hexagon:2611.01185v1

Arrow's Theorem in Elementary Arithmetic

Santiago Calderón Rodríguez

Abstract

We prove the finite version of Arrow's theorem in $I\Delta_0 + \exp$ for weak individual and social preferences. The combinatorial argument uses a finite primeness principle: if a disjoint union of coalitions is winning, one of its parts is winning. The first winning prefix therefore produces a winning singleton. A separate profile argument shows that this voter controls strict social comparisons even when other voters are indifferent. All auxiliary profiles use at most three ranks. We give an explicit arithmetization, construct these profiles by bounded binary comprehension, and justify the bounded search for the first winning prefix. Profiles and welfare tables are coded below 2^{nm^2} and $2^{m^2 2^{nm^2}}$, respectively. For the full-domain finite arithmetization specified here, the result establishes the elementary arithmetic upper bound proposed in Eastaugh's Conjecture 4.6.

2020 Mathematics Subject Classification. Primary 03F30; Secondary 91B14, 03B30.
Key words and phrases. Arrow's theorem, elementary arithmetic, bounded induction, weak orders, reverse mathematics.

1 Introduction

The finite impossibility theorem of Arrow is classical; for conventional finite proofs, see Geanakoplos [3] and Fey [2]. The contribution here concerns its arithmetic upper bound, with weak preferences and the bounds required for a uniform arithmetization made explicit.

Eastaugh proves Arrow's theorem in RCA_0 and obtains its first-order finite formulation in primitive recursive arithmetic by conservativity [1, Theorem 4.5 and the following discussion]. He formulates the following conjecture:

> "The first-order formalisation of Arrow's theorem is provable in $\mathrm{I}\Delta_0 + \exp$."

This is Conjecture 4.6 of the same paper. We establish its finite arithmetical content for the explicit arithmetical sentence θ_{A} defined in Section 4.1.

The proof has two parts. First, we give an ordinary finite social-choice argument. Its central observation is that winning coalitions satisfy enough of a primeness condition to force a winning singleton. The full algebra of ultrafilters is unnecessary for this finite step. Second, we show that the argument is available in elementary arithmetic. The required profiles have bounded numerical codes, and the search predicate for the first winning prefix is itself bounded, although it quantifies over every valid profile.

The distinction matters. Finiteness alone does not identify an admissible induction formula, and exponential bounds on the final sentence alone do not establish its provability in elementary arithmetic. We supply the profile constructions and the induction matrices that make the argument uniform in the numbers of voters and alternatives. A tie-preserving construction is essential: an argument on strict input orders would not establish the full weak-preference theorem.

We use EA for the functional presentation of $I\Delta_0 + \exp$ with a symbol $E(x) = 2^x$ and induction for bounded formulas in that language. The presentation is recalled in Section 4. Our main result is

$$\mathsf{EA} \vdash \theta_{\mathrm{A}}.$$

The conventional graph translation gives the corresponding statement in $I\Delta_0 + \exp$. The proof of the combinatorial theorem is in Sections 2–3; its arithmetical realization is established in Section 4. Arithmetic details used in binary coding are collected in Appendix A.

2 Finite primeness and social choice

Write $[r] = \{i : i < r\}$ for a finite ordinal. Let $V = [n]$, $n > 0$, be the voters and $X = [m]$, $m \geq 3$, the alternatives. A weak order R on X is a reflexive, transitive, total binary relation. The notation aRb means that a is ranked at least as highly as b. Write $a \succ_R b$ for $aRb \wedge \neg bRa$, and $a \sim_R b$ for $aRb \wedge bRa$. Let $\mathcal{W}(X)$ be the weak orders on X. A profile is $P = (R_i^P)_{i<n} \in \mathcal{W}(X)^V$.

A social welfare function has the full domain $F : \mathcal{W}(X)^V \to \mathcal{W}(X)$. It satisfies *Pareto* if

$$(\forall i < n \; a \succ_{R_i^P} b) \quad \Longrightarrow \quad a \succ_{F(P)} b.$$

It satisfies *independence of irrelevant alternatives* (IIA) if, whenever P, Q agree at every voter on both directed comparisons of a, b, the orders $F(P), F(Q)$ also agree on both comparisons. A voter $d < n$ is a *dictator* if

$$\forall P \in \mathcal{W}(X)^V \; \forall a, b \in X \quad a \succ_{R_d^P} b \implies a \succ_{F(P)} b.$$

Dictatorship in this sense permits the social order to refine the dictator's indifferences. The same voter must work for all profiles and pairs.

Lemma 2.1 (Strict comparisons in a weak order)**.** *The strict part of a weak order is irreflexive and transitive. It also satisfies*

$$c \succ_R b \quad \Longrightarrow \quad c \succ_R a \;\vee\; a \succ_R b. \tag{1}$$

Proof. Irreflexivity follows from the two contradictory conjuncts of $a \succ_R a$. If $a \succ_R b$ and $b \succ_R c$, transitivity gives aRc. Were cRa, it would give cRb, contrary to $b \succ_R c$. Thus $a \succ_R c$. For (1), suppose $\neg(c \succ_R a)$. Totality implies aRc: otherwise cRa together with $\neg aRc$ would imply $c \succ_R a$. Hence aRb by transitivity. If bRa, then bRc, contrary to $c \succ_R b$. This proves $a \succ_R b$. □

The finite principle used below requires very little structure on a family of coalitions.

Lemma 2.2 (The first winning prefix)**.** *Let $\mathcal{U}$ be a family of subsets of $[n]$ such that $[n] \in \mathcal{U}$, $\varnothing \notin \mathcal{U}$, and*

$$C \cap D = \varnothing, \quad C \cup D \in \mathcal{U} \quad \Longrightarrow \quad C \in \mathcal{U} \;\vee\; D \in \mathcal{U}.$$

Then $\{d\} \in \mathcal{U}$ for some $d < n$.

Proof. Put $C_k = \{i < n : i < k\}$ for $k \leq n$. Let $k \leq n$ be the least index with $C_k \in \mathcal{U}$. It exists because $C_n = [n]$. Since $C_0 = \varnothing$, write $k = d+1$ with $d < n$. The union $C_{d+1} = C_d \dot{\cup} \{d\}$ is disjoint, so one of its parts belongs to $\mathcal{U}$. Minimality rules out C_d, leaving $\{d\} \in \mathcal{U}$. □

No upward closure, intersection closure, or monotonicity of the prefix membership pattern was used. In the arithmetic application, the family $\mathcal{U}$ will be notation for a bounded predicate, rather than a set whose existence must first be proved. The least-index step will be justified by a bounded induction in Lemma 4.3.

3 Winning coalitions

Fix a full-domain social welfare function F satisfying Pareto and IIA. For $C \subseteq V$ and distinct $a, b \in X$, a profile is *polarized by C on (a, b)* if voters in C strictly prefer a to b and voters outside C strictly prefer b to a. Write $\mathrm{Win}(C; a, b)$ if $a \succ_{F(P)} b$ in every such profile. This is almost decisiveness on the pair. In contrast, strong decisiveness allows arbitrary preferences outside C; that conclusion is proved in Lemma 3.4.

Every displayed three-alternative order $a \succ b \succ c$ below is realized by ranks $2, 1, 0$, respectively, with all unlisted alternatives at rank 0. A relation defined by comparing ranks is a weak order: reflexivity, transitivity and totality follow from the corresponding comparisons of the ranks. A profile specified separately on voter regions is therefore a legitimate member of the unrestricted domain. We will also use the rank assignment $(2, 1, 1)$ to realize a top alternative above an indifferent pair. All constructions consequently have at most three ranks. The profile to which strong transfer is applied remains arbitrary; this restriction concerns only the newly constructed auxiliary profiles.

3.1 Pair independence of winning

Lemma 3.1 (A polarized witness)**.** *If a profile P is polarized by C on (a, b) and $a \succ_{F(P)} b$, then* $\mathrm{Win}(C; a, b)$.

Proof. For any other profile Q with that polarization, the two directed comparison bits at each voter are $(1, 0)$ in C and $(0, 1)$ outside C, in both P and Q. IIA equates both social bits, so $a \succ_{F(Q)} b$. □

Lemma 3.2 (Expansion of the winning pair)**.** *If* $\mathrm{Win}(C; a, b)$ *for one distinct pair, then* $\mathrm{Win}(C; x, y)$ *for every distinct $x, y \in X$.*

Proof. First let a, b, c be distinct and assume $\mathrm{Win}(C; a, b)$. Construct profiles with the following ranks, displayed in descending order:

	C	$V \setminus C$
P	$a \succ b \succ c$	$b \succ c \succ a$
Q	$c \succ a \succ b$	$b \succ c \succ a$

In P, winning gives $a \succ_{F(P)} b$, while Pareto gives $b \succ_{F(P)} c$. Strict transitivity gives $a \succ_{F(P)} c$. The profile is also polarized by C on (a, c), so Lemma 3.1 gives $\mathrm{Win}(C; a, c)$. In Q, winning gives $a \succ_{F(Q)} b$ and Pareto gives $c \succ_{F(Q)} a$. Hence $c \succ_{F(Q)} b$ and $\mathrm{Win}(C; c, b)$. We have thus proved the two operations

$$(a, b) \longmapsto (a, c), \qquad (a, b) \longmapsto (c, b) \quad (a, b, c \text{ distinct})$$

on winning pairs.

Using a third alternative c, these operations give $(a, b) \mapsto (a, c) \mapsto (b, c) \mapsto (b, a)$. For an arbitrary target (x, y), if $x = b$ start from the reverse pair (b, a): use it directly if $y = a$, and otherwise change its second endpoint to y. The latter triple is distinct because $y \neq a, b$. If $x \neq b$, obtain (x, b) directly when $x = a$, and by changing the first endpoint of (a, b) when $x \neq a$. If $y = b$ this is the target; otherwise change the second endpoint of (x, b) to y. Here x, b, y are distinct. This exhausts the equality cases and proves the assertion without induction on $|X|$. □

Fix the pair $(0, 1)$ and write $\mathrm{Win}(C)$ for $\mathrm{Win}(C; 0, 1)$. The lemma shows that the choice of distinct reference pair is immaterial.

3.2 Primeness and arbitrary profiles

Lemma 3.3 (Disjoint-union primeness)**.** *For disjoint coalitions C, D,*

$$\mathrm{Win}(C \cup D) \quad \Longrightarrow \quad \mathrm{Win}(C) \ \vee \ \mathrm{Win}(D).$$

Proof. Choose distinct a, b, c. By Lemma 3.2, the hypothesis gives $\mathrm{Win}(C \cup D; c, b)$. Construct

C	D	$V \setminus (C \cup D)$
$a \succ c \succ b$	$c \succ b \succ a$	$b \succ a \succ c.$

The disjointness makes these three regions a partition. The profile is polarized by $C \cup D$ on (c, b), so its social order has $c \succ b$. Lemma 2.1 gives $c \succ a$ or $a \succ b$ socially. In the first case the profile is polarized by D on (c, a), so Lemma 3.1 and pair expansion give $\mathrm{Win}(D)$. In the second case it is polarized by C on (a, b), giving $\mathrm{Win}(C)$. □

Lemma 3.4 (Strong transfer, including indifference)**.** *If $\mathrm{Win}(C)$, then for every profile P and distinct $x, y \in X$,*

$$(\forall i \in C \ x \succ_{R_i^P} y) \quad \Longrightarrow \quad x \succ_{F(P)} y.$$

Proof. Choose z distinct from x, y. Construct a profile Q as follows. In C put $x \succ z \succ y$. Outside C, put z above x, y and retain the original weak comparison of x, y. More explicitly, for each voter outside C, use the ranks

comparison in P	$\rho(z)$	$\rho(x)$	$\rho(y)$
$x \succ y$	2	1	0
$y \succ x$	2	0	1
$x \sim y$	2	1	1

and give all unlisted alternatives rank 0. Totality in P makes the table exhaustive. Each assigned relation is a weak order.

The profile Q is polarized by C on (x, z). Pair expansion and winning yield $x \succ_{F(Q)} z$. Every voter in Q strictly prefers z to y, so Pareto gives $z \succ_{F(Q)} y$. Thus $x \succ_{F(Q)} y$. For voters in C, the comparison of x, y in both P and Q is $(1, 0)$ by hypothesis. For voters outside C, both directed bits are preserved by the table, including $(1, 1)$ when they are indifferent. IIA therefore transfers the strict social comparison to P. □

Theorem 3.5 (Finite Arrow)**.** *For $n > 0$ and $m \geq 3$, every full-domain social welfare function on weak orders satisfying Pareto and IIA has a dictator.*

Proof. The full coalition wins by Pareto. The empty coalition does not win: in a profile where everyone strictly prefers 1 to 0, Pareto gives that social comparison, whereas winning by the empty coalition on $(0, 1)$ would give the opposite strict comparison. Such a profile exists, for example by assigning ranks 2 to 1, 1 to 0, and 0 to all others. By Lemmas 2.2 and 3.3, some singleton $\{d\}$ wins. If d strictly prefers x to y in any profile, then $x \neq y$ and Lemma 3.4 with $C = \{d\}$ gives the same strict social comparison. This is dictatorship, with the one voter d independent of the profile and alternatives. □

4 Realization in elementary arithmetic

We now give a uniform arithmetic proof of the finite theorem. No quantification over a set of coalitions or a space of functions is needed in this part: all data are numbers, and coalition notation abbreviates bounded formulas.

4.1 The theory and the arithmetic sentence

Our language is $0, S, +, \cdot, E, <, =$. The basic axioms are those of Robinson arithmetic, the defining equation $s < t \leftrightarrow \exists u\ t = s + Su$, and

$$E(0) = 1, \qquad E(Sx) = E(x) + E(x).$$

We allow induction with parameters for every formula built using only term-bounded quantifiers $\forall x < t$, $\exists x < t$, where t does not contain x. Terms may contain E. This is the usual functional presentation of elementary arithmetic. Its conservative relation to $I\Delta_0 + \exp$ is stated, with attribution to Kaye, in Pollett [4, Section 2, Theorem 6]. Eliminating E means using its total, uniquely defined arithmetical graph. Consequently the provability claim for an E-formula means the corresponding graph-translated claim in the language without that function symbol. The arithmetic proofs below use exactly bounded induction in the stated functional language.

Put

$$w = m^2, \quad L = nw, \quad B = E(L), \quad H = wB, \quad T = E(H). \tag{2}$$

Define

$$\mathrm{Bit}(s, j) \ \equiv\ \exists q < s + 1\ \exists r < E(j)\ [s = qE(j + 1) + E(j) + r]. \tag{3}$$

The indices of profile and social bits are

$$\iota(i, a, b) = (im + a)m + b, \qquad \tau(p, a, b) = wp + am + b.$$

Write

$$R_i^p(a, b) \equiv \mathrm{Bit}(p, \iota(i, a, b)), \qquad S_p^f(a, b) \equiv \mathrm{Bit}(f, \tau(p, a, b)).$$

Their strict parts are denoted $a \succ_i^p b$ and $a \succ_p^f b$. Every quantifier in the following definitions has its displayed finite bound:

$$\begin{aligned}
\mathrm{Good}(p) \equiv\ & [\forall i < n \forall a < m\ R_i^p(a, a)] \\
& \wedge [\forall i < n \forall a, b, c < m\ ((R_i^p(a, b) \wedge R_i^p(b, c)) \to R_i^p(a, c))] \\
& \wedge [\forall i < n \forall a, b < m\ (R_i^p(a, b) \vee R_i^p(b, a))], \\
\mathrm{SocialGood}(f, p) \equiv\ & [\forall a < m\ S_p^f(a, a)] \\
& \wedge [\forall a, b, c < m\ ((S_p^f(a, b) \wedge S_p^f(b, c)) \to S_p^f(a, c))] \\
& \wedge [\forall a, b < m\ (S_p^f(a, b) \vee S_p^f(b, a))], \\
\mathrm{TableGood}(f) \equiv\ & \forall p < B\ (\mathrm{Good}(p) \to \mathrm{SocialGood}(f, p)), \\
\mathrm{Pareto}(f) \equiv\ & \forall p < B\ [\mathrm{Good}(p) \to \forall a, b < m\ ((\forall i < n\ a \succ_i^p b) \to a \succ_p^f b)].
\end{aligned}$$

For IIA put

$$\mathrm{Same}(p, q, a, b) \equiv \forall i < n\ [(R_i^p(a, b) \leftrightarrow R_i^q(a, b)) \wedge (R_i^p(b, a) \leftrightarrow R_i^q(b, a))]$$

and

$$\begin{aligned}
\mathrm{IIA}(f) \equiv \forall p < B \forall q < B\ [(\mathrm{Good}(p) \wedge \mathrm{Good}(q)) \to \forall a, b < m [\mathrm{Same}(p, q, a, b) \to \\
((S_p^f(a, b) \leftrightarrow S_q^f(a, b)) \wedge (S_p^f(b, a) \leftrightarrow S_q^f(b, a)))]].
\end{aligned}$$

Finally set

$$\mathrm{Dict}(f, d) \equiv \forall p < B\ [\mathrm{Good}(p) \to \forall a, b < m\ (a \succ_d^p b \to a \succ_p^f b)].$$

The dependence on n, m is suppressed. The sentence to be proved is

$$\theta_{\mathrm{A}} \equiv \forall n \forall m \forall f\ [(0 < n \wedge 3 \leq m \wedge f < T \wedge \mathrm{TableGood}(f) \wedge \mathrm{Pareto}(f) \wedge \mathrm{IIA}(f)) \longrightarrow \exists d < n\ \mathrm{Dict}(f, d)]. \tag{4}$$

Here $s \leq t$ abbreviates $s < St$. Its matrix is $\Delta_0(E)$. The bound on the full table includes all binary input codes, whether or not they encode valid profiles; only valid profiles are constrained.

4.2 Binary comprehension and profile codes

The arithmetic facts needed for the next proof are established in Appendix A. In particular, they are derived using the bounded induction matrices given there.

Lemma 4.1 (Bounded binary comprehension)**.** *For each fixed bounded formula $A(j, \bar{u})$, elementary arithmetic proves*

$$\forall \ell\ \exists q < E(\ell)\ \forall j < \ell\ (\mathrm{Bit}(q, j) \leftrightarrow A(j, \bar{u})).$$

Proof. Induct on ℓ in the bounded matrix after the leading universal quantifier. For $\ell = 0$ choose $q = 0 < E(0) = 1$. Given $q < E(\ell)$ representing the first ℓ bits, distinguish $A(\ell)$ from its negation. If $A(\ell)$, use $q' = q + E(\ell)$. Lemma A.2 gives the correct bit at ℓ, preserves every bit below ℓ, and gives $q' < E(\ell + 1)$. If $\neg A(\ell)$, keep $q' = q$; its bit at ℓ is false and exponential growth gives the new bound. For each $j < \ell + 1$, the discrete-order split $j < \ell$ or $j = \ell$ verifies the required equivalence. The induction matrix quantifies only over $q < E(\ell)$ and $j < \ell$, with A bounded. No second-order comprehension principle is involved. □

Lemma 4.2 (Rectangle coding)**.** *Elementary arithmetic proves, for $i < n$ and $a, b < m$,*

$$am + b < w, \qquad \iota(i, a, b) < L, \qquad p < B \to \tau(p, a, b) < H.$$

The profile index is injective on triples with $a, b < m$. For every fixed bounded formula $Q(i, a, b)$ there is a code $p < B$ such that

$$\forall i < n \forall a, b < m \quad R_i^p(a, b) \leftrightarrow Q(i, a, b).$$

Proof. The quotient comparison in Lemma A.1 gives $am + b < m^2$ from $a < m, b < m$. It also gives $im + a < nm$ from $i < n, a < m$, and then $(im + a)m + b < (nm)m = nm^2$. Apply it to $p < B$ and $am + b < w$ to obtain $pw + (am + b) < Bw = wB$. These are the stated bounds. If two profile indices agree, division uniqueness with divisor m first equates their final remainders b, b' and their quotients $im + a, i'm + a'$. A second application equates a, a' and i, i'.

Apply Lemma 4.1 at length L to

$$A(j) \equiv \exists i < n \exists a < m \exists b < m\ [j = \iota(i, a, b) \wedge Q(i, a, b)].$$

At $j = \iota(i, a, b)$, injectivity identifies every witnessing triple with i, a, b, proving $A(j) \to Q(i, a, b)$. Conversely the same triple witnesses $A(j)$ when $Q(i, a, b)$ holds. Compose these equivalences with the bit equivalence from binary comprehension. □

4.3 A common three-rank construction

We now realize every auxiliary profile used in the combinatorial proof without an enumeration of the weak orders. Let $H(i,t), M(i,t)$ be bounded formulas with disjoint truth sets for each voter. They specify the top and middle ranks. The bottom rank consists of the remaining alternatives. The corresponding weak comparison is the bounded formula

$$Q(i,a,b) \equiv H(i,a) \ \vee \ [M(i,a) \wedge \neg H(i,b)] \ \vee \ [\neg H(i,b) \wedge \neg M(i,b)]. \tag{5}$$

When H, M are disjoint, this is comparison of ranks $2, 1, 0$. Explicitly, a top-ranked alternative is at least as high as every alternative; a middle one is at least as high as exactly the non-top ones; and a bottom one is at least as high as exactly the bottom ones. This gives reflexivity and totality. If aQb and bQc, the rank of a is at least that of b and that of b at least that of c; the three possible ranks give aQc. This is a fixed finite case argument about Boolean formulas, independent of n, m. Rectangle coding therefore supplies a valid profile code $p < B$.

All required instances can now be written explicitly. For an order $a \succ b \succ c$, take $H(i,t) \equiv t = a$ and $M(i,t) \equiv t = b$. Selecting such orders on a bounded voter region $C(i)$ uses

$$H = (C \wedge H_0) \vee (\neg C \wedge H_1), \qquad M = (C \wedge M_0) \vee (\neg C \wedge M_1).$$

The two region-specific pairs of flags are disjoint, and hence so are H, M. The expansion profiles use this selection twice, with the orders displayed in Lemma 3.2. For the disjoint-union profile use the three regions C, $\neg C \wedge D$, $\neg C \wedge \neg D$, with top and middle alternatives (a,c), (c,b) and (b,a), respectively. Disjointness of C, D identifies the middle region with D. The reverse-unanimity profile in Theorem 3.5 uses $H(i,t) \equiv t = 1$, $M(i,t) \equiv t = 0$.

For the strong-transfer profile of Lemma 3.4, fix the original code p and distinct x, y, z. Put $u_i = R_i^p(x,y)$ and $v_i = R_i^p(y,x)$ as formulas, and use

$$\begin{aligned} H(i,t) &\equiv (C(i) \wedge t = x) \vee (\neg C(i) \wedge t = z), \\ M(i,t) &\equiv (C(i) \wedge t = z) \\ &\qquad \vee [\neg C(i) \wedge ((t = x \wedge u_i) \vee (t = y \wedge v_i))]. \end{aligned}$$

The three alternatives are distinct, so H, M are disjoint. Inside C their ranks are $x : 2, z : 1, y : 0$. Outside C, totality in the original valid profile gives $u_i \vee v_i$, and the three cases yield exactly the rank table in Lemma 3.4. Thus both weak comparison bits are preserved outside C, including indifference, and the new code is valid. All these flags are bounded combinations of equality, coalition formulas, and the bounded bit formula (3).

When a third alternative is required, it can be chosen from $0, 1, 2$ by fixed equality cases: if $x = 0$, use 1 unless $y = 1$, then use 2; if $x \neq 0$ and $y \neq 0$, use 0; if $x \neq 0$ and $y = 0$, use 1 unless $x = 1$, then use 2. Each selected numeral is $< m$ and distinct from x, y. There is no induction over alternatives in this selection.

4.4 The bounded search and the main result

Lemma 4.3 (Bounded least element)**.** *For every fixed bounded formula $P(k)$ and term b, elementary arithmetic proves*

$$(\exists k < b \ P(k)) \ \longrightarrow \ \exists k < b \ [P(k) \wedge \forall j < k \ \neg P(j)].$$

Proof. Keep the parameters fixed and put $M(k) \equiv P(k) \wedge \forall j < k \neg P(j)$. Induct on t in the bounded formula

$$A(t) \equiv (\exists k < t \ P(k)) \to \exists k < t \ M(k).$$

At zero its antecedent is false. For the step, suppose $A(t)$ and $\exists k < t+1\ P(k)$. If $\exists k < t\ P(k)$, apply $A(t)$ and retain the resulting minimal witness under the larger bound $t+1$. Otherwise every $j < t$ fails P. A witness $k < t+1$ for P must equal t, by the successor split; hence $P(t)$ and $M(t)$, so use $t < t+1$ as the witness. This proves $A(t+1)$. Instantiating the universal induction conclusion at b proves the claim. No monotonicity of P is assumed. □

For a bounded coalition predicate $C(i)$ define

$$\mathrm{Pol}(C, p, a, b) \equiv \forall i < n\ [(C(i) \to a \succ_i^p b) \wedge (\neg C(i) \to b \succ_i^p a)],$$
$$\mathrm{Win}(C; a, b) \equiv \forall p < B\ [(\mathrm{Good}(p) \wedge \mathrm{Pol}(C, p, a, b)) \to a \succ_p^f b].$$

These are bounded formulas. In particular,

$$P(k) \equiv \mathrm{Win}(\{i < n : i < k\}; 0, 1) \tag{6}$$

is bounded, with n, m, f as parameters. The apparent quantification over all profiles in the combinatorial proof is precisely the bounded quantifier $\forall p < B$ in this formula.

Theorem 4.4. *Elementary arithmetic proves* θ_{A}.

Proof. Take arbitrary numerical parameters n, m, f and assume the antecedent of (4). Discreteness gives $0, 1, 2 < m$, and the successor axioms make these numerals distinct. Use the bounded bit relations above as the individual and social weak orders. Their weak-order properties follow from Good and TableGood, and the two remaining assumptions provide exactly the bounded instances of Pareto and IIA.

The proof of Lemma 3.1 is a first-order deduction on the two directed comparison bits. The expansion, primeness, and strong-transfer lemmas use the bounded profiles constructed in Section 4.3, each with a witness $< B$ and the required validity and comparison properties. Every quantifier over voters, alternatives and profiles is therefore bounded by n, m, B. In these applications the coalition predicates are built from $i < k$, $i = d$, and Boolean combinations of those formulas; no set of winning coalitions is constructed.

Pareto gives $P(n)$ and the reverse-unanimity profile gives $\neg P(0)$. Apply Lemma 4.3 to (6) with bound $n+1$. The witness n shows that the bounded set searched is nonempty. Let $k < n+1$ be its least member. Since $\neg P(0)$, the predecessor axiom yields $k = d+1$. The bounds imply $d < n$, and minimality gives $\neg P(d)$ because $d < d+1 = k$.

The discrete-order identity $i < d+1 \leftrightarrow (i < d \vee i = d)$ identifies the prefix coalition as the disjoint union $C_{d+1} = C_d \dot\cup \{d\}$. Primeness and $P(d+1)$ give $P(d) \vee \mathrm{Win}(\{d\}; 0, 1)$. The first disjunct is impossible, so the singleton wins. For any $p < B$ satisfying $\mathrm{Good}(p)$ and any $x, y < m$ with $x \succ_d^p y$, we have $x \neq y$. Apply strong transfer to the singleton to obtain $x \succ_p^f y$. Bounded universal introduction over p, x, y gives $\mathrm{Dict}(f, d)$, with $d < n$.

This proves the bounded existential conclusion of (4). Discharge its antecedent and universally quantify f, m, n. The only inductions beyond the coding arithmetic are the bounded binary comprehension induction and the bounded least-element induction displayed above. Thus the argument is a proof in the specified theory EA. □

The proof strengthens the PRA upper bound for this sentence because it replaces an existence argument about an entire family of coalitions by a bounded search on one list of prefixes. The witnesses for the auxiliary profiles lie below B, while the fixed input table lies below T. The induction formula may inspect all these profiles without leaving $\Delta_0(E)$. This accounts for the arithmetic strength of the proof; the relative size of the finite domains alone would not do so.

5 Correspondence with the finite formulation

We explain why (4) is the full finite assertion, rather than a restricted-domain version. In ordinary finite mathematics, every profile has a code $p < B$: apply binary comprehension on the L positions to its comparison matrix. The index is injective, and the transferred weak-order axioms give $\mathrm{Good}(p)$. Conversely every valid code defines such a profile.

Every full-domain social welfare function has a table $f < T$. For each valid $p < B$, place the weak comparison bits of its social value in block p of length w, and put zeros in invalid blocks. The table positions are below H, so binary comprehension on H bits gives $f < T$. It satisfies exactly the displayed predicates whenever the function satisfies the corresponding social conditions. Conversely, a table satisfying these predicates defines a social welfare function: choose the least valid representative code of each profile. If two codes represent the same profile, IIA equates their two social bits on every pair, so the social value is independent of this choice. The dictatorial conclusion transfers by the same bit equivalences. This finite interpretation is distinct from the proof inside arithmetic, where all inputs are numerical tables and binary comprehension is invoked only for fixed bounded formulas.

Eastaugh's finite formulation uses weak orders, unrestricted domain, strict unanimity and strict dictatorship [1, Theorem 1.1]. The same conditions occur here. Explicit reflexivity is redundant in the presence of his strong connectedness convention. Relabelling finite sets by $[n], [m]$ preserves all these conditions. The indexed presentation in his Definitions 3.3–3.5 also causes no finite domain loss: an atomic algebra on a finite voter set contains every subset by finite unions of singletons. The voter classes assigned each weak order are therefore coalitions. Quasi-partition embedding, applied to those classes, supplies each finite profile. Repeated indices for a profile have the same social value by IIA on every pair. Thus they factor through the finite table presentation above.

The first-order sentence in Eastaugh's discussion is specified through finite coding, rather than a unique fully expanded formula. Equation (4) supplies such a coding with all weak profiles included. Theorem 4.4 therefore proves the finite arithmetical content of Conjecture 4.6 in the conventional elementary theory. No claim about the weakest theory proving the result is needed for this conclusion.

A Arithmetic for bounded binary coding

We give the coding arithmetic in the language used above. All parameters in an induction are fixed. Write $1 = S0$ and $s \le t$ for $s < St$.

A.1 Elementary algebra and order

The Robinson axioms used are

$$Sx \neq 0, \qquad Sx = Sy \to x = y, \qquad x \neq 0 \to \exists y\ x = Sy,$$

$$x + 0 = x, \qquad x + Sy = S(x + y), \qquad x0 = 0, \qquad x(Sy) = xy + x.$$

Here and below multiplication is also written by juxtaposition. The required semiring identities follow by quantifier-free induction. For $0 + x = x$, the zero case is an axiom, and the step is $0 + Sx = S(0 + x) = Sx$. For $(s + t) + x = s + (t + x)$ the zero case reduces both sides to $s + t$; the step takes the successor of both sides of the induction hypothesis. For $(Ss) + x = S(s + x)$, the zero case follows from addition by zero; the step reduces both sides to $SS(s + x)$. Commutativity is proved from the zero case $s + 0 = 0 + s$ and $s + Sx = S(s + x) = S(x + s) = (Sx) + s$.

For additive cancellation induct on x in $(s + x = t + x) \to s = t$. At zero reduce the additions by zero; at Sx, successor injectivity reduces the premise to $s + x = t + x$. Commutativity gives cancellation of a common left summand.

The identity $(Ss)x = sx + x$ has zero base case. For the step, the recursion axiom and the induction hypothesis give

$$(Ss)(Sx) = (sx + x) + Ss = (sx + s) + Sx = s(Sx) + Sx,$$

using the additive identities just proved. Induction gives $0x = 0$, since $0(Sx) = 0x + 0$. For $s(t + x) = st + sx$ the zero case reduces to $st = st + 0$; the successor step reduces both sides to $st + (sx + s)$. Commutativity of multiplication follows from the zero case and $s(Sx) = sx + s = xs + s = (Sx)s$. This gives distributivity on the other side as well. For $(st)x = s(tx)$ the zero case has both sides zero; the successor step expands both sides to $s(tx) + st$. Finally $s1 = s0 + s = s$.

Expand $s < t$ as $t = s + Su$. Then no element is below zero, since $s + Su = S(s + u) \neq 0$, and $s < Ss$ is witnessed by $u = 0$. From $s < St$ one obtains $t = s + u$ by successor injectivity. If $u = 0$ this gives $s = t$; otherwise writing $u = Sv$ gives $s < t$. This is the successor split. The same expansion, separating $u = 0$ from $u \neq 0$, gives $s < t \to (Ss < t \vee Ss = t)$ and $s < t \to Ss < St$. If $t = s + Su$ and $v = t + Sz$, then $v = s + S(Su + z)$, proving transitivity. A loop $s < s$ would yield $s + 0 = s + Su$ and hence $0 = Su$ by cancellation.

For totality induct on x in the quantifier-free formula $s < x \vee x < Ss$. The zero case uses $0 < Ss$. If $s < x$, then $s < Sx$ by transitivity. Otherwise $x < Ss$; the successor split gives $x < s$ or $x = s$. In the first case $Sx < Ss$, and in the second $s < Sx$. This proves the induction step. A further successor split gives trichotomy. The characterization $s \leq t \leftrightarrow \exists u\ t = s + u$ follows by expanding $s < St$ and cancelling successors. Its witnesses compose by addition, proving transitivity of $\leq$; the comparison just proved gives its totality.

Positive differences also prove the needed monotonicity facts directly. If $t = s + Su$, then $t + v = (s + v) + Su$ and $t + v = s + S(u + v)$, so $s < t$ implies both $s + v < t + v$ and $s < t + v$. An equation $s + v < s$ would, after expansion and cancellation, equate zero with a successor, and is impossible. The positive-difference definition of order can itself be bounded: if $t = s + Su = u + Ss$, then $u < t$. Hence $s < t \leftrightarrow \exists u < t\ t = s + Su$. Keeping $<$ as a primitive relation therefore introduces no stronger class of induction matrices when compared with its bounded definition.

Lemma A.1 (Division and quotient comparison)**.** *For $b \neq 0$ and each x, elementary arithmetic proves unique division*

$$\exists q < x + 1\ \exists r < b \quad x = qb + r.$$

If $q < q'$ and $r < b$, then $qb + r < q'b + r'$ for every r'. Whenever $b \neq 0$ and $x = qb + r$, one has $q < x + 1$.

Proof. For existence induct on x in the displayed bounded formula, with b fixed. At zero use $q = r = 0$; the predecessor axiom for $b \neq 0$ gives $0 < b$. Given $x = qb + r$, either $Sr < b$ or $Sr = b$. In the first case use q, Sr for Sx; its quotient bound is widened from $q < Sx$ to $q < SSx$. In the second case use $Sq, 0$, since $Sx = qb + Sr = qb + b = (Sq)b$ and $Sq < SSx$ follows from the induction bound. These cases exhaust $r < b$ by discreteness.

If $q < q'$, write $q' = q + Su$. Distributivity gives $q'b + r' = qb + b + (ub + r')$. From $r < b$ obtain $qb + r < qb + b$, and then $qb + r < qb + b + (ub + r')$. Thus two divisions of the same x cannot have distinct quotients, by trichotomy. Equal quotients give equal remainders by cancellation. For the last assertion, write $b = Su$. Then $x = q + (qu + r)$, which witnesses $q < Sx$ in the definition of $<$. □

A.2 Exponential and bit arithmetic

Elementary arithmetic proves $E(x) \neq 0$ by quantifier-free induction. The base is $E(0) = 1 \neq 0$. For the step, write $E(x) = Su$; then $E(Sx) = E(x) + Su = S(E(x) + u) \neq 0$. Induction on t in the atomic formula $E(s + t) = E(s)E(t)$ proves the exponential sum law. At zero use $E(0) = 1$; the step uses

$$E(s + St) = 2E(s + t) = 2E(s)E(t) = E(s)E(St),$$

where $2v$ denotes $v + v$ and distributivity justifies the equalities. Positivity gives $E(x) < E(Sx) = E(x) + E(x)$. Induction on t in $\forall j < t\ E(j) < E(t)$ proves strict monotonicity: its base is empty, and at St split $j < St$ into $j < t$ and $j = t$, using growth in both cases and the induction hypothesis in the first.

Lemma A.2 (Bit laws)**.** *For the formula* (3)*, elementary arithmetic proves*

$$\begin{aligned} s < E(j) &\to \neg\,\mathrm{Bit}(s, j), \\ s < E(j) &\to [\mathrm{Bit}(s + E(j), j) \wedge s + E(j) < E(j + 1)], \\ \mathrm{Bit}(s + E(j + 1)t, j) &\leftrightarrow \mathrm{Bit}(s, j), \\ j < k &\to [\mathrm{Bit}(s + E(k), j) \leftrightarrow \mathrm{Bit}(s, j)]. \end{aligned}$$

Proof. Put $A = E(j)$ and $D = E(j + 1) = A + A$. A bit witness writes $s = qD + A + r \geq A$, excluding $s < A$. If $s < A$, the witnesses $q = 0, r = s$ give $\mathrm{Bit}(s+A, j)$, and $s+A < A+A = D$ supplies its bound.

For periodicity, a witness q, r for $\mathrm{Bit}(s, j)$ becomes $q + t, r$ for $\mathrm{Bit}(s + Dt, j)$. The quotient bound required by the bit formula follows from the last assertion of Lemma A.1. Conversely divide $s = q_0D + r_0$, with $r_0 < D$. Then $s + Dt = (q_0 + t)D + r_0$. A bit witness also writes this number as $q_1D + (A + r_1)$, where $r_1 < A$ and $A + r_1 < D$. Division uniqueness gives $r_0 = A + r_1$. Hence $s = q_0D + A + r_1$, a bit witness whose quotient again has the necessary bound. Finally, if $j < k$, write $k = Sj + u$ using its positive difference. The sum law gives $E(k) = E(Sj)E(u)$, so periodicity with $t = E(u)$ proves preservation of the bit at j. □

For clarity, the complete list of induction matrices used in the arithmetic construction is recorded below. The parameters s, t, b and all formula parameters remain fixed. The first twelve rows are quantifier-free.

Induction matrix in x	Purpose
$0 + x = x$	Additive zero
$(s + t) + x = s + (t + x)$	Additive associativity
$(Ss) + x = S(s + x)$	Left successor
$s + x = x + s$	Additive commutativity
$(s + x = t + x) \to s = t$	Cancellation
$(Ss)x = sx + x$	Left multiplicative successor
$0x = 0$	Multiplicative zero
$s(t + x) = st + sx$	Distributivity
$sx = xs$	Multiplicative commutativity
$(st)x = s(tx)$	Multiplicative associativity
$s < x \vee x < Ss$	Order comparison
$E(x) \neq 0$	Exponential nonzeroness
$E(s + x) = E(s)E(x)$	Exponential sum law; atomic
$\forall j < x\ E(j) < E(x)$	Exponential monotonicity
$\exists q < Sx \exists r < b\ x = qb + r$	Division, assuming $b \neq 0$
$\exists q < E(x) \forall j < x(\mathrm{Bit}(q, j) \leftrightarrow A(j))$	Binary comprehension, A bounded
$(\exists k < x\ P(k)) \to \exists k < x[P(k) \wedge \forall j < k \neg P(j)]$	Least element, P bounded

Substitution, Boolean combinations and term-bounded quantifiers preserve boundedness. Expanding Bit adds only the two bounded existential quantifiers in (3). Thus every matrix in the table belongs to $\Delta_0(E)$, including the least-element matrix when P is the universal-over-profile predicate (6). The universal closures of these induction conclusions are ordinary logical generalizations, not induction on unbounded matrices.

The explicit representation bounds are as follows. A profile has L bits and a code $< B = E(L)$; a welfare table has H bits and a code $< T = E(H)$. For an input bit at $j < L$, its remainder bound $E(j)$ is $< B$ and its quotient bound is $s + 1$ with $s < B$. For an output bit at $j < H$, the corresponding bounds are $E(j) < T$ and $s + 1$ with $s < T$. These are legitimate fixed-depth exponential terms. The argument introduces no variable-height iteration of exponentiation and no induction with an unbounded matrix.

Use of generative AI

Generative AI (ChatGPT) was used to assist with the mathematical development, drafting, bibliographic research, and internal review of this manuscript.

References

[1] Benedict Eastaugh (2025). *Arrow's theorem, ultrafilters, and reverse mathematics*. The Review of Symbolic Logic 18(2), 439–462. Published online 29 February 2024; arXiv:2306.06471v2, 24 April 2024. https://doi.org/10.1017/S1755020324000054. https://arxiv.org/abs/2306.06471v2.

[2] Mark Fey (2014). *A straightforward proof of Arrow's theorem*. Economics Bulletin 34(3), 1792–1797. https://www.accessecon.com/Pubs/EB/2014/Volume34/EB-14-V34-I3-P164.pdf.

[3] John Geanakoplos (2005). *Three brief proofs of Arrow's impossibility theorem*. Economic Theory 26(1), 211–215. https://doi.org/10.1007/s00199-004-0556-7.

[4] Chris Pollett (2000). *Translating $I\Delta_0 + \exp$ proofs into weaker systems*. Mathematical Logic Quarterly 46(2), 249–256. https://doi.org/10.1002/(SICI)1521-3870(200005)46:2<249::AID-MALQ249>3.0.CO;2-R. Author version dated 20 February 2003, Section 2, Theorem 6: https://www.cs.sjsu.edu/faculty/pollett/papers/inter2.pdf.