SIAM J. COMPUT.
Vol. 37, No. 2, pp. 502–521

DEFINABILITY OF LANGUAGES BY GENERALIZED FIRST-ORDER FORMULAS OVER $(\mathbb{N}, +)$*

AMITABHA ROY† AND HOWARD STRAUBING†

Abstract. We consider an extension of first-order logic by modular quantifiers of a fixed modulus q. Drawing on collapse results from finite model theory and techniques of finite semigroup theory, we show that if the only available numerical predicate is addition, then sentences in this logic cannot define the set of bit strings in which the number of 1's is divisible by a prime p that does not divide q. More generally, we completely characterize the regular languages definable in this logic. The corresponding statement, with addition replaced by arbitrary numerical predicates, is equivalent to the conjectured separation of the circuit complexity class ACC from NC^1. Thus our theorem can be viewed as proving a highly uniform version of the conjecture.

Key words. finite model theory, circuit complexity, semigroup theory

AMS subject classifications. 68Q70, 68Q19, 03C98, 68Q17, 20M35

DOI. 10.1137/060658035

1. Background.

The circuit complexity class $ACC(q)$ is the family of languages recognized by constant-depth polynomial-size families of circuits containing unbounded fan-in AND, OR, and MOD_q gates for some fixed modulus $q > 0$. It is known that if q is a prime power and p is a prime that does not divide q, then $ACC(q)$ does not contain the language L_p consisting of all bit strings in which the number of 1's is divisible by p (see Razborov [17] and Smolensky [19]). But for moduli q that have distinct prime divisors, little is known, and the task of separating ACC, the union of the $ACC(q)$, from NC^1 is an outstanding unsolved problem in circuit complexity.

$ACC(q)$ has a model-theoretic characterization as the family of languages definable in an extension of first-order logic which contains predicate symbols for arbitrary relations on the natural numbers, and in which special "modular quantifiers" of modulus q occur along with ordinary quantifiers (see Barrington et al. [3] and Straubing [20]). Since there are languages that are complete for NC^1 under constant-depth reductions, in order to separate NC^1 from ACC, it is sufficient to show that for each $q > 1$ there is a language in NC^1 that does not belong to $ACC(q)$. This suggests that one might be able to attack the problem by model-theoretic means. However, the problem has resisted solution by this or any other method, and little progress has been made since the appearance of Smolensky's work.

Recently, Krebs, Lange, and Reifferscheid [11] raised the possibility of proving the separation for logics with a restricted class of numerical predicates. It is already known (see Straubing, Thérien, and Thomas [21]) that if the only available numerical predicate is $<$, then all the languages definable with ordinary and modular quantifiers of modulus q are regular, and all the groups in the syntactic monoids of these languages are solvable, of cardinality dividing a power of q. This implies, for example, that if q is odd, then one cannot define the set of bit strings with an even number of 1's in this logic. The natural next step is to allow the ternary relation $x + y = z$ on the natural

*Received by the editors April 24, 2006; accepted for publication (in revised form) January 4, 2007; published electronically May 22, 2007.
http://www.siam.org/journals/sicomp/37-2/65803.html

†Computer Science Department, Boston College, Chestnut Hill, MA 02476 (aroy@cs.bc.edu, straubin@cs.bc.edu).

numbers. One can prove the analogue of the separation between AC^0 and NC^1 in this setting by purely model-theoretic means, without recourse to results from circuit complexity (originally proved by Lynch [14]; the question is discussed at length in Barrington et al. [5]). In the present paper we extend this to formulas with ordinary and modular quantifiers over the numerical predicate $x+y=z$. This can be viewed as proving the separation between ACC and NC^1 in a highly uniform setting (recently, a circuit interpretation of this logic was given by Behle and Lange [9]).

We note that natural uniform versions of AC^0 and ACC result when one allows both addition and multiplication as numerical predicates (see Barrington, Immerman, and Straubing [4]). These formulas behave very differently and are much harder to analyze by model-theoretic means. So separating ACC from NC^1 even in this natural uniform setting still appears to be a very difficult problem.

We find it more convenient to first work in the setting of infinite bit strings that contain finitely many 1's. We view such a string as a particularly rudimentary structure (a linearly ordered finite set of 1's) embedded in the natural numbers. We are then faced with the question of how much of the expressive power of the larger structure (in this case, the integers under addition) is needed to express properties of the embedded structure (for instance, that the number of 1's is even). This is precisely the kind of problem considered in the study of "embedded finite models," and we are able to draw upon various collapse results that already appear in the model-theoretic literature. We obtain our result by first showing, in section 3, that it is sufficient to consider sentences that only quantify over positions in a bit string that contain a 1. The underlying quantifier-elimination procedure, while rather complicated in the case of modular quantifiers, is based on an idea that goes back to Presburger [16]. In section 4, we use another model-theoretic collapse, this one based on Ramsey's theorem, to show that it is sufficient to consider sentences in which the only numerical predicate is $<$, which can be analyzed by known semigroup-theoretic methods. Semigroup theory has been used in the past to obtain rather weak lower bounds for computations by circuits and branching programs (see, e.g., Barrington and Straubing [6]). By coupling the algebra in this way with ideas from model theory, we are able to extend its reach.

Nurmonen [15] establishes different nonexpressibility results for sentences with modular quantifiers, using a version of Ehrenfeucht–Fraïssé games. Schweikardt [18] proves nonexpressibility results for logics with different generalized quantifiers over the base $(\mathbb{N},+)$. Extension of the Ramsey property to generalized quantifiers is discussed in Benedikt and Libkin [10]. We have relied heavily on the account of collapse results for embedded finite models contained in two expository works by Libkin: the survey article [12] and the book [13].

Of course, we are most interested in proving the separation over arbitrary numerical predicates or, at the very least, over a class of numerical predicates that includes both addition and multiplication. In the final section we discuss both the prospects for generalizing the present work, and the obstacles to doing so.

2. Notation and statement of result.

We consider first-order logic $FO[+]$ with a single ternary relation $x+y=z$. Formulas are interpreted in the natural numbers $\mathbb{N}$. We adjoin to this logic a single unary relation π. The resulting formulas are interpreted in bit strings, with $\pi(x)$ taken to mean that the bit in position x is 1. In fact we can consider several such interpretations: in finite bit strings ($w \in \{0,1\}^*$), in infinite bit strings ($w \in \{0,1\}^{\mathbb{N}}$), and in infinite bit strings with a finite number of 1's ($w \in \{0,1\}^*0^\omega$, where 0^ω denotes an infinite sequence of 0's). A sentence ϕ in this logic accordingly defines three sets of strings:

$$L_\phi^{fin} = \{w \in \{0,1\}^* : w \models \phi\},$$

$$L_\phi^{\infty} = \{w \in \{0,1\}^{\mathbb{N}} : w \models \phi\},$$

and

$$L_\phi^{fs} = \{w \in \{0,1\}^* 0^\omega : w \models \phi\}.$$

(The letters "*fs*" stand for "finite support.")

For example, let ϕ be the sentence

$$\exists x \exists y ((x = y + y) \wedge \pi(x)),$$

which asserts that there is a 1 in an even-numbered position. Note that for this sentence L_ϕ^{fs} is a proper subset of L_ϕ^{∞}, and that $L_\phi^{fs} = L_\phi^{fin} 0^\omega$.

We denote this logic by $FO[\pi, +]$. More generally, if $\mathcal{R}$ is any set of relations on $\mathbb{N}$, we denote the analogous logic by $FO[\pi, \mathcal{R}]$. We define the languages L_ϕ^{fin}, etc., in exactly the same way.

To this apparatus we adjoin *modular quantifiers* $\exists^{r \bmod q}$ for a fixed modulus q and $0 \leq r < q$. The interpretation of $\exists^{r \bmod q} x\ \phi$ is, informally, "the number of positions x for which ϕ holds is congruent to r modulo q." More precisely, let $\phi(x, y_1, \ldots, y_k)$ be a formula with free variables $x, y_1, \ldots, y_k$. Let $w \in \{0,1\}^*$ or $w \in \{0,1\}^{\mathbb{N}}$, and let $a_1, \ldots, a_k < |w|$. (If w is infinite, this last condition is automatically satisfied for any natural numbers a_i.) Then we define

$$w \models (\exists^{r \bmod q} x\ \phi)(a_1, \ldots, a_k)$$

iff

$$|\{b < |w| : w \models \phi(b, a_1, \ldots, a_k)\}| \equiv r \pmod{q}.$$

(In particular, for infinite strings w, this implies that the set $\{b < |w| : w \models \phi(b, a_1, \ldots, a_k)\}$ is finite.) For example, the sentence

$$\exists^{0 \bmod 2} x\ \pi(x)$$

defines, in all three interpretations, the set of strings with an even number of 1's.

We denote this logic by $(FO + MOD_q)[\pi, +]$.

Here is our main result. Let $m > 1$, and let L_m denote the set of all finite bit strings in which the number of 1's is divisible by m.

THEOREM 2.1. *If m is a prime that does not divide q, then there is no sentence ϕ in $(FO + MOD_q)[\pi, +]$ such that $L_\phi^{fin} = L_m$ or $L_\phi^{\infty} = L_m 0^\omega$.*

Remark. If we consider instead the family $\mathcal{N}$ of all relations on $\mathbb{N}$, then the family of languages in $\{0,1\}^*$ definable by sentences in $(FO + MOD_q)(\pi, \mathcal{N})$ is precisely the nonuniform circuit complexity class $ACC(q)$ (see [3, 20]). If we let × denote multiplication in $\mathbb{N}$, then $(FO + MOD_q)[\pi, +, \times]$ is the natural uniform version of $ACC(q)$ (see [4]). For these logics, the analogues of Theorem 2.1 are equivalent to the conjectured separation of $ACC(q)$ and NC^1 in the nonuniform and uniform cases, respectively. Thus our theorem can be thought of as establishing this separation in a highly uniform setting.

In our proof of Theorem 2.1, we will use some notions from the algebraic theory of finite automata: To each regular language $L \subseteq \Sigma^*$ there is associated a finite monoid $M(L)$ (the *syntactic monoid* of L) and a homomorphism $\mu_L : \Sigma^* \rightarrow M(L)$ (the *syntactic morphism* of L) such that the value $\mu_L(w)$ determines whether or not $w \in L$. That is, there is a subset X of $M(L)$ such that $L = \mu_L^{-1}(X)$. ($M(L)$ is the *smallest* monoid with this property: It is the monoid of transformations on the states of the minimal automaton of L induced by elements of Σ^*. The homomorphism μ_L maps a word w to the transformation it induces, and X is the set of transformations that take an initial state to an accepting state.)

If $L \subseteq \Sigma^*$ and $\lambda \in \Sigma$, we say λ is a *neutral letter* for L if for any $u, v \in \Sigma^*$, $u\lambda v \in L$ iff $uv \in L$. In other words, deleting or inserting occurrences of λ does not affect a word's membership in L. In the algebraic setting, λ is a neutral letter for L iff $\mu_L(\lambda)$ is the identity of $M(L)$. For example, each of the languages $L_m \subseteq \{0,1\}^*$ defined above has 0 as a neutral letter.

3. Collapse to active-domain formulas. While our goal is to prove a result about definability of sets of finite strings, most of our argument concerns definability of sets of infinite strings. An easy reduction makes the connection between the two models.

LEMMA 3.1. *Let ϕ be a sentence of $(FO + MOD_q)[\pi, +]$ and let $L = L_\phi^{fin}$. Then there is a sentence ϕ' of $(FO + MOD_q)[\pi, +]$ such that*

$$L_{\phi'}^{fs} = L_{\phi'}^{\infty} = L0^\omega.$$

Proof. We define a formula $\phi[\leq x]$ with a single free variable x by rewriting it from the innermost quantifier outward, replacing each instance of

$$\mathcal{Q} z \alpha,$$

where $\mathcal{Q}$ is the quantifier $\exists$ or $\exists^{r \bmod q}$, by

$$\mathcal{Q} z((z \leq x) \wedge \alpha).$$

Then $L0^\omega$ is defined by the sentence

$$\exists x(\forall y(\pi(y) \rightarrow y \leq x) \wedge \phi[\leq x]). \qquad \square$$

Remark. Obviously, Lemma 3.1 holds for any of the logics $(FO + MOD_q)[\pi, \mathcal{R}]$ in which $\leq$ is definable.

An *active-domain formula* in $(FO + MOD_q)[\pi, +]$ is one in which every quantifier occurs in the form

$$\mathcal{Q} x(\pi(x) \wedge \alpha),$$

where $\mathcal{Q}$ is either the ordinary existential quantifier or a modular quantifier, and α is a formula. We call these *active-domain quantifiers*. In other words, we allow quantification only over positions that contain the bit 1. Libkin [12] sketches a proof that one can replace every formula in $FO[\pi, +]$ by an equivalent active-domain formula, provided one extends the signature (the *natural-active collapse*). Here we generalize this result to formulas that contain modular quantifiers. (We should add that the collapse to active-domain formulas holds for arbitrary finite structures—for instance, graphs—embedded in $(\mathbb{N}, +)$, not just sequences of 1's. One proves, in general, that any formula is equivalent to one in which quantification only ranges over elements of the embedded structure.)

We consider the logic

$$(FO + MOD_q)[\pi, +, <, 0, 1, \{\equiv_s : s > 1\}],$$

in which + is now treated as a binary function, 0 and 1 are constants, and $\equiv_s$ is a binary relation symbol denoting congruence modulo s. Of course, all these new constants and relations are definable in $FO[+]$, but we need to include them formally as part of the language in order to carry out the quantifier elimination.

THEOREM 3.2. *Let ϕ be a formula of $(FO + MOD_q)[\pi, +, <, 0, 1, \{\equiv_s : s > 1\}]$, with free variables in $\{x_1, \dots, x_r\}$. Then there is an active-domain formula ψ in the same logic such that for all $w \in \{0,1\}^* 0^\omega$ and $a_1, \dots, a_r \in \mathbb{N}$, we have $w \models \phi(a_1, \dots, a_r)$ iff $w \models \psi(a_1, \dots, a_r)$.*

Proof. The proof is by induction on the construction of ϕ. There is nothing to prove in the base case of quantifier-free formulas. For the inductive step, we assume

$$\phi = \mathcal{Q}z\ \phi', \tag{3.1}$$

where $\mathcal{Q}$ is either an existential quantifier ($\exists$) or a modular quantifier ($\exists^{k \bmod q}$) and ϕ' is a formula such that any quantifier appearing in ϕ' is an active-domain quantifier. We assume that ϕ' has free variables $x_1, x_2, \dots, x_r$ and bound variables (hence active-domain variables) $y_1, y_2, \dots, y_s$.

Notation. We shall write $\hat{\mathbf{v}}^m$ to denote the tuple $(v_1, v_2, \dots, v_m)$. When m is obvious from the context or is irrelevant, we simply write $\hat{\mathbf{v}}$ and refer to the ith coordinate as $\hat{\mathbf{v}}_i$.

Terms in our logic are expressions of the form

$$a_0 + a_1 w_1 + \cdots + a_k w_k,$$

where the a_i are in $\mathbb{N}$ and the w_i are variables. Atomic formulas have the form

$$\sigma = \tau, \quad \sigma < \tau, \quad \sigma > \tau, \quad \sigma \equiv_m \tau, \quad \pi(\sigma),$$

where σ, τ are terms. We can eliminate atomic formulas of the form $\pi(\sigma)$ by introducing a new active-domain variable y and replacing the atomic formula by

$$\exists y(\pi(y) \wedge y = \sigma).$$

We can rewrite each atomic formula $\sigma = \tau$ in ϕ that involves z as $nz = \rho$, where ρ does not involve z. Strictly speaking, ρ is not a term in our logic, since we do not have subtraction available, so this must be regarded as a shorthand for $nz + \rho_1 = \rho_2$, where ρ_1, ρ_2 are genuine terms that do not involve z. Later we will view the expression ρ as defining a partial function on $\mathbb{N}^{r+s}$. Similarly, we rewrite other atomic formulas involving z as

$$nz < \rho, \quad nz > \rho, \quad nz \equiv_m \rho,$$

where ρ does not involve z.

Let l be the least common multiple of the coefficients of z in these atomic formulas. Then since

$$\begin{aligned} nz = \rho \quad &\text{iff } lz = (l/n)\rho, \\ nz < \rho \quad &\text{iff } lz < (l/n)\rho, \\ nz \equiv_m \rho \quad &\text{iff } lz \equiv_{m(l/n)} (l/n)\rho \end{aligned}$$

we can suppose that z always appears with the same coefficient l in every atomic subformula of ϕ'.

Making a change of variable $z \mapsto lz$, we see that ϕ is equivalent to the following formula:

$$\mathcal{Q}\, z\ (z \equiv_l 0 \wedge \phi'),$$

where if z occurs in an atomic formula, it occurs with coefficient 1, and where each such formula has the form $z = \rho$, $z < \rho$, $z > \rho$, $z \equiv_m \rho$, where ρ does not involve z.

Atomic formulas in ϕ' of the form $z \equiv_m \rho$ can be replaced by

$$\bigvee_{i=0}^{m-1} (z \equiv_m i \wedge \rho \equiv_m i),$$

so we may suppose that in every such atomic formula ρ is a constant in $\mathbb{N}$. Let l' be the least common multiple of the moduli occurring in such atomic formulas. Then ϕ is equivalent to

$$\mathcal{Q}\, z \bigvee_{j=0}^{l'-1} \Big[z \equiv_{l'} j \quad \wedge \phi'_j \Big], \tag{3.2}$$

where ϕ'_j is the formula obtained from ϕ' upon replacing each congruence $z \equiv_m i$ by **true** or **false**, depending on whether this is consistent with $z \equiv_{l'} j$.

If $\mathcal{Q} = \exists$ in (3.2), then we can rewrite it as

$$\bigvee_{j=0}^{l'-1} \exists z \Big[z \equiv_{l'} j \quad \wedge \phi'_j \Big]. \tag{3.3}$$

Suppose $\mathcal{Q} = \exists^{k \bmod q}$. Observe that if $\alpha_1, \dots, \alpha_t$ are pairwise mutually exclusive, then we can rewrite

$$\exists^{k \bmod q} z \bigvee_{i=1}^{t} \alpha_i$$

as

$$\bigvee \bigwedge_{i=1}^{t} \exists^{k_i \bmod q} z\ \alpha_i,$$

where the disjunction is over all t-tuples $(k_1, \dots, k_t) \in \mathbb{Z}_q^t$ for which $\sum_{i=1}^t k_i = k$. Thus we can rewrite (3.2) as a boolean combination of formulas of the form

$$\exists^{k' \bmod q} z \Big[z \equiv_{l'} j \quad \wedge \phi'_j \Big].$$

We can thus assume that ϕ has the form

$$\mathcal{Q}\, z\ \Big((z \equiv_d c) \wedge \phi' \Big),$$

where $\mathcal{Q}$ is an ordinary existential or ordinary modular quantifier and ϕ' is an active-domain formula in which every atomic formula involving z is either of the form $z < \rho$, $z = \rho$, or $z > \rho$.

We now fix an instantiation of $\hat{\mathbf{x}}^r$, the free variables of ϕ, by a tuple $\hat{\mathbf{a}}^r \in \mathbb{N}^r$. To simplify the notation, we will not make explicit reference to $\hat{\mathbf{a}}^r$ in the remainder of the proof. Each ρ appearing on the right-hand side of one of our atomic formulas accordingly defines a partial function g from $\mathbb{N}^s$ into $\mathbb{N}$, where s is the number of active-domain variables. We set $\rho(t_1, t_2, \ldots, t_s)$ to be the value obtained by substituting $t_i \in \mathbb{N}$ for the variable y_i, $1 \leq i \leq s$, in ρ if this value is nonnegative; $\rho(t_1, \ldots, t_s)$ is undefined otherwise. We let $\{g_i : i \in I\}$ denote the set of these partial functions.

Let $w \in \{0,1\}^* 0^\omega$, and let $D \subseteq \mathbb{N}$ denote the set of positions in w that contain 1's. (That is, D is the active domain of w.) Let

$$\mathcal{B} = \bigcup_{i \in I} \{g_i(\hat{\mathbf{y}}) | \hat{\mathbf{y}} \in D^s\}.$$

Write $\mathcal{B}$ as an ordered set $\{b_0, b_1, \ldots, b_{p-1}\}$, where $b_0 < b_1 < b_2 < \cdots < b_{p-1}$. We denote by (a, b) the set $\{x \in \mathbb{N} : a < x < b\}$. By an *interval* in $\mathcal{B}$, we will mean either the leftmost interval $(-1, b_0)$, intervals of the form (b_i, b_{i+1}) for $0 \leq i \leq p-2$, or the rightmost interval (b_{p-1}, ∞).

LEMMA 3.3. *If there exists an integer z_0 in an interval in $\mathcal{B}$ such that*

$$w \models \phi'(z_0),$$

then

$$w \models \phi'(z_0')$$

for every z_0' in the interval. (That is, if an interval contains a witness, then every point in the interval is a witness.)

Proof. The proof is by induction on the construction of ϕ'. We will show that for every subformula ψ of ϕ' and every instantiation $\hat{\mathbf{d}}$ of the free active-domain variables by a tuple over D, $w \models \psi(z_0, \hat{\mathbf{d}})$ implies $w \models \psi(z_0', \hat{\mathbf{d}})$.

Since all atomic formulas of ϕ' that involve z have one of the forms $z < g_j(\hat{\mathbf{y}})$, $z = g_j(\hat{\mathbf{y}})$, or $z > g_j(\hat{\mathbf{y}})$ for some $j \in I$, and since $g_j(\hat{\mathbf{d}}) \in \mathcal{B}$ for all tuples $\hat{\mathbf{d}}$ over D, the claim holds for the atomic subformulas of ϕ'. The property clearly is preserved under boolean operations. Now suppose that the property holds for some subformula ψ of ϕ', and that $y_1, \ldots, y_j$ are the free active-domain variables in ψ. Our hypothesis applied to ψ implies that if z_0 and z_0' belong to the same interval of $\mathcal{B}$, then

$$\{\hat{\mathbf{d}} \in D^j : w \models \psi(z_0, \hat{\mathbf{d}})\} = \{\hat{\mathbf{d}} \in D^j : w \models \psi(z_0', \hat{\mathbf{d}})\}.$$

In particular, for each fixed $d_2, \ldots, d_j \in D$,

$$\{d_1 \in D : w \models \psi(z_0, \hat{\mathbf{d}})\} = \{d_1 \in D : w \models \psi(z_0', \hat{\mathbf{d}})\},$$

so, in particular, these two sets have the same cardinality. Thus if $\mathcal{Q}$ is either an existential or modular quantifier,

$$w \models \mathcal{Q} y_1(\pi(y_1) \wedge \psi(z_0, d_2, \ldots, d_j))$$

iff

$$w \models \mathcal{Q} y_1(\pi(y_1) \wedge \psi(z_0', d_2, \ldots, d_j)).$$

Thus the property is preserved under active-domain quantification. $\square$

We define the function $\chi_{c,d} : \mathbb{Z} \to \mathbb{Z}$ as follows:

$$\chi_{c,d}(\alpha) = \begin{cases} (c-\alpha) \bmod d & \text{if } \alpha \not\equiv_d c, \\ d & \text{otherwise.} \end{cases}$$

Corollary 3.4. *Let (l, r) be an interval in $\mathcal{B}$ such that $l \equiv_{dq} \alpha$. Then*

$$w \models \{(z_0 \equiv_d c) \wedge \phi'(z_0)\}$$

for some $z_0 \in (l, r)$ iff

$$l + \chi_{c,d}(\alpha) < r \quad \textit{and} \quad w \models \phi'(l + \chi_{c,d}(\alpha)).$$

Proof. Lemma 3.3 implies that if there is a witness at all in the interval (l, r), then *any* integer z_0 in the interval such that $z_0 \equiv_d c$ would be a witness. The integer $l + (c-\alpha) \bmod d$ satisfies this requirement if $c \not\equiv_d \alpha$. If $c \equiv_d \alpha$, then the integer $l + d$ satisfies the requirement. □

Remark. We count witnesses in two iterations: First, we count the number modulo q of witnesses z (if they exist) strictly contained in intervals (l, r), where $l < z < r$ and l, r are successive points in $\mathcal{B}$, and then we *separately* count points of $\mathcal{B}$ which are themselves witnesses. As a result, we need to distinguish the cases $c \equiv l \bmod d$ and $c \not\equiv l \bmod d$ in our formulas. The function $\chi_{c,d}$ enables us to distinguish between the two cases.

We also have a special property concerning the infinite interval (b_{p-1}, ∞), as follows.

Corollary 3.5. *Let $b_{p-1} \equiv_{dq} \alpha$. If*

$$w \models \exists^{k \bmod q} z \ \{(z \equiv_d c) \wedge \phi'\},$$

then

$$w \not\models \phi'(b_{p-1} + \chi_{c,d}(\alpha)).$$

Proof. If

$$w \models \phi'(b_{p-1} + \chi_{c,d}(\alpha)),$$

then Lemma 3.3 implies that every $z_0 \in (b_{p-1}, \infty)$ such that $z_0 \equiv_d c$ would be a witness. However,

$$w \models \exists^{k \bmod q} z \ \{(z \equiv_d c) \wedge \phi'\}$$

implies that there are only a finite number of witnesses. □

We also note the following fact.

Lemma 3.6. *Let $l, r \in \mathbb{N}$, where $l \leq r$, and let $c, d, q, \alpha, \beta \in \mathbb{N}$ be such that*

$$l \equiv \alpha \bmod dq \quad \textit{and} \quad r \equiv \beta \bmod dq.$$

Let $\eta_q(\alpha, \beta)$ denote the number modulo q of integers x in (l, r) such that $x \equiv_d c$. Then $\eta_q(\alpha, \beta)$ depends only on α, β, c, d, q.

Proof. Since the number mod q of points $x \equiv_d c$ in the interval (l, r) does not change under the maps $r \mapsto r + adq$, $l \mapsto l + bdq$ (where $a, b \in \mathbb{Z}$), $\eta_q(\alpha, \beta)$ is independent of the actual values of l and r. □

Remark 3.1. An explicit formula for $\eta_q(\alpha,\beta)$ is

$$\eta_q(\alpha,\beta) \equiv 1 + \frac{\beta - \alpha - (c-\alpha) \bmod d - (\beta - c) \bmod d}{d} - \delta \pmod{q},$$

where

$$\delta = \begin{cases} 2 & \text{if } \alpha \equiv_d c \text{ and } \beta \equiv_d c, \\ 1 & \text{exactly one of } \alpha \text{ or } \beta \text{ is } \equiv_d c, \\ 0 & \text{otherwise.} \end{cases}$$

However, the point of Lemma 3.6 is that $\eta_q(\alpha,\beta)$ depends only on the constants α, β, c, d, q, and so wherever it appears in our formulas, say, in the form $\eta_q(\alpha,\beta) \equiv_q \gamma$ (see, e.g., the formula CountZero(x,y) below), we can replace this by true or false. This renders the exact form of the expression $\eta_q(\alpha,\beta)$ irrelevant.

We now proceed to the quantifier elimination by building an active-domain formula equivalent to $\phi = \exists^{k \bmod q} z((z \equiv_d c) \wedge \phi'(z))$. The idea is to write a formula that counts, modulo q, the number of witnesses to $(z \equiv_d c) \wedge \phi'(z)$ in each interval of $\mathcal{B}$. At each step of the argument we show how to express some property of w in our language. Our initial result will be a formula in which the arbitrary quantifier is replaced by quantification over elements of $\mathcal{B}$, but in the end we will show how to rewrite these in terms of active-domain quantifiers.

Membership in $\mathcal{B}$: The formula Member(x) asserts that $x \in \mathcal{B}$:

$$\exists^a \hat{\mathbf{y}} \bigvee_{i \in I} (g_i(\hat{\mathbf{y}}) = x),$$

where $\exists^a \hat{\mathbf{y}}\ \alpha$ is an abbreviation for

$$\exists y_1(\pi(y_1) \wedge \exists y_2(\pi(y_2) \wedge \cdots \exists y_s(\pi(y_s) \wedge \alpha) \cdots)).$$

(x,y) *is an interval*: The formula $I(x,y)$ asserts that x and y are successive elements of $\mathcal{B}$:

$$\begin{aligned} &(x<y) \wedge \text{Member}(x) \wedge \text{Member}(y) \\ &\wedge \neg\exists z\ \big(\text{Member}(z) \wedge \big\{(x<z) \vee (z<y)\big\}\big). \end{aligned} \tag{3.4}$$

The interval (x,y) *in* $\mathcal{B}$ *has* $0 \bmod q$ *witnesses*: This is expressed by the sentence InteriorPointCountZero(x,y):

$$I(x,y) \wedge \text{CountZero}(x,y),$$

where *CountZero*(x,y) is

$$\begin{aligned} &\bigvee_{\substack{0 \le \alpha \le dq-1 \\ 0 \le \beta \le dq-1}} \Big[(x \equiv_{dq} \alpha) \wedge (y \equiv_{dq} \beta) \\ &\wedge \Big\{(x + \chi_{c,d}(\alpha) < y) \implies \Big(\neg\phi'(x + \chi_{c,d}(\alpha)) \vee \eta_q(\alpha,\beta) \equiv_q 0\Big)\Big\}\Big]. \end{aligned}$$

Remark 3.2. Since the function $\chi_{c,d}(\alpha)$ depends only on the constants c, d, and α, we can substitute the value of $\chi_{c,d}(\alpha)$ wherever it appears in our formulas, for example, in the formula for CountZero(x,y) above. Thus it is not necessary to express $\chi_{c,d}(\alpha)$ in terms of a boolean formula. A similar comment holds for $\eta_q(\alpha,\beta)$ (see Remark 3.1).

Interval (x,y) *in* $\mathcal{B}$ *contains* $\gamma \bmod q$ *witnesses, where* $\gamma \not\equiv_q 0$: This is expressed by the sentence InteriorPointCountNonZero(x,y,γ):

$$I(x,y) \wedge \text{CountNonZero}(x,y,\gamma),$$

where *CountNonZero*(x,y,γ) is

$$\bigvee_{\substack{0\le\alpha\le dq-1\\ 0\le\beta\le dq-1}} \Big[(x \equiv_{dq} \alpha) \wedge (y \equiv_{dq} \beta)$$
$$\wedge\ \ (x+\chi_{c,d}(\alpha) < y)\ \ \wedge\ \ \phi'(x+\chi_{c,d}(\alpha)) \wedge \eta_q(\alpha,\beta) \equiv_q \gamma\Big].$$

Interval (x,y) *in* $\mathcal{B}$ *contains* $\gamma \bmod q$ *witnesses*: This is expressed by the sentence InteriorPointCount(x,y,γ):

$$(\gamma \equiv_q 0 \implies \text{InteriorPointCountZero}(x,y))$$
$$\wedge\, (\gamma \not\equiv_q 0 \implies \text{InteriorPointCountNonZero}(x,y,\gamma)).$$

Minimum and maximum elements of $\mathcal{B}$: The formula for Min(x) is

$$\text{Member}(x) \wedge \neg\exists y(\text{Member}(y) \wedge y < x).$$

We define Max(x) similarly.

The leftmost interval contains $\gamma \bmod q$ *witnesses*: The formula $W(\gamma)$ given by

$$\exists x\ \Big[\text{Min}(x) \wedge \Big\{(\gamma \equiv_q 0) \implies \text{CountZero}(0,x)\Big\}$$
$$\wedge \Big\{(\gamma \not\equiv_q 0) \implies \text{CountNonZero}(0,x,\gamma)\Big\}\Big]$$

says that the interval $(0,b_0)$ contains $\gamma \bmod q$ witnesses. We have to modify this depending on whether or not 0 is itself a witness. Thus if $c \neq 0$, we set $\mathcal{C}_L(\gamma)$ to be $W(\gamma)$; otherwise, we set it to be $\phi'(0) \wedge W(\gamma-1)$.

The rightmost interval contains no witnesses: This is expressed by $\mathcal{C}_R$:

$$\exists\, x\ \left\{\text{Max}(x) \wedge \bigwedge_{0\le\alpha\le dq-1} \{(x \equiv_{dq} \alpha) \to \neg\phi'(x+\chi_{c,d}(\alpha))\}\right\}.$$

Number mod q *of intervals* (b_i, b_{i+1}) *containing* $\gamma \bmod q$ *witnesses*: The sentence $H(\delta,\gamma)$ asserts that there are $\delta \bmod q$ intervals (x,y) with endpoints in $\mathcal{B}$ having $\gamma \bmod q$ witnesses:

$$\text{H}(\delta,\gamma) = \exists^{\delta \bmod q}\, x\ \exists\, y\ \text{InteriorPointCount}(x,y,\gamma).$$

Number mod q *of witnesses from intervals* (b_i, b_{i+1}): The formula $\mathcal{C}_{\text{int}}(\gamma)$ asserts that the number of witnesses contained in intervals (b_i, b_{i+1}), where $b_i, b_{i+1} \in \mathcal{B}$, is congruent to $\gamma \bmod q$:

$$\bigvee_{\substack{0\le\gamma_j\le q-1\\ 0\le j\le q-1\\ \sum_{j=0}^{q-1} j\gamma_j \equiv \gamma \bmod q}} \ \bigwedge_{i=0}^{q-1} H(i,\gamma_i).$$

Number mod q *of witnesses from* $\mathcal{B}$: The sentence $\mathcal{C}_{\mathcal{B}}(\gamma)$ asserts that the number of witnesses $b_i \in \mathcal{B}$ is congruent to γ mod q:

$$\exists^{\gamma \bmod q}\, l\ (\mathrm{Member}(l) \wedge (l \equiv_d c) \wedge \phi'(l)).$$

Total number mod q *of witnesses*: The sentence $\mathcal{C}_{\mathrm{tot}}(\gamma)$ asserts that the total number of witnesses is congruent to γ modulo q:

$$\bigvee_{\substack{0 \le \gamma_1, \gamma_2, \gamma_3 \le q-1 \\ \gamma_1+\gamma_2+\gamma_3 \equiv_q \gamma}} (\mathcal{C}_{\mathcal{B}}(\gamma_1) \wedge \mathcal{C}_L(\gamma_2) \wedge \mathcal{C}_{\mathrm{int}}(\gamma_3)).$$

Thus $\exists^{k \bmod q} z\big\{(z \equiv_d c) \wedge \phi(z)\big\}$ is equivalent to the sentence

$$\mathcal{T} = \mathcal{C}_{\mathrm{tot}}(k) \wedge \mathcal{C}_R.$$

Note that $\mathcal{T}$ is *almost* active-domain. The non–active-domain quantifiers in $\mathcal{T}$ are of the form

$$\exists\, x\ \{\mathrm{Member}(x) \wedge \mathcal{T}'(x)\} \text{ or of the form } \exists^{k \bmod q} x\ \{\mathrm{Member}(x) \wedge \mathcal{T}'(x)\}.$$

In the first case, we can replace the ordinary existential quantifier in front of x by the definition of Member(x) to get an active-domain formula of the form

$$\exists^a \hat{\mathbf{y}} \bigvee_{i \in I} \mathcal{T}'(g_i(\hat{\mathbf{y}})).$$

Rewriting the second formula with active-domain quantifiers is more complicated. Let $g_1, \ldots, g_m$ be the partial functions, and let $\mathcal{B}_i$ be the set of points in $g_i(D^s)$ that are not in $g_j(D^s)$ for any $j > i$. Since $\mathcal{B}$ is the disjoint union of the $\mathcal{B}_i$, we can rewrite

$$\exists^{k \bmod q} x\ \{\mathrm{Member}(x) \wedge \mathcal{T}'(x)\}$$

as a boolean combination of sentences of the form

$$\exists^{k' \bmod q} x\ \{\mathrm{Member}_j(x) \wedge \mathcal{T}'(x)\}, \tag{3.5}$$

where Member$_j(x)$ asserts that x belongs to $\mathcal{B}_j$. It is easy enough writing an active-domain formula that asserts that x is in $\mathcal{B}_j$, but how do we count the number of elements in $\mathcal{B}_j$ with a given property?

Let $\prec$ denote the lexicographic ordering on D^s. We can express $\hat{\mathbf{y}} \prec \hat{\mathbf{y}}'$ as a boolean combination of the formulas $y_i < y_i'$ and $y_i = y_i'$. Let $LL_i(\hat{\mathbf{y}})$ be the formula

$$\neg\exists^a \hat{\mathbf{y}}'((g_i(\hat{\mathbf{y}}) = g_i(\hat{\mathbf{y}}')) \wedge (\hat{\mathbf{y}} \prec \hat{\mathbf{y}}')).$$

This asserts that $\hat{\mathbf{y}}$ is the lexicographically maximal s-tuple yielding the value $g_i(\hat{\mathbf{y}})$ under g_i. (Implicit in this is the assertion that $g_i(\hat{\mathbf{y}})$ is defined, which is expressed by a simple inequality.) We can thus rewrite our formula (3.5) as

$$\exists^{k' \bmod q}(\hat{\mathbf{y}} \in D^s)\left(LL_j(y) \wedge \mathcal{T}'(g_j(\hat{y})) \wedge \neg\exists \hat{\mathbf{y}}' \bigvee_{i > j} (g_i(\hat{\mathbf{y}}') = g_j(\hat{\mathbf{y}}))\right).$$

Finally, we note that modular quantification over s-tuples of elements of D is expressible in terms of modular quantification over active-domain elements. Indeed,

$$\exists^{k \bmod q}(y_1, y_2)\ \alpha$$

is equivalent to the disjunction of

$$\bigwedge_{i=0}^{q-1} \exists^{i \bmod q} y_1\ \exists^{f(i) \bmod q} y_2\ \alpha \tag{3.6}$$

over all functions f from $\mathbb{Z}_q$ to itself such that $\sum_{i=0}^{q-1} if(i) = k$, and we can extend this inductively to quantification over tuples of arbitrary size.

We have said nothing about how to eliminate ordinary non–active-domain quantifiers. This case is treated in Libkin [12], which was the starting point for the present proof. The argument follows the same pattern, but is much simpler, since we do not need to count either points in the images of the g_i or points in their domains. We merely have to assert that there exists some $u \in \mathcal{B}$ such that

$$\left\{ \bigvee_{\substack{0 \le e \le d-1 \\ u+e \ge 0 \\ u+e \equiv_d c}} \phi'(u+e) \right\} \vee \left\{ \bigvee_{\substack{0 \le e \le d-1 \\ u-e \ge 0 \\ u-e \equiv_d c}} \phi'(u-e) \right\}$$

holds, and this is easily carried out using the Member formula introduced earlier. □

4. Collapse to formulas with $<$ as the only numerical predicate.

4.1. Ramsey property. Our discussion here closely parallels that of Libkin [13]. Let $\mathcal{R}$ be any set of relations on $\mathbb{N}$, and let $\phi(x_1, \dots, x_k)$ be an active-domain formula in $(FO + MOD_q)[\pi, \mathcal{R}]$. We say that ϕ has the *Ramsey property* if for each infinite subset X of $\mathbb{N}$ there exists an infinite subset Y of X and an active-domain formula $\psi(x_1, \dots, x_k)$ in $(FO + MOD_q)[\pi, <]$ that satisfies the following condition: If $w \in \{0,1\}^* 0^\omega$ and all the 1's in w are in positions belonging to Y, then for all $a_1, \dots, a_k \in Y$,

$$w \models \phi(a_1, \dots, a_k) \text{ iff } w \models \psi(a_1, \dots, a_k).$$

Lemma 4.1. *Let $\mathcal{N}$ be the set of all relations on $\mathbb{N}$. Every active-domain formula in $(FO + MOD_q)[\pi, \mathcal{N}]$ has the Ramsey property.*

Proof. The Ramsey property for an assortment of generalized quantifiers is proved by Benedikt and Libkin [10] (also in [13, Lemma 13.15, p. 259]) by using induction on the quantifier depth. While they do not explicitly consider the modular quantifiers that we use here, there is no essential change in the proof. For clarity, we include the inductive step for modular quantifiers.

Let $\phi(\hat{\mathbf{x}}) = \exists^{k \bmod q} y\ [\pi(y) \wedge \phi_1(y, \hat{\mathbf{x}}^r)]$ be an active-domain formula in $(FO + MOD_q)[\pi, \mathcal{N}]$. By the induction hypothesis (from Lemma 13.15 in [13]), for each infinite subset X of $\mathbb{N}$ there exists an infinite subset Y of X and an active-domain formula $\psi_1(y, \hat{\mathbf{x}})$ in $(FO + MOD_q)[\pi, <]$ such that if $w \in \{0,1\}^* 0^\omega$ and all the 1's in w are in positions belonging to Y, then for all $\hat{\mathbf{a}}^r \in Y^r$ and $b \in Y$, $w \models \psi_1(b, \hat{\mathbf{a}})$ iff $w \models \phi_1(b, \hat{\mathbf{a}})$. This implies that for every $\hat{\mathbf{a}}$,

$$\{b \in Y | w \models \psi_1(b, \hat{\mathbf{a}})\} = \{b \in Y |\ w \models \phi_1(b, \hat{\mathbf{a}})\}.$$

Let $\psi(\hat{\mathbf{x}}) = \exists^{k \bmod q} y\ [\pi(y) \wedge \psi_1(y, \hat{\mathbf{x}})]$. Then for every w such that its 1's are in Y and $\hat{\mathbf{a}} \in Y^r$, $w \models \psi(\hat{\mathbf{a}})$ iff

$$|\{b \in Y | w \models \psi_1(b, \hat{\mathbf{a}})\}| \equiv_q k.$$

This happens iff

$$|\{b \in Y | w \models \phi_1(b, \hat{\mathbf{a}}\}| \equiv_q k$$

since the two sets are identical. Thus $w \models \psi(\hat{\mathbf{a}})$ iff $w \models \phi(\hat{\mathbf{a}})$. □

The Ramsey property allows us to capture a subset of a language expressible by a formula ϕ (which satisfies the Ramsey property) using a new formula over a very limited vocabulary (the only numerical predicate allowed is $<$). This limited vocabulary restricts the kind of language that can be expressed.

Lemma 4.2. *Let $L_\psi = \{w | \, w \in \{0,1\}^*\}$ be the set of finite bit strings defined by an active-domain sentence $\psi \in (FO + MOD_q)[\pi, <]$.*

(i) *The language L_ψ is regular. Moreover, the syntactic monoid $M(L_\psi)$ contains only solvable groups whose order divides a power of q.*
(ii) *L_ψ has 0 as a neutral letter.*
(iii) *Let $z \in \Sigma^*$. Then $z \in L_\psi$ iff $z0^\omega \models \psi$.*

Proof. Condition (i) is a result of Straubing, Thérien, and Thomas [21]. Inserting or deleting 0's from any string satisfying ψ does not alter the truth value of any atomic formula of the form $x < y$, provided the variables represent positions containing 1, which is the case here, since ψ is active-domain. Conditions (ii) and (iii) then follow by an easy induction on the quantifier depth. □

4.2. Proof of Theorem 2.1. Let m be a prime that does not divide q, and suppose, contrary to the claim in the theorem, that L_m is defined by a sentence ϕ of $(FO + MOD_q)[\pi, +]$. By Lemma 3.1, Theorem 3.2, and Lemma 4.1, there exists an active-domain sentence ψ of $(FO + MOD_q)[\pi, <]$ and an infinite subset Y of $\mathbb{N}$ such that for all $w \in \{0,1\}^*0^\omega$ in which all 1's are in positions belonging to Y, $w \models \psi$ iff $w \in L_m 0^\omega$. Let L_ψ denote the set of *finite* bit strings that satisfy ψ. We prove the following lemma.

Lemma 4.3. *$L_m = L_\psi$.*

Proof. We first show that $L_\psi \subseteq L_m$. Let $z' \in L_\psi$. We pad z' with 0's so that the 1's in the new padded string z'' appear in positions included in the set Y. Since $z'' \in L_\psi$ (by Lemma 4.2 (ii)), we conclude that $z''0^\omega \models \psi$ (by Lemma 4.2 (iii)). Since the 1's in $z''0^\omega$ appear in positions in Y, $z''0^\omega \models \phi$. Hence $z''0^\omega \in L_m 0^\omega$, so $z'' \in L_m$. Removing additional neutral letter 0's introduced while padding z', we conclude that $z' \in L_m$.

The opposite inclusion ($L_m \subseteq L_\psi$) is proved by reversing each step above. □

Since the syntactic monoid of L_m is the cyclic group Z_m and that of L_ψ has groups of order dividing a power of q (via Lemma 4.2), we have a contradiction since $(m, q) = 1$. Thus L_m cannot be defined by a sentence in $(FO + MOD_q)[\pi, +]$. This completes the proof.

4.3. Other nondefinability results. Here we show how to extend Theorem 2.1 to prove nonexpressibility results for other languages. We begin by removing the restriction to binary alphabets.

Let Σ be a finite alphabet and let us consider languages definable in the logic $\mathcal{L}_{q,\Sigma,+} = (FO + MOD_q)[\{\pi_\sigma : \sigma \in \Sigma\}, +]$, where each π_σ is a unary predicate: $\pi_\sigma x$ is interpreted to mean that the letter in position x is σ. We designate a special letter

$\lambda \in \Sigma$, and say that a formula is active-domain (with respect to λ) if every existential and modular quantifier $\mathcal{Q}$ occurs in the form $\mathcal{Q}x((\vee_{\sigma \neq \lambda} \pi_\sigma x) \wedge \alpha)$. Note that we need never use the atomic formula $\pi_\lambda x$, even in non–active-domain formulas, as it is equivalent to the conjunction of the $\neg\pi_\sigma x$ over all letters σ not equal to λ. All the preceding results hold in this broader setting, with no changes to their proofs. We thus have the following theorem.

THEOREM 4.4. *Let $L \subseteq \Sigma^*$, with $\lambda \in \Sigma$ a neutral letter for L. If L is definable in $\mathcal{L}_{q,\Sigma,+}$, then it is definable by a sentence of $(FO + MOD_q)[\{\pi_\sigma : \sigma \in \Sigma\}, <]$. In particular, L is regular, and every group in $M(L)$ is solvable, with cardinality dividing a power of q.*

The foregoing theorem allows us to give an effective characterization of all the *regular* languages in $\mathcal{L}_{q,\Sigma,+}$.

THEOREM 4.5. *Let $L \subseteq \Sigma^*$ be regular. L is definable in $\mathcal{L}_{q,\Sigma,+}$ iff for all $t > 0$ every group in $\mu_L(\Sigma^t)$ is solvable and has cardinality dividing a power of q.*

The reduction to the neutral letter case is somewhat involved, so we delegate the proof to the next section. The same property is known to characterize the regular languages in $ACC(q)$, provided that the conjectured separation of $ACC(q)$ and NC^1 holds [3].

Since L is regular, there exist integers k and l such that $\mu_L(\Sigma^{k+l}) = \mu_L(\Sigma^k)$ (since $\mu_L(\Sigma^t) \subseteq M(L)$ for all $t \geq 0$ and $M(L)$ is finite). Thus we can effectively enumerate all the sets $\mu_L(\Sigma^t)$ and all their subgroups. We thus have the following result.

COROLLARY 4.6. *Given an integer $q > 1$ and a regular language $L \subseteq \Sigma^*$, the question of whether L is definable in $\mathcal{L}_{q,\Sigma,+}$ is decidable.*

Here is an application of Theorem 4.5. Let G be a finite group and let $\Sigma \subseteq G$ be a set of generators of G. We treat G as a finite alphabet; to each word $w \in \Sigma^*$ we assign the group element $\phi(w)$ that results by multiplying together the letters of w. The *word problem for G* (with respect to Σ) is the language $\{w \in \Sigma^* : \phi(w) = 1\}$. Barrington [2] showed that the word problem for any finite nonsolvable group is complete for NC^1 with respect to constant-depth reductions, so that the conjectured separation of ACC from NC^1 is equivalent to the assertion that no such word problem belongs to ACC. We can verify directly that no such word problem L is definable in $\mathcal{L}_{q,\Sigma,+}$: L is a regular language, and it is easy to check that $M(L) = G$ and $\mu_L = \phi$. If G is nonsolvable, then its commutator subgroup G' is also nonsolvable, and thus every element of G' is the image of a word over Σ of length divisible by $|G|$ (each commutator is an image of a word of the form $uvu^{|G|-1}v^{|G|-1}$, where $u, v \in \Sigma$). We can pad each of these words with a sufficient number of copies of $\sigma^{|G|}$ (for some fixed $\sigma \in \Sigma$) so that they all have the same length t. Thus $G' \subseteq \phi(\Sigma^t)$. Since G' is nonsolvable, Theorem 4.5 now implies that L is not definable is $\mathcal{L}_{q,\Sigma,+}$.

THEOREM 4.7. *No word problem of a finite nonsolvable group is definable in any $\mathcal{L}_{q,\Sigma,+}$.*

Note that it is precisely the nonsolvability of G, rather than the relation between $|G|$ and q, that is at issue here: For instance, a word problem of the alternating group of degree 5, whose cardinality is 60, is not definable in $\mathcal{L}_{30,\Sigma,+}$ even though the cardinality and modulus are consistent. On the other hand, the word problem for any solvable group of order 60 is definable in this logic.

5. Proof of Theorem 4.5.

5.1. Two essential lemmas. Let Σ be a finite alphabet. We prove that definability in $(FO + MOD_q)[\{\pi_\sigma : \sigma \in \Sigma\}, +, <]$ (which we denote by $\mathcal{L}$ for the rest of this section) is preserved under inverse length-multiplying morphisms and quotients.

Remark. Note that we are admitting $x < y$ as an atomic formula, rather than simply defining it in terms of $+$. This is largely a matter of convenience; we could still carry out the proof if we allowed only $+$ as a numerical predicate.

Given a language $L \subseteq \Sigma^*$ and strings $u, v \in \Sigma^*$, we define the language $u^{-1}Lv^{-1} = \{w \in \Sigma^* | uwv \in L\}$.

Lemma 5.1. *Let $L \subseteq \Sigma^*$ be definable in $\mathcal{L}$. Then $u^{-1}Lv^{-1}$ is also definable in $\mathcal{L}$.*

Proof. It suffices to prove that $\sigma^{-1}L$ and $L\sigma^{-1}$ are definable in $\mathcal{L}$ for each $\sigma \in \Sigma$. We exhibit a proof of the first of these assertions by constructing a formula $\psi[\phi]$ for $\sigma^{-1}L$ given a formula ϕ for L. (We omit the almost identical proof of the second assertion.) To accomplish this, we encode each position x in σv by a pair of positions (x_1, x_2) in v: We map x to $(1, x-1)$ if $x > 0$, and to $(0, 0)$ if $x = 0$. Note that this requires $|v| \geq 2$, so we must treat the case where $|v| < 2$ separately. The encoding is clearly injective; let us denote its inverse by α.

We first write a formula $\psi_1[\phi]$ satisfied by all strings $v \in \Sigma^*$ of length 0 or 1 such that $\sigma v \models \phi$ (such a formula is trivial to write since there are only three strings to consider). For strings v of length ≥ 2, we show how to construct $\psi_2[\phi]$ by recursion over the term structure of ϕ. The final formula $\psi[\phi]$ is $\psi_1[\phi] \wedge \psi_2[\phi]$.

Our inductive hypothesis is the following: Given a formula $\phi(x_1, x_2, \ldots, x_k)$, there exists a formula $\psi_2[\phi](x_{1,1}, x_{2,1}, \ldots, x_{1,k}, x_{2,k})$ such that if $|v| \geq 2$, then $v \models \psi_2[\phi](b_{1,1}, b_{2,1}, \ldots, b_{1,k}, b_{2,k})$ iff $\sigma v \models \phi(\alpha(b_{1,1}, b_{2,1}), \ldots, \alpha(b_{1,k}, b_{2,k}))$. In particular, the former condition can hold only if all the $\alpha(b_{1,k}, b_{2,k})$ are defined. When there are no free variables then $\sigma v \models \phi$ iff $v \models \psi_2[\phi]$ as desired (if $|v| \geq 2$).

The formula $\psi_2[\phi]$ is defined below, depending on the following choices for ϕ:

(1) $Q_\tau(x)$: If $\tau \neq \sigma$, then $\psi_2[\phi] = (x_1 = 1) \wedge Q_\tau(x_2)$; otherwise set $\psi_2[\phi] = (Q_\sigma(x_2) \wedge x_1 = 1) \vee (x_1 = 0)$.

(2) $x + y = z$: We enumerate the subcases depending on the number of x_1, y_1, z_1 equal to 0:

$$\begin{aligned} \psi_2[\phi] = ((x_1 = y_1 = z_1 = 1) \wedge (x_2 + y_2 + 1 = z_2)) \\ \vee ((x_1 = 0) \wedge (y_1 = z_1 = 1) \wedge (y_2 = z_2)) \\ \vee ((y_1 = 0) \wedge (x_1 = z_1 = 1) \wedge (x_2 = z_2)) \\ \vee (x_1 = y_1 = z_1 = 0). \end{aligned}$$

(3) $\neg\phi_1$: $\psi_2[\phi] = \neg\psi_2[\phi_1]$.

(4) $\phi_1 \wedge \phi_2$: $\psi_2[\phi] = \psi_2[\phi_1] \wedge \psi_2[\phi_2]$.

(5) $\exists\, x\ \phi_1$: $\psi_2[\phi] = \exists\,(x_1, x_2)\ \psi_2[\phi]$.

(6) $\exists^{a \bmod q}\, x\ \phi_1$:

$$\begin{aligned} \psi_2[\phi] = (\exists^{a \bmod q}(x_1, x_2)(x_1 = 1) \wedge \psi_2[\phi_1] \wedge \neg\exists(x_1, x_2)(x_1 = 0 \wedge \psi_2[\phi])) \\ \vee (\exists^{a-1 \bmod q}(x_1, x_2)(x_1 = 1) \wedge \psi_2[\phi_1] \wedge \exists(x_1, x_2)(x_1 = 0 \wedge \psi_2[\phi_1])). \end{aligned}$$

Note that both modular and existential quantification over tuples (x_1, x_2) can be expressed as a boolean combination of quantification over x_1 and x_2 (see (3.6) and the remarks preceding it). Also note that we strictly cannot have terms like $(x + 1) = y$ in our logic as we have written above; we still use these as a (clearer) shorthand for the more elaborate formula $\neg\exists z((x < z) \wedge (z < y)) \wedge (x \neq y)$. □

Lemma 5.2. *Let Σ, Γ be finite alphabets and let $f : \Gamma^* \to \Sigma^*$ be a homomorphism such that $f(\Gamma) \subseteq \Sigma^r$ for some fixed $r > 0$. If $L \subseteq \Sigma^*$ is definable in $\mathcal{L}$, then $f^{-1}(L) \subseteq \Gamma^*$ is also definable in $\mathcal{L}$.*

Proof. Let ϕ be a formula in $\mathcal{L}$, such that $w \in L$ iff $w \models \phi$. We construct (via recursion over the term structure of ϕ) a formula $\psi[\phi]$ in $\mathcal{L}$ such that for any $v \in \Gamma^*$, $v \models \psi[\phi]$ iff $f(v) \models \phi$. Once again, we do this by encoding each position in $f(v)$ by a pair of positions in v. In this case, x is encoded by $(x \bmod r, \lfloor x/r \rfloor)$. Note that this requires $|v| \geq r$, so again we will have to treat the finite number of exceptions separately. The inverse of this encoding, $\alpha(x_1, x_2) = rx_1 + x_1$, is defined iff $x_1 < r$.

We first write a formula $\psi_1[\phi]$ satisfied by the (finite) set of strings $v \in \Gamma^*$, where $|v| < r$ and $f(v) \models \phi$:

$$\psi_1[\phi] = \bigvee_{\substack{v=\sigma_0\sigma_1\ldots\sigma_{s-1} \\ s<r \\ f(v)\models\phi}} \bigwedge_{i=0}^{s-1} Q_{\sigma_i}(i).$$

For strings v of length $\geq r$, we show how to construct $\psi_2[\phi]$ by recursion over the term structure of ϕ. The final formula $\psi[\phi]$ is $\psi_1[\phi] \wedge \psi_2[\phi]$.

Our inductive hypothesis is the following: Given a formula $\phi(x_1, x_2, \ldots, x_k)$, there exists a formula $\psi_2[\phi](x_{1,1}, x_{2,1}, \ldots, x_{1,k}, x_{2,k})$ such that if $|v| \geq r$, then $v \models \psi_2[\phi](b_{1,1}, b_{2,1}, \ldots, b_{1,k}, b_{2,k})$ iff $f(v) \models \phi(\alpha(b_{1,1}, b_{2,1}), \ldots, \alpha(b_{1,k}, b_{2,k}))$. In particular, the former condition can hold only if all the $\alpha(b_{1,k}, b_{2,k})$ are defined. When there are no free variables then $f(v) \models \phi$ iff $v \models \psi_2[\phi]$ as desired (if $|v| \geq r$).

We set $\psi[\phi] = \psi_1[\phi] \wedge \psi_2[\phi]$, where the formula $\psi_2[\phi]$ is defined recursively, depending on the following choices for ϕ:

(1) $Q_\sigma x$: Then $\psi_2[\phi] = (\bigvee_{f(\gamma)_i=\sigma} Q_\gamma(x_2) \wedge x_1 = i)$.

(2) $x + y = z$: This would imply that $x_1 + y_1 - z_1 = r(z_2 - x_2 - y_2)$. Since $1 \leq x_1 + y_1 - z_1 < 2r$ and $r | (x_1 + y_1 - z_1)$, the left-hand side $x_1 + y_1 - z_1$ is either r or 0 (and this determines the right-hand side's values). Thus

$$\psi_2[\phi] = (x_1 + y_1 = z_1 \wedge x_2 + y_2 = z_2) \vee (x_1 + y_1 = z_1 + r \wedge x_2 + y_2 + 1 = z_2).$$

(3) $\neg\phi_1$: $\psi_2[\phi] = \neg\psi_2[\phi_1]$.

(4) $\phi_1 \wedge \phi_2$: $\psi_2[\phi] = \psi_2[\phi_1] \wedge \psi_2[\phi_2]$.

(5) $\exists\, x\ \phi_1$: $\psi_2[\phi] = \exists\, (x_1, x_2)\ ((x_1 < r) \wedge \psi_2[\phi_1])$.

(6) $\exists^{a \bmod q}\, x\ \phi_1$: $\psi_2[\phi] = \exists^{a \bmod q}\, (x_1, x_2)\ ((x_1 < r) \wedge \psi_2[\phi_1])$.

As in Lemma 5.1, both modular and existential quantification over tuples (x_1, x_2) can be expressed as a boolean combination of quantification over x_1 and x_2 (see (3.6) and the remarks preceding it). □

5.2. Reduction to the neutral-letter case. We prove that every group contained in $\mu_L(\Sigma^t)$ (in the statement of Theorem 4.5) is the syntactic monoid of a (regular) language with a neutral letter definable in $\mathcal{L}$. Then Theorem 4.4 implies that every such group has to be solvable and has cardinality dividing a power of q. This reduction to the neutral letter case is done in Lemma 5.3 below. Note that the reverse direction follows easily from Straubing, Thérien, and Thomas [21]: If every group in $\mu_L(\Sigma^t)$ is solvable and has order dividing a power of q, then every subgroup of $M(L)$ is solvable and has order dividing a power of q, and this implies that L is definable in $(FO + MOD_q)[\{\pi_\sigma : \sigma \in \Sigma\}, <]$ and hence is definable in $\mathcal{L}_{q,\Sigma,+}$.

LEMMA 5.3. *Let $L \subseteq \Sigma^*$ be regular, and suppose L is definable in $\mathcal{L}$. Then for every $t \geq 0$ and every group $G \subseteq \mu_L(\Sigma^t)$, there exists a finite alphabet $\Gamma = \Gamma_G$ and a language $L_G \subseteq \Gamma^*$, such that L_G has a neutral letter and is definable in $\mathcal{L}$. Moreover, L_G is regular and $M(L_G) = G$.*

Proof. We define the finite alphabet

$$\Gamma = \{\gamma_w : w \in \Sigma^t,\, \mu_L(w) \in G\}.$$

The map $\gamma_w \mapsto w$ extends to a homomorphism f from Γ^* into Σ^* such that $f(\Gamma) \subseteq \Sigma^t$. We define

$$L_G = \{v \in \Gamma^* : \mu_L(f(v)) = e\},$$

where e is the identity of G.

Note that L_G has a neutral letter γ_v, where $\mu_L(v) = e$. We will show shortly that L_G is definable by a sentence of $\mathcal{L}$. First note that L_G is regular: It is recognized by a deterministic finite automaton (DFA) with state set G, initial and accepting state e, and state transitions

$$\gamma_w : g \mapsto g\mu_L(w).$$

Every state of this automaton is accessible from the initial state, and equivalent states must be identical, because of cancellation in the group. Thus this is the minimal DFA of L_G, and consequently $M(L_G) = G$.

It remains to establish the claim about definability of L_G in $\mathcal{L}$. It is well known that if $K \subseteq \Sigma^*$ is regular, then for each $m \in M(K)$, the set $\mu_K^{-1}(m)$ is a finite boolean combination of languages of the form

$$u^{-1}Kv^{-1} = \{w \in \Sigma^* : uwv \in K\},$$

where $u, v \in \Sigma^*$. We have

$$L_G = f^{-1}(\mu_L^{-1}(e)),$$

so our claim will follow if we can show that definability is preserved under the language operations

$$K \mapsto u^{-1}Kv^{-1}$$

and

$$K \mapsto f^{-1}(K).$$

This was established by Lemmas 5.1 and 5.2. □

6. Monadic predicates. In this section, we consider definability of languages in first-order logic with modular quantifiers when we allow monadic (i.e., arity 1) numerical predicates. More specifically, we consider the logic $MON_q = (FO + MOD_q)[<, \{\pi_\sigma\}_{\sigma\in\Sigma}, \theta_1, \theta_2, \ldots, \theta_r]$, where θ_i, $1 \leq i \leq r$, are bit-valued functions on $\mathbb{N}$.

We define a map

$$\widehat{\ }: \Sigma^* \to (\Sigma \times \{0,1\}^r)^*$$

as follows:

$$w = \sigma_0\sigma_1 \ldots \sigma_{n-1} \mapsto \widehat{w} = (\sigma_0, \gamma_{1,0}, \gamma_{2,0}, \ldots, \gamma_{r,0}) \cdots (\sigma_{n-1}, \gamma_{1,n-1}, \gamma_{2,n-1}, \ldots, \gamma_{r,n-1}),$$

where $\gamma_{i,j} = \theta_i(j)$. Given $L \subseteq \Sigma^*$, we denote $\widehat{L} = \{\widehat{w}|\ w \in L\}$.

Lemma 6.1. *Let ϕ be a sentence in MON_q. There exists a language $K \subseteq (\Sigma \times \{0,1\}^r)^*$ such that* (a) *K is regular, and every group in the syntactic monoid of K is solvable with order dividing a power of q;* (b) *if $w \in \Sigma^*$, then $w \models \phi$ iff $\widehat{w} \in K$.*

Proof. We take the formula ϕ and rewrite it by replacing every occurrence of $\theta_i(x)$ by the disjunction of all $\pi_{(\sigma,v)}x$, with $\sigma \in \Sigma$ and $v \in \{0,1\}^r$, for which the ith component of v is 1. Likewise we replace every occurrence of $\pi_\sigma x$ by the disjunction of $\pi_{(\sigma,v)}$ over all $v \in \{0,1\}^r$. By [21], the resulting sentence $\widehat{\phi}$, interpreted in words over $\Sigma \times \{0,1\}^r$, defines a regular language K whose syntactic monoid possesses the desired property, and it is clear that $w \models \phi$ iff $\widehat{w} \models \hat{\phi}$. (Observe that not every element of K is $\widehat{w}$ for some $w \in \Sigma^*$.) □

We need the following lemma, which follows from Ramsey's theorem.

Lemma 6.2. *Consider a k-coloring of the set $\{(i,j)|\ 1 \leq i \leq j\} \subseteq \mathbb{N} \times \mathbb{N}$. Then there is an infinite sequence $\{i_j\}$ with*

$$1 \leq i_1 < i_2 < \cdots$$

such that all (i_j, i_{j+1}) have the same color.

(We note that the full strength of Ramsey's theorem is not required here, as we do not need all (i_j, i_k) with $j < k$ to have the same color. A weaker combinatorial principle, along the lines of the Erdös–Szekeres theorem on the existence of long monotone subsequences of arbitrary sequences, will suffice. See [6], which is the source for the kind of argument that we use in the present section.)

Theorem 6.3. *If L is a language with a neutral letter definable in MON_q, then it is regular and definable in $(FO+MOD_q)[<, \{\pi_\sigma\}_{\sigma\in\Sigma}]$. Furthermore, the syntactic monoid of L is solvable and every group in the syntactic monoid has order dividing a power of q.*

Proof. We let $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_t\}$ and let $\lambda \in \Sigma$ be the neutral letter for L (so that $\lambda = \sigma_i$ for some i).

We extend the notation we used to define the function $\widehat{\ }$: We set $\widehat{(w,i)}$ to be the suffix of length $|w|$ of $\widehat{vw}$, where v is any string of length i. This is independent of the choice of the string v. Note that $\widehat{w} = \widehat{(w,0)}$.

Suppose L is definable by a sentence ϕ in MON_q. Let $K \subseteq (\Sigma \times \{0,1\}^r)^*$ be the regular language whose existence is proved in Lemma 6.1. Let M be its syntactic monoid and let $\mu : (\Sigma \times \{0,1\}^r)^* \to M$ be its syntactic morphism. Furthermore let $X \subseteq M$ be such that $K = \mu^{-1}(X)$.

Let $w = \tau_1\tau_2\ldots\tau_n \in \Sigma^*$ and $|w| = n$. We color (i,j), $1 \leq i < j$, $i,j \in \mathbb{N}$, by $(m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_t})$, where $m_{\sigma_k} = \mu(\sigma_k\lambda^{\widehat{j-i-1}, i}-1) \in M$. By Lemma 6.2, there is a sequence $1 \leq i_1 < i_2 < \cdots < i_{n+1}$ such that (i_j, i_{j+1}), $0 \leq j \leq n$, have the same color. Define

$$\mathrm{pad}(w) = \lambda^{i_1-1}\tau_1\lambda^{i_2-i_1-1}\tau_2\ldots\lambda^{i_n-i_{n-1}-1}\sigma_n\lambda^{i_{n+1}-i_n-1}.$$

Since λ is a neutral letter for L, $w \in L$ iff $\mathrm{pad}(w) \in L$. Observe that

$$\mu(\widehat{\mathrm{pad}(w)}) = m_0 m_{\tau_1} m_{\sigma_2} \cdots m_{\tau_n},$$

where $m_0 = \mu(\widehat{\lambda^{i_1-1}})$. Thus $w \in L$ iff $m_0\nu(w) \in X$, where $\nu : \Sigma^* \to M$ is the homomorphism defined by $\nu(\sigma_i) = m_{\sigma_i}$ for $1 \leq i \leq t$. This implies that there is a set $Y = \{m \in M|\ m_0 m \in X\}$ such that $w \in L$ iff $\nu(w) \in Y \subset M$. Thus L is regular, and its syntactic monoid is a quotient of a submonoid of M, which implies that all the groups in $M(L)$ are solvable and have order dividing a power of q. The conclusion about logical definability of L now follows from the results of [21]. □

7. Directions for further research. In many steps of the algorithm for reducing a sentence defining L_m to an active-domain sentence, we introduced ordinary quantifiers even when the original formula had only modular quantifiers. If there were a way to avoid this, we could also prove, by the same techniques, that the language $0^*1\{0,1\}^*$ cannot be defined by a formula over $(\mathbb{N},+)$ having only modular quantifiers. If addition is replaced by arbitrary numerical predicates, this statement is equivalent to the conjecture that the circuit complexity class CC^0 does not contain the language 1^*. (CC^0 is the class of languages recognized by constant-depth, polynomial-size circuit families in which every gate is a MOD_q gate for a fixed modulus q. See Barrington, Straubing, and Thérien [7].)

One can ask in general for what classes $\mathcal{C}$ of numerical predicates we have that every language in $(FO + MOD_q)[\mathbb{N},\mathcal{C}]$ with a neutral letter is regular and definable using only the ordering in $<$. The question is discussed at length in [5], and in [12] in the more general context of collapse results for embedded finite models. One can investigate whether, as is the case for first-order logic, finite VC-dimension of $(\mathbb{N},\mathcal{C})$ implies the collapse. This would require generalizing the results of Baldwin and Benedikt [1] to modular quantifiers.

But there is a limit to how far we can push this approach. We are really interested in proving our result over a base of arbitrary numerical predicates, or at the very least over the base $\{+,\times\}$. However, with $\{+,\times\}$, one can express all problems in the arithmetic hierarchy (section 4 in [5]). Specifically, it is possible in this logic to define the set of infinite strings with an even number of 1's in first-order logic without using modular quantifiers! Let $E(x)$ be the numerical predicate "the binary expansion of x contains an even number of 1's," and $B(x,y)$ the predicate "bit y in the binary expansion of x is 1." Then the set of infinite bit strings with an even number of 1's is defined by

$$\exists x(E(x) \wedge \forall y(\pi(y) \leftrightarrow B(x,y))).$$

Both E and B are definable over $(+,\times)$. This shows that we cannot extend the collapse arguments to these richer logics. It also shows (since we know, from circuit complexity, that first-order sentences cannot define PARITY for *finite* strings) that there are important differences between finite and infinite strings as regards definability.

One possible approach to formulas with more general numerical predicates is to try to prove some version of the collapse results for sentences interpreted in finite strings that are known to define regular languages. We do know, for example, thanks to the circuit lower bounds, that regular languages definable by first-order sentences with arbitrary numerical predicates are all definable in $FO[<,\{\equiv_s\colon s>1\}]$, and the same holds even when we add modular quantifiers of fixed prime modulus, so we do indeed have a collapse result, although this has never been proved directly by model-theoretic means (see [3] and [20]).

Acknowledgments. We acknowledge helpful discussions with Klaus-Jörn Lange, Denis Thérien, David Mix Barrington, and the late Clemens Lautemann. We also thank Andreas Krebs for pointing out to us that our original proofs of Lemmas 5.1 and 5.2 were unnecessarily long and complicated, and for supplying the simpler arguments given here.

REFERENCES

[1] J. Baldwin and M. Benedikt, *Stability theory, permutations of indiscernibles and embedded finite models*, Trans. Amer. Math. Soc., 352 (2000), pp. 4937–4969.

[2] D. M. Barrington, *Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1*, J. Comput. System Sci., 38 (1989), pp. 150–164.

[3] D. M. Barrington, K. Compton, H. Straubing, and D. Thérien, *Regular languages in NC^1*, J. Comput. System Sci., 44 (1992), pp. 478–499.

[4] D. M. Barrington, N. Immerman, and H. Straubing, *On uniformity in NC^1*, J. Comput. System Sci., 41 (1990), pp. 274–306.

[5] D. M. Barrington, N. Immerman, C. Lautemann, N. Schweikardt, and D. Thérien, *First-order expressibility of languages with neutral letters or the Crane Beach conjecture*, J. Comput. System Sci., 70 (2005), pp. 101–127.

[6] D. M. Barrington and H. Straubing, *Superlinear lower bounds for bounded-width branching programs*, J. Comput. System Sci., 50 (1995), pp. 374–381.

[7] D. M. Barrington, H. Straubing, and D. Thérien, *Nonuniform automata over groups*, Inform. and Comput., 89 (1990), pp. 109–132.

[8] D. M. Barrington and D. Thérien, *Finite monoids and the fine structure of NC^1*, J. ACM, 35 (1988), pp. 941–952.

[9] C. Behle and K.-J. Lange, *$FO[<]$-uniformity*, in Proceedings of the IEEE Conference on Computational Complexity, 2006, pp. 183–189.

[10] M. Benedikt and L. Libkin, *Relational queries over interpreted structures*, J. ACM, 47 (2000), pp. 644–680.

[11] A. Krebs, K.-J. Lange, and S. Reifferscheid, *Characterizing TC^0 in terms of infinite groups*, in Proceedings of the 22nd International Symposium on Theoretical Aspects of Computer Science (STACS'05), Lecture Notes in Comput. Sci. 3404, Springer, Berlin, 2005, pp. 496–507.

[12] L. Libkin, *Embedded finite models and constraint databases*, in Finite Model Theory and Its Applications, E. Grädel et al., eds., Springer, New York, 2005.

[13] L. Libkin, *Elements of Finite Model Theory*, Springer, New York, 2004.

[14] J. F. Lynch, *On sets of relations definable by addition*, J. Symbolic Logic, 47 (1982), pp. 659–668.

[15] J. Nurmonen, *Counting modulo quantifiers on finite structures*, Inform. and Comput., 160 (2000), pp. 183–207.

[16] M. Presburger, *Ueber die Vollstaendigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, in Comptes Rendus du I congrès de Mathématiciens des Pays Slaves, Warsaw, Poland, 1929, pp. 92–101.

[17] A. A. Razborov, *Lower bounds for the size of circuits of bounded depth with basis* $\{\wedge, \oplus\}$, Math. Notes Soviet Acad. Sci., 41 (1987), pp. 333–338.

[18] N. Schweikardt, *Arithmetic, first-order logic, and counting quantifiers*, ACM Trans. Comput. Log., 6 (2005), pp. 634–671.

[19] R. Smolensky, *Algebraic methods in the theory of lower bounds for Boolean circuit complexity*, in Proceedings of the 19th ACM Symposium on Theory of Computing (STOC), 1987, pp. 77–82.

[20] H. Straubing, *Finite Automata, Formal Logic and Circuit Complexity*, Birkhäuser, Boston, 1994.

[21] H. Straubing, D. Thérien, and W. Thomas, *Regular languages defined with generalized quantifiers*, Inform. and Comput., 118 (1995), pp. 289–301.