily definable in $(\omega_1, +, \cdot)$.

4.2 The Positive First-Order Case

The above theorems cannot be applied to Turing enumerability since they refer to elementary definitions, not to *positive* elementary definitions. Unfortunately, the proofs of the theorems cannot simply be reformulated in a 'positive' way. They use negations to define the smallest element in a set A with respect to a well-ordering $<$: the defining formula is given by $\phi(x) = A(x) \wedge \neg\exists x' \bigl(x' < x \wedge A(x')\bigr)$.

This is a fundamental problem: the set $\{(M, x) \mid x \text{ is the smallest word accepted by } M\}$ is not recursively enumerable. Thus if we insist on finding the smallest element in every recursively enumerable set, we will not be able to apply the theorems to Turing machines. Fortunately, a closer examination of the proofs shows that we do not actually need the *smallest* element in A, but just *any* element of A as long as the same element is always chosen.

This is not as easy as it may sound—as is well-recognised in set theory, where the axiom of choice is needed for this choosing operation. Suppose you and a friend wish to agree on a certain element of A, but neither you nor your friend know the set A beforehand. Rather, you must decide on a generic method of picking an element such that, when the set A becomes known to you and your friend, you will both pick the same element. Methods like 'pick some element from A' will not guarantee that you both pick the same element, except if the set happens to be a singleton.

We need a (partial) recursive *choice function* that assigns to every Turing machine M a word that is accepted by M, provided such a word exists. Such a choice function does, indeed, exist: it maps M to the first word that is accepted by M during a dovetailed simulation of M on all words.

In the following, first-order logic is augmented by choice operators. Choice operators have been used for example by [11], but following definitions are adapted to the purposes of this paper and differ from the formalism used in [11]. On the sematic side we augment logical structures by a choice function; on the syntactic side we augment first-order logic by a choice operator ε:

Definition 4.6. A *choice function* on a set U is a function $\zeta \colon \mathcal{P}(U) \to U$ such that $\zeta(A) \in A$ for all nonempty $A \subseteq U$.

Definition 4.7. A *choice structure* is a pair $(\mathcal{S}, \zeta)$ consisting of a logical structure $\mathcal{S}$ and a choice function ζ on the universe of $\mathcal{S}$.

Definition 4.8 (Syntax of the choice operator). *First-order formulas with choice* are defined inductively the usual way with one addition: if x is a variable and ϕ is a first-order formula with choice, so is $\varepsilon(x, \phi)$.

In the next definition, $\phi^{(\mathcal{S},\zeta)}(x) = \bigl\{u \in U \mid (\mathcal{S}, \zeta) \models \phi[x = a]\bigr\}$ denotes the set of all u that make ϕ hold in $(\mathcal{S}, \zeta)$, when plugged in for the variable x.

Definition 4.9 (Semantics of the choice operator). The semantics of first-order logic with choice operator is defined in the usual way with the following addition: a formula of the form $\varepsilon(x, \phi)$ holds in a choice structure $(\mathcal{S}, \zeta)$ for an assignment α, if $\phi^{(\mathcal{S},\zeta)}(x)$ is nonempty and $\alpha(x) = \zeta\bigl(\phi^{(\mathcal{S},\zeta)}(x)\bigr)$.

As an example, consider the logical structure $\mathcal{S} = (\mathbb{N}, +, \cdot, <, 0)$ and let ζ map every nonempty set of natural numbers to its smallest element. Let $\phi(x, y, z) = \varepsilon\bigl(z, 0 < z \wedge \exists a\, (x \cdot a = z) \wedge \exists b\, (y \cdot b = z)\bigr)$. Then $\phi^{(\mathcal{S},\zeta)}(x, y, z)$ is the set of all triples (n, m, k) such that k is the least common multiple of n and m: the formula $0 < z \wedge \exists a\, (x \cdot a = z) \wedge \exists b\, (y \cdot b = z)$ is true for all positive z that are multiples of both x and y; thus the choice operator picks the smallest one of these.

The following theorem shows that the class of recursively enumerable sets can be characterised in terms of first-order logic with choice.

Theorem 4.10. *For every alphabet Σ there exists a choice structure $(\mathcal{S}_{\mathrm{RE}|\Sigma^*}, \zeta)$ such that a language $A \subseteq \Sigma^*$ is recursively enumerable iff it is positively elementarily definable with choice in $(\mathcal{S}_{\mathrm{RE}|\Sigma^*}, \zeta)$.*

We can now formulate the cross product theorem and the nonspeedup theorem in such a way that they can be applied both to finite automata and to Turing machines.

Theorem 4.11 (Cross product theorem, positive version). *Let $(\mathcal{S}, \zeta)$ be a choice structure. Let the inequality relation be positively elementarily definable in $(\mathcal{S}, \zeta)$. Let every finite relation that is elementarily definable with choice in $(\mathcal{S}, \zeta)$ be positively elementarily definable with choice in $(\mathcal{S}, \zeta)$. Let $f, g\colon U \to U$ be functions. If $f \times g$ is positively $(n+m)$-enumerable with choice in $(\mathcal{S}, \zeta)$, then f is positively n-enumerable with choice in $(\mathcal{S}, \zeta)$ or g is positively m-enumerable with choice in $(\mathcal{S}, \zeta)$.*

Theorem 4.12 (Nonspeedup theorem, positive version). *Let $(\mathcal{S}, \zeta)$ be a choice structure. Let U be its universe. Let the inequality relation be positively elementarily definable in $(\mathcal{S}, \zeta)$. Let every finite relation that is elementarily definable with choice in $(\mathcal{S}, \zeta)$ be positively elementarily definable with choice in $(\mathcal{S}, \zeta)$. Let $A \subseteq U$. If χ_A^n is positively n-enumerable with choice in $(\mathcal{S}, \zeta)$, then A is positively elementarily definable with choice in $(\mathcal{S}, \zeta)$.*

The cross product theorem, theorem 4.11, is a consequence of its positive version, theorem 4.2. (And not the other way round, as one might perhaps expect.) The same is true for the nonspeedup theorem. To see this, consider a well-orderable structure $\mathcal{S}$ whose existence is postulated in theorem 4.2. Define a choice structure $(\mathcal{S}', \zeta)$ as follows: $\mathcal{S}'$ has the same universe as $\mathcal{S}$ and contains *all relations that are elementarily definable in $\mathcal{S}$*. The function ζ maps each set A to its smallest element with respect the well-ordering of $\mathcal{S}$'s universe. With these definitions, a relation is positively elementarily definable with choice in $(\mathcal{S}', \zeta)$ iff it is elementarily definable in $\mathcal{S}$.

4.3 The Higher-Order Case

We just saw that the cross product theorem for a certain logic, namely first-order logic, is a consequence of the cross product theorem for a less powerful logic, namely positive first-order logic. We may ask whether we can similarly apply the theorems for first-order logic to higher-order logics.

This is indeed possible and we can use the same kind of argument as above: Consider any logical structure $\mathcal{S}$. Define a new structure $\mathcal{S}'$ as follows: it has the same universe as $\mathcal{S}$ and it contains every relation that is higher-order definable in $\mathcal{S}$. Then a relation is elementarily definable in $\mathcal{S}'$ iff it is higher-order definable in $\mathcal{S}$. This allows us to transfer the cross product theorem and all of the weak cardinality theorems *to all logics that are at least as powerful as first-order logic.* Just one example of such a transfer is the following:

Theorem 4.13 (Cross product theorem for higher-order logic).
Let $\mathcal{S}$ be a well-orderable logical structure with universe U. Let $f, g\colon U \to U$ be functions. If $f \times g$ is higher-order $(n+m)$-enumerable in $\mathcal{S}$, then f is higher-order n-enumerable in $\mathcal{S}$ or g is higher-order m-enumerable in $\mathcal{S}$.

5 Separability Theorems for First-Order Logic

Kummer's cardinality theorem can be reformulated in terms of separability. In [27] it is shown that it is equivalent to the following statement, where $A^{\binom{n}{k}}$ denotes the set of all n-tuples of distinct words such that exactly k of them are in A.

Theorem 5.1 (Separability version of Kummer's cardinality theorem).
Let A be a language. Suppose there exist recursively enumerable supersets of $A^{\binom{n}{0}}$, $A^{\binom{n}{1}}$, ..., $A^{\binom{n}{n}}$ whose intersection is empty. Then A is recursive.

In [27] it is also shown that the above statement is still true if we replace 'recursive enumerable' by 'co-recursively enumerable'.

The weak cardinality theorems for first-order logic can be reformulated in a similar way. Let us start with the cardinality theorem for two words. It can be stated equivalently as follows, where $\bar{A} = U \setminus A$ denotes the complement of A.

Theorem 5.2. *Let $\mathcal{S}$ be a well-orderable logical structure with universe U. Let every finite relation on U be elementarily definable in $\mathcal{S}$. Let $A \subseteq U$. Suppose there exist elementarily definable supersets of $A \times A$, $A \times \bar{A}$, and $\bar{A} \times \bar{A}$ whose intersection is empty. Then A is elementarily definable in $\mathcal{S}$.*

The restricted cardinality theorem can be reformulated in terms of elementary separability. Let us call two sets A and B *elementarily separable* in a structure $\mathcal{S}$ if there exists a set C with $A \subseteq C \subseteq \bar{B}$ that is elementarily definable in $\mathcal{S}$.

Theorem 5.3. *Let $\mathcal{S}$ be a well-orderable structure with universe U. Let every finite relation on U be elementarily definable in $\mathcal{S}$. Let $A \subseteq U$. If $A^{\binom{n}{0}}$ and $A^{\binom{n}{n}}$ are elementarily separable in $\mathcal{S}$, then A is elementarily definable in $\mathcal{S}$.*

6 Conclusion

This paper proposed a new, logic-based approach to the proof of (weak) cardinality theorems. The approach has two advantages:

1. It unifies previous results in a single framework.
2. The results can easily be applied to other computational models.

Regarding the first advantage, only the cross product theorem and the nonspeedup theorem are completely 'unified' by the theorems presented in this paper: the Turing machine versions and the finite automata versions of these theorems are just different instantiations of theorems 4.2 and 4.3.

For the cardinality theorem for two words and for the restricted cardinality theorem the situation is (currently) more complex. These theorem hold for Turing machines and for finite automata, but different proofs are used. In particular, the logical theorems cannot be instantiated for Turing enumerability. Nevertheless, the logical approach is fruitful here: the logical theorem *can* be instantiated for new models like Presburger arithmetics.

Organised by computational model, the results of this paper can be summarised as follows: the cross product theorem and the nonspeedup theorem

- hold for Presburger arithmetic,
- hold for finite automata,
- do not hold for polynomial-time machines,
- hold for Turing machines,
- hold for natural number arithmetic,
- hold for ordinal number arithmetic.

The cardinality theorem for two inputs and the restricted cardinality theorem

- hold for Presburger arithmetic,
- hold for finite automata,

- do not hold for polynomial-time machines,
- hold for Turing machines,
- hold for natural number arithmetic,
- do not hold for ordinal number arithmetic.

The behaviour of ordinal number arithmetic is interesting: the cardinality theorem for two inputs and the restricted cardinality theorem fail since there exist ordinal numbers that are not elementarily definable, but this is not a 'problem' for the cross product theorem and the nonspeedup theorem.

The results of this paper raise the question of whether the cardinality theorem holds for first-order logic. I conjecture that this is the case, that is, I conjecture that for well-orderable structures $\mathcal{S}$ in which all finite relations can be elementarily defined, if $\#_A^n$ is elementarily n-enumerable then A is elementarily definable. Proving this conjecture would also settle the open problem of whether the cardinality theorem holds for finite automata.

References

[1] H. Austinat, V. Diekert, and U. Hertrampf. A structural property of regular frequency classes. *Theoretical Comput. Sci.*, 2003. To appear.

[2] H. Austinat, V. Diekert, U. Hertrampf, and H. Petersen. Regular frequency computations. In *Proc. RIMS Symposium on Algebraic Systems, Formal Languages and Computation*, volume 1166 of *RIMS Kokyuroku*, pages 35–42. Research Inst. for Mathematical Sci., Kyoto University, Japan, 2000.

[3] R. Beigel. *Query-Limited Reducibilities*. PhD thesis, Stanford University, Stanford, USA, 1987.

[4] R. Beigel, W. Gasarch, M. Kummer, G. Martin, T. McNicholl, and F. Stephan. The complexity of ODD_n^A. *J. Symbolic Logic*, 65(1):1–18, 2000.

[5] J. R. Büchi. On a decision method in restricted second-order arithmetic. In E. Nagel, P. Suppes, and A. Tarski, editors, *Proceedings of the 1960 International Congress on Logic, Methodology and Philosophy of Science*, pages 1–11. Stanford University Press, 1962.

[6] J. Cai and L. A. Hemachandra. Enumerative counting is hard. *Information and Computation*, 82(1):34–44, July 1989.

[7] W. Gasarch. Bounded queries in recursion theory: A survey. In *Proceedings of the Sixth Annual Structure in Complexity Theory Conference*, pages 62–78, Chicago, Illinois, 30 June–3 July 1991. IEEE Computer Society Press.

[8] V. Harizanov, M. Kummer, and J. Owings. Frequency computations and the cardinality theorem. *J. Symbolic Logic*, 52(2):682–687, 1992.

[9] L. A. Hemachandra. The strong exponential hierarchy collapses. *J. Comput. Syst. Sci.*, 39(3):299–322, Dec. 1989.

[10] E. Hemaspaandra, L. A. Hemaspaandra, and H. Hempel. A downward collapse within the polynomial hierarchy. *SIAM J. Comput.*, 28(2):383–393, 1998.

[11] D. Hilbert and P. Bernay. *Grundlagen der Mathematik II*, volume 50 of *Die Grundlehren der mathematischen Wissenschaft in Einzeldarstellungen.* Springer-Verlag, second edition, 1970.

[12] A. Hoene and A. Nickelsen. Counting, selecting, and sorting by query-bounded machines. In *Proc. 10th Symposium on Theoretical Aspects of Comp. Sci.*, volume 665 of *LNCS*, pages 196–205. Springer-Verlag, 1993.

[13] N. Immerman. Nondeterministic space is closed under complementation. *SIAM J. Comput.*, 17(5):935–938, Oct. 1988.

[14] C. G. Jockusch, Jr. *Reducibilities in Recursive Function Theory.* PhD thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1966.

[15] J. Kadin. $\mathrm{P}^{\mathrm{NP}[O(\log n)]}$ and sparse Turing-complete sets for NP. *J. Comput. Syst. Sci.*, 39(3):282–298, Dec. 1989.

[16] E. B. Kinber. Frequency computations in finite automata. *Cybernetics*, 2:179–187, 1976.

[17] M. Kummer. A proof of Beigel's cardinality conjecture. *J. Symbolic Logic*, 57(2):677–681, June 1992.

[18] M. Kummer and F. Stephan. Effecitive search problems. *Mathematical Logic Quarterly*, 40:224–236, 1994.

[19] S. R. Mahaney. Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis. *J. Comput. Syst. Sci.*, 25(2):130–143, Oct. 1982.

[20] R. McNaughton. Review of [5]. *J. Symbolic Logic*, 28(1):100–102, 1963.

[21] A. Nickelsen. On polynomially $\mathcal{D}$-verbose sets. In *Proc. 14th Symposium on Theoretical Aspects of Comp. Sci.*, volume 1200 of *LNCS*, pages 307–318. Springer-Verlag, 1997.

[22] J. C. Owings, Jr. A cardinality version of Beigel's nonspeedup theorem. *J. Symbolic Logic*, 54(3):761–767, Sept. 1989.

[23] E. L. Post. Recursively enumerable sets of positive integers and their decision problems. *Bulletin of the American Mathematical Society*, 50:284–316, 1944.

[24] R. Szelepcsényi. The method of forced enumeration for nondeterministic automata. *Acta Informatica*, 23:279–284, 1988.

[25] T. Tantau. Comparing verboseness for finite automata and Turing machines. In *Proc. 19th Symposium on Theoretical Aspects of Comp. Sci.*, volume 2285 of *LNCS*, pages 465–476. Springer-Verlag, 2002.

[26] T. Tantau. Towards a cardinality theorem for finite automata. In *Proc. 27th International Symposium on Mathematical Foundations of Comp. Sci.*, volume 2420 of *LNCS*, pages 625–636. Springer-Verlag, 2002.

[27] T. Tantau. *On Structural Similarities of Finite Automata and Turing Machine Enumerability Classes.* PhD thesis, Technische Universität Berlin, 2003.

Technical Appendix

Proof of theorem 4.2. Let $f \times g$ be elementarily $(n+m)$-enumerable in $\mathcal{S}$ via a relation R. In the following, two relations F and G are constructed such that either f is elementarily n-enumerable via F or g is elementarily m-enumerable via G.

The construction of the relations F and G is based on an abstract form of *easy-hard arguments.* Easy-hard arguments have been used in complexity theory in different proofs, see for example [15] or [10]. In such an argument one shows that either all words in Σ^* are *easy* (in a sense to be defined), in which case a language is, well, easy; or there exists a *hard* word, which allows us to decide all *other* words, provided we know the characteristic value of the hard word.

Translated to the more abstract setting of this proof, 'easy' is a property of the elements of U. If all $u \in U$ are easy, then f will be elementarily n-enumerable via F. Otherwise, in case a hard element u_{hard} exists, g will be elementarily m-enumerable via G.

Before we proceed, let us fix some notations. Let $<$ be a well-ordering of U that is elementarily definable in $\mathcal{S}$. Such a well-ordering exists by assumption. Let $R[u,v]$ denote the set $\bigl\{(x,y) \in U^2 \mid (u,v,x,y) \in R\bigr\}$. It is the set of all pairs that are 'enumerated' by R for the pair (u,v). Let us also use the notation '$(x,y) \in R[u,v]$' in formulas, where it just means '$R(u,v,x,y)$'.

Definition of easy elements and advisors
Let us call an element $u \in U$ *easy* if there exists a $v \in U$ such that in $R[u,v]$ at least $m+1$ pairs have the same first component x. Such a v will be called an *advisor for u.* The 'advisor relation' $A := \bigl\{(u,v) \mid v \text{ is an advisor for } u\bigr\}$ can be defined elementarily as follows:

$$(u,v) \in A \;:\Longleftrightarrow\; \exists x \exists y_1 \cdots \exists y_{m+1} \bigl(\text{distinct}(y_1,\dots,y_{m+1}) \wedge \textstyle\bigwedge_{i=1}^{m+1} (x,y_i) \in R[u,v]\bigr).$$

The formula $\text{distinct}(y_1,\dots,y_{m+1})$ is an abbreviation for $\bigwedge_{1 \le i < j \le m+1} \neg\, y_i = y_j$. The set of easy elements is elementarily definable as the formula $\phi_{\text{easy}}(u) := \exists v\, A(u,v)$ shows.

Case 1: A hard element exists
Suppose there exists a hard element. Let $u_{\text{hard}} \in U$ be the smallest such element with respect to $<$. This element is elementarily definable in $\mathcal{S}$ via the formula $\phi_{u_{\text{hard}}}(x) = \phi_{\text{hard}}(x) \wedge \neg\exists x' \bigl(x' < x \wedge \phi_{\text{hard}}(x')\bigr)$.

The element $f(u_{\text{hard}})$ can also be defined elementarily in $\mathcal{S}$: Let us fix some elementarily definable element v_* of U. Consider the set $R[u_{\text{hard}}, v_*]$. It has size at most $n+m$ and we can thus elementarily define the first element of this set, the second element, and so on. Since one of these elements is $\bigl(f(u_{\text{hard}}), g(v_*)\bigr)$, say the i-th one, we can construct a formula that singles out the 'first component of the i-th element of $R[u_{\text{hard}}, v_*]$'.

Let $y \in G[v] :\Longleftrightarrow \bigl(f(u_{\text{hard}}), y\bigr) \in R[u_{\text{hard}}, v]$. The graph of g is a subset of G since for all $v \in U$ we have $\bigl(f(u_{\text{hard}}), g(v)\bigr) \in R[u_{\text{hard}}, v]$. Since u_{hard} is hard, for all v the set $\bigl\{y \in U \mid \bigl(f(u_{\text{hard}}), y\bigr) \in R[u_{\text{hard}}, v]\bigr\}$ has size at most m. Thus G is m-bounded and g is elementarily m-enumerable via G.

Case 2: All elements are easy
Suppose that all $u \in U$ are easy. Let A' be defined as follows: $(x,y) \in A' :\Longleftrightarrow A(x,y) \wedge \neg\exists y' \bigl(y' < y \wedge A(x,y')\bigr)$. Since all elements u are easy, they all have advisors. Thus A' is the graph of a (total) function that maps every element u to an advisor for u, namely to the smallest one. Let

$$x \in F[u] \;:\Longleftrightarrow\; \exists v \bigl(A'(u,v) \wedge \exists y\, (x,y) \in R[u,v]\bigr).$$

The first part of the formula fixes v to be the smallest advisor for u. In the set $R[u,v]$ at least $m+1$ pairs have the same first component (recall that this was the defining property of advisors). Thus there are at most $n+m-m=n$ different x with $(x,y)\in R[u,v]$. Since the graph of f is a subset of F, the function f is elementarily n-enumerable. $\square$

Proof of theorem 4.3. We argue by induction on n. For $n=1$ the claim is correct. Suppose χ_A^{n+1} is elementarily $(n+1)$-enumerable in $\mathcal{S}$. Applying the cross product theorem to $\chi_A^{n+1}=\chi_A^n\times\chi_A$ yields that χ_A^n is elementarily n-enumerable in $\mathcal{S}$ or that χ_A is elementarily definable in $\mathcal{S}$. In the first case we are done by the induction hypothesis, in the second case we directly have the claim. $\square$

Proof of theorem 4.4. Suppose that $\#_A^2$ is elementarily 2-enumerable via a relation R. Our first aim is to switch from the cardinality function $\#_A^2$ to the characteristic function χ_A^2. Ideally, if we could show that χ_A^2 is elementarily 2-enumerable, then theorem 4.2 would yield the claim. Unfortunately, if R enumerates both the numbers 0 and 1 on input (x,y), we only know $\chi_A^2(x,y)\in\{00,01,10\}$; and if R enumerates both the numbers 1 and 2, we only know $\chi_A^2(x,y)\in\{01,10,11\}$. Thus, as first step, we only show that χ_A^2 is elementarily 3-enumerable.

Let C_2 be the ternary relation that is defined as follows:

$$\begin{aligned} b\in C_2[x,y] :\iff\ & \bigl(b=00 && \to 0\in R[x,y]\vee x=y\bigr)\\ \wedge\ & \bigl(b=01\vee b=10 && \to 1\in R[x,y]\wedge\neg\, x=y\bigr)\\ \wedge\ & \bigl(b=11 && \to 2\in R[x,y]\vee x=y\bigr).\end{aligned}$$

Recall from the previous proof that $C_2[x,y]=\{b\mid(x,y,b)\in C_2\}$. The graph of χ_A^2 is contained in C_2 (hence the name) and $C_2[x,y]$ is always a subset of one of the following sets: $\{00,01,10\}$, $\{00,11\}$, and $\{01,10,11\}$.

Unlike 0, 1, and 2, the constants 00, 01, 10, and 11 are not necessarily in the universe U. Thus we might be unable to 'refer' to these constants in the formula that defines the relation C_2. However, these constants are only used 'internally' and we can pick any four distinct elements of U and interpret them as 00, 01, 10, and 11 respectively. (If U has less than four elements the claim is trivial.)

The second aim is to enumerate sets of minimal size for χ_A^3, that is, for any *three* input elements. This is achieved by the relation C_3 that is defined as follows:

$$b\in C_3[x,y,z] :\iff \bigvee_{b_1b_2b_3\in\{0,1\}^3}\bigl(b=b_1b_2b_3\wedge b_1b_2\in C_2[x,y]\wedge b_1b_3\in C_2[x,z]\wedge b_2b_3\in C_2[y,z]\bigr).$$

The formula expresses that the bitstring $b\in\{0,1\}^3$ is consistent with the sets enumerated by C_2 on every selection of two elements. In particular, $\chi_A^3(x,y,z)\in C_3[x,y,z]$. Once more, we pick any eight distinct elements of U to represent bitstrings of length three.

The next step is to employ an easy-hard argument similar to the argument used in the proof of theorem 4.2. This time, let us call a *pair* (x,y) of elements *easy* if there exists an element z such that $\bigl\{b_1b_2\mid b_1b_2b_3\in C_3[x,y,z]\bigr\}$ has size at most 2. The element z will be called an *advisor* for (x,y). The advisor relation, denoted B in this proof in order to avoid a name clash with the set A, is the following ternary relation:

$$\begin{aligned}(x,y,z)\in B :\iff \neg\bigvee_{\substack{b,c,d\,\in\{0,1\}^2,\\ b,c,d \text{ distinct}}} & \bigl(b0\in C_3[x,y,z]\vee b1\in C_3[x,y,z]\bigr)\\ \wedge\ & \bigl(c0\in C_3[x,y,z]\vee c1\in C_3[x,y,z]\bigr)\\ \wedge\ & \bigl(d0\in C_3[x,y,z]\vee d1\in C_3[x,y,z]\bigr).\end{aligned}$$

The formula $\phi_{\text{easy}}(x,y) := \exists z\, B(x,y,z)$ is true exactly for easy pairs (x,y).

Case 1: Existence of a hard pair that is partly in and out

Suppose there exists a hard pair $(x_{\text{hard}}, y_{\text{hard}})$ with $\chi_A(x_{\text{hard}}) \neq \chi_A(y_{\text{hard}})$, that is, $\chi_A^2(x_{\text{hard}}, y_{\text{hard}}) = 01$ or $\chi_A^2(x_{\text{hard}}, y_{\text{hard}}) = 10$. We only need to consider the case $\chi_A^2(x_{\text{hard}}, y_{\text{hard}}) = 01$ since the other case is symmetric. We can freely use x_{hard} and y_{hard} is formulas in the following, since all finite sets are elementarily definable by assumption.

I claim that $z \in A$ holds iff $011 \in C_3[x_{\text{hard}}, y_{\text{hard}}, z]$. To prove this, we show that there exists at most one bitstring in $P := C_3[x_{\text{hard}}, y_{\text{hard}}, z]$ that starts with 01. Suppose we had both $010 \in P$ and $011 \in P$. Then $000 \notin P$, since otherwise $\{b_2b_3 \mid b_1b_2b_3 \in P\} \supseteq \{10, 11, 00\}$, contradicting the assumption that one possibility has been excluded for $\#_A^2(y_{\text{hard}}, z)$. Likewise, $101 \notin P$ and also $111 \notin P$, since otherwise $\{b_1b_3 \mid b_1b_2b_3 \in P\} \supseteq \{00, 01, 11\}$.

Since $(x_{\text{hard}}, y_{\text{hard}})$ is a hard pair, we have either $\{b_1b_2 \mid b_1b_2b_3 \in P\} = \{00, 01, 10\}$ or $\{b_1b_2 \mid b_1b_2b_3 \in P\} = \{01, 10, 11\}$. In the first case, since $000 \notin P$ and $00 \in \{b_1b_2 \mid b_1b_2b_3 \in P\}$, we must have $001 \in P$. Likewise, since $101 \notin P$ and $10 \in \{b_1b_2 \mid b_1b_2b_3 \in P\}$, we must have $100 \in P$. But then $P \supseteq \{010, 011, 001, 100\}$ and thus $\{b_2b_3 \mid b_1b_2b_3 \in P\} \supseteq \{10, 11, 01, 00\}$, a contradiction. Similarly, in the second case we must have $100 \in P$ and $110 \in P$ and thus $P \supseteq \{010, 011, 100, 110\}$, which yields $\{b_2b_3 \mid b_1b_2b_3 \in P\} \supseteq \{10, 11, 00\}$, also a contradiction. This shows that P contains only one bitstring starting with 01.

Case 2: All hard pairs are either in or out

For this case, assume that $\chi_A(x_{\text{hard}}) = \chi_A(y_{\text{hard}})$ holds for every hard pair $(x_{\text{hard}}, y_{\text{hard}})$. The aim is to show that χ_A^2 is elementarily 2-enumerable, which implies the claim by theorem 4.2. The rough idea is as follows. On input of two elements x and y, we first check whether the pair (x,y) is hard, using the formula $\neg\phi_{\text{easy}}$. If so, by assumption we know that $\chi_A(x) = \chi_A(y)$ and we can output the set $\{00, 11\}$. Otherwise, the pair is easy. In this case we know that there exists an element z, namely an advisor, such that $\bigl\{b_1b_2 \mid b_1b_2b_3 \in C_3[x,y,z]\bigr\}$ has size at most 2. Once we have fixed such an advisor, we can output the set.

In detail, the construction is as follows. Let B' be defined by $(x,y,z) \in B' :\iff B(x,y,z) \wedge \neg\exists z' \bigl(z' < z \wedge B(x,y,z')\bigr)$, where $<$ is a well-ordering of U that is elementarily definable in $\mathcal{S}$. The relation B' is the graph of a partial function that maps every easy pair (x,y) to an advisor for it and that is undefined for all hard pairs. Consider the relation T that is defined as follows:

$$\begin{aligned} b \in T[x,y] :\iff \quad & \bigl(\neg\phi_{\text{easy}}(x,y) \to \bigl(b = 00 \vee b = 11\bigr)\bigr) \\ & \wedge \Bigl(\phi_{\text{easy}}(x,y) \to \exists z\bigl(B'(x,y,z) \wedge (b0 \in C_3[x,y,z] \vee b1 \in C_3[x,y,z])\bigr)\Bigr). \end{aligned}$$

The first line ensures that T enumerates $\{00, 11\}$ if (x,y) is a hard pair. If it is easy, the second line first fixes z such that it is an advisor and then 'outputs' all bitstrings in the set $C_3[x,y,z]$ with the last bit removed. Since (x,y) is easy, this set will have size at most 2. Thus χ_A^2 is elementarily 2-enumerable via T. □

Proof of theorem 4.5. We prove the claim by induction on n. For $n = 1$ the claim is true. So suppose the claim has already been shown for $n - 1$.

Let $\#_A^n$ be elementarily n-enumerable via a relation R such that $R[x_1, \dots, x_n]$ never contains both 0 and n for any $x_i \in U$. As in the previous proofs, we define easy elements, based on a notion of advisors. Let us call a tuple $(y_1, \dots, y_n) \in U^n$ an *advisor* for a tuple $(x_1, \dots, x_{n-1}) \in U^{n-1}$ if it satisfies the following relation:

$$\begin{aligned} (x_1, \dots, x_{n-1}, y_1, \dots, y_n) \in B :\iff \quad & \text{distinct}(x_1, \dots, x_{n-1}, y_1, \dots, y_n) \\ & \wedge 0 \in R[y_1, \dots, y_n] \wedge \textstyle\bigwedge_{i=1}^n n \in R[x_1, \dots, x_{n-1}, y_i]. \end{aligned}$$

Note that an advisor tuple can only, but need not, exist if at least one x_i is in A. Let us call a tuple $(x_1, \dots, x_{n-1})$ of pairwise different elements *easy* if

1. at least one x_i is not in A or
2. there exists an advisor for it.

A tuple $(x_1, \dots, x_{n-1})$ of pairwise different elements is *hard* if it is not easy.

Case 1: Existence of a hard tuple
Suppose there exists a hard tuple $(x_1^{\text{hard}}, \dots, x_{n-1}^{\text{hard}})$. Since all finite sets are elementarily definable, we can freely use x_i^{hard} in formulas in the following. Let

$$y \in \hat{A} :\iff n \in R\big[x_1^{\text{hard}}, \dots, x_{n-1}^{\text{hard}}, y\big] \vee \textstyle\bigvee_{i=1}^{n-1} y = x_i^{\text{hard}}.$$

I claim $\hat{A} =_{\text{ae}} A$. This means that A and $\hat{A}$ are equal almost everywhere, that is, that their symmetric difference is finite. This will prove that A is elementarily definable.

Since condition 1 does not hold for hard tuples, all x_i^{hard} are in A. For $y \in A \setminus \{x_1^{\text{hard}}, \dots, x_{n-1}^{\text{hard}}\}$ we thus have $\#_A^n(x_1, \dots, x_{n-1}, y) = n$, which implies $n \in R[x_1^{\text{hard}}, \dots, x_{n-1}^{\text{hard}}, y]$. Thus for all $y \in A$ we have $y \in \hat{A}$.

For $y \notin A$, we can have $n \in R[x_1^{\text{hard}}, \dots, x_{n-1}^{\text{hard}}, y]$ for at most $n-1$ different y's, since otherwise such y's would form an advisor for $(x_1^{\text{hard}}, \dots, x_{n-1}^{\text{hard}})$, contradicting the assumption that condition 2 does not hold. Thus $y \notin \hat{A}$ whenever $y \notin A$, except for these finitely many exceptions.

Case 2: All tuples are easy
Suppose all tuples of pairwise different elements are easy. We argue that $\#_A^{n-1}$ is elementarily $(n-1)$-enumerable via a relation T for which $T[x_1, \dots, x_{n-1}]$ never contains both 0 and $n-1$ for any x_i. This yields the claim by the induction hypothesis. For the definition of T, first consider the following relation $\tilde{T}$, which 'works' only for distinct x_i:

$$\begin{aligned} k \in \tilde{T}[x_1, \dots, x_{n-1}] :\iff \quad & \big[\big(\ \exists y_1 \cdots \exists y_n\, B(x_1, \dots, x_{n-1}, y_1, \dots, y_n)\big) \to k > 0\big] \\ \wedge\ & \big[\big(\neg\exists y_1 \cdots \exists y_n\, B(x_1, \dots, x_{n-1}, y_1, \dots, y_n)\big) \to k < n-1\big]. \end{aligned}$$

For distinct x_i, if there exists an advisor tuple for $(x_1, \dots, x_{n-1})$, the very existence of the advisor tuple ensures that for at least one x_i we have $x_i \in A$. Thus $\#_A^{n-1}(x_1, \dots, x_{n-1}) > 0$. If there does not exist an advisor tuple, which can only happen if condition 1 holds, at least one x_i is not in A. Thus $\#_A^{n-1}(x_1, \dots, x_{n-1}) < n-1$.

The desired relation T that works for all x_i, not just for distinct x_i, can be obtained from $\tilde{T}$ as follows:

$$\begin{aligned} k \in T[x_1, \dots, x_{n-1}] :\iff \quad & \big(\ \text{distinct}(x_1, \dots, x_{n-1}) \to k \in \tilde{T}[x_1, \dots, x_{n-1}]\big) \\ \wedge\ & \big(\neg\, \text{distinct}(x_1, \dots, x_{n-1}) \to k < n-1\big). \end{aligned}$$

□

Proof of theorem 4.10. The logical structure $\mathcal{S}_{\text{RE}|\Sigma^*}$ has the universe Σ^*. It contains each recursively enumerable relation on Σ^* as an operation. In particular, its signature is countably infinite. The choice function ζ maps a subset $A \subseteq \Sigma^*$ to a word Σ^* according to the following rules: If A is not recursively enumerable or empty, it maps A to the empty word. If A is recursively enumerable by some machine M, it maps A to the first word that is accepted during a dovetailed simulation of M on all words.

Trivially, every recursively enumerable relation is positively elementarily definable with choice in $(\mathcal{S}_{\mathrm{RE}|\Sigma^*}, \zeta)$. The hard part is proving that only recursively enumerable relations can be defined thus. We prove this using structural induction on positive first-order formulas with choice.

If ϕ and ψ define recursively enumerable sets, so do $\phi \wedge \psi$ and $\phi \vee \psi$. The set defined by $\exists x\, \phi$ is also recursively enumerable since we can 'search' for an x that makes ϕ true using dovetailing. The set defined by $\varepsilon(x, \phi)$ is also recursive enumerable: Let M be the machine that accepts the set defined by ϕ. We run a dovetailed simulation of M on all inputs. If this simulation halts and the first word accepted is x, then we accept. □

Proof of theorem 4.11. Since the proof is similar to the proof of the normal version of the cross product theorem, the following presentation is condensed. Let $f \times g$ be positively elementarily $(n+m)$-enumerable with choice in $(\mathcal{S}, \zeta)$ via a relation R. We construct two relations F and G such that either f is positively elementarily n-enumerable with choice via F or g is positively elementarily m-enumerable with choice via G.

Definition of easy elements and advisors

As in the proof of theorem 4.2, let us call an element $u \in U$ *easy* if it has an advisor, which is a $v \in U$ such that in $R[u,v]$ at least $m+1$ pairs have the same first component x. The advisor relation $A := \bigl\{(u,v) \mid v \text{ is an advisor for } u\bigr\}$ can be positively elementarily defined in $(\mathcal{S}, \zeta)$ as follows:

$$(u,v) \in A \;:\Longleftrightarrow\; \exists x \exists y_1 \cdots \exists y_{m+1} \bigl(\mathrm{distinct}(y_1, \dots, y_{m+1}) \wedge \textstyle\bigwedge_{i=1}^{m+1} (x, y_i) \in R[u,v]\bigr).$$

Let $\phi_{\mathrm{easy}}(u) := \exists v\, A(u,v)$.

Case 1: A hard element exists

Suppose there exists a hard element. We can elementarily define such an element using the choice operator: the formula $\varepsilon\bigl(x, \neg\phi_{\mathrm{easy}}(u)\bigr)$ will be true exactly for one element $x = u_{\mathrm{hard}}$. The element $f(u_{\mathrm{hard}})$ can also be elementarily defined with choice. For a fixed elementarily definable element v_* of U consider the set $R[u_{\mathrm{hard}}, v_*]$. It has size at most $n+m$ and one of its elements is $\bigl(f(u_{\mathrm{hard}}), g(v_*)\bigr)$. By repeatedly applying the choice operator to the set, we can define any particular pair elementarily with choice. Thus we can construct a formula that singles out the 'first component of the element of $R[u_{\mathrm{hard}}, v_*]$ obtained after i elements have been picked from it'. Since both u_{hard} and $f(u_{\mathrm{hard}})$ can be defined elementarily with choice, by assumption they can also be defined *positively* elementarily with choice.

Let $y \in G[v] :\Longleftrightarrow \bigl(f(u_{\mathrm{hard}}), y\bigr) \in R[u_{\mathrm{hard}}, v]$. The graph of g is a subset of G since for all $v \in U$ we have $\bigl(f(u_{\mathrm{hard}}), g(v)\bigr) \in R[u_{\mathrm{hard}}, v]$. Since u_{hard} is hard, for all v the set $\bigl\{y \in U \mid \bigl(f(u_{\mathrm{hard}}), y\bigr) \in R[u_{\mathrm{hard}}, v]\bigr\}$ has size at most m. Thus G is m-bounded and g is elementarily m-enumerable via G.

Case 2: All elements are easy

Suppose that all $u \in U$ are easy. Then they all have advisors. Let

$$x \in F[u] \;:\Longleftrightarrow\; \exists v \Bigl(\varepsilon\bigl(v, A(u,v)\bigr) \wedge \exists y\, (x,y) \in R[u,v]\Bigr).$$

The first part of the formula fixes v to be a fixed advisor for u. In the set $R[u,v]$ at least $m+1$ pairs have the same first component. Thus there are at most $n+m-m = n$ different x with $(x,y) \in R[u,v]$. Since the graph of f is a subset of F, the function f is positively elementarily n-enumerable with choice. □

Proof of theorem 4.12. The proof is identical to the proof of theorem 4.3, with the reference to the cross product theorem being replaced by a reference to its positive version. □

Proof of theorem 5.2. Let $B_2 \supseteq A \times A$, $B_1 \supseteq A \times \bar{A}$, and $B_0 \supseteq \bar{A} \times \bar{A}$ be elementarily definable in $\mathcal{S}$. Let $B_2 \cap B_1 \cap B_0 = \emptyset$. Then the function $\#_A^2$ can be elementarily 2-enumerated via a relation R that is defined as follows: For a pair (x, y) with $x \neq y$ let $(x, y, 2) \in R$ if $(x, y) \in B_2$ and $(y, x) \in B_2$; let $(x, y, 1) \in R$ if $(x, y) \in B_1$ or $(y, x) \in B_1$; and let $(x, y, 0) \in R$ if $(x, y) \in B_0$ and $(y, x) \in B_0$. For a pair (x, x) let $(x, x, 0) \in R$ and $(x, x, 1) \in R$. The relation R is 2-bounded and contains the graph of $\#_A^2$. Thus A is elementarily definable in $\mathcal{S}$ by theorem 4.4. □

Proof of theorem 5.3. Let C separate $A^{\binom{n}{0}}$ and $A^{\binom{n}{n}}$. Then the function $\#_A^n$ can be elementarily n-enumerated via a relation R that is defined as follows: For a tuple $(x_1, \dots, x_n)$ of pairwise distinct elements let $(x_1, \dots, x_n, i) \in R$ for all $i \in \{1, \dots, n-1\}$; let $(x_1, \dots, x_n, 0) \in R$ if $(x_1, \dots, x_n) \in C$; and let $(x_1, \dots, x_n, n) \in R$ if $(x_1, \dots, x_n) \notin C$. For tuples of non-distinct elements let $(x_1, \dots, x_n, i) \in R$ for all $i \in \{0, \dots, n-1\}$. The relation R is n-bounded, it contains the graph of $\#_A^n$, and it never 'enumerates' both 0 and n. Thus A is elementarily definable in $\mathcal{S}$ by theorem 4.5. □