# Introduction to model-theoretic methods for proofs of bounded generation

Dave Witte Morris

University of Lethbridge, Alberta, Canada
http://people.uleth.ca/~dave.morris
Dave.Morris@uleth.ca

**Abstract.** These expository talks will describe three classical methods from the model theory of first-order logic, and describe situations in which they can be used to show that every element of a group is the product of the same number of elements of a given generating set. (For example, the methods sometimes show there is some $C$, such that every element of the commutator subgroup is the product of $C$ commutators.) The methods are: the Compactness Theorem, ultraproducts, and nonstandard analysis.



## Introduction

### Lemma (undergraduate Linear Algebra)

*$n \times n$ matrix $T$ is invertible $\Leftrightarrow$ $T \rightsquigarrow \mathrm{Id}$ by elementary row ops*
*$\Leftrightarrow$ $T$ is a product of elementary matrices.*
(*True over any field.*)

### Corollary (from first-order logic)

*For fixed $n$, can use same # of row ops for every $n \times n$ matrix.*
*I.e., $\exists C$, every $n \times n$ invertible matrix (over any field) is the product of $C$ elementary matrices.*

**Exer.** Look at a proof of the lemma, and find some $C$, such that row reducing the matrix only takes $C$ operations.

But the exercise is unnecessary:
Logic tells us that $C$ exists, without having to do extra work.



### Notation

Let $S$ be a subset of a group $G$.

- $\langle S \rangle$ = subgroup generated by $S$
  $= \{ s_1 s_2 \cdots s_k \mid s_i \in S^{\pm 1},\ k \in \mathbb{N} \}$
- $\langle S \rangle_r = \{ s_1 s_2 \cdots s_k \mid s_i \in S^{\pm 1},\ k \le r \}$

### Definition

- $S$ generates $G$ if $\langle S \rangle = G$
- $S$ boundedly generates $G$ if $\langle S \rangle_r = G$ for some $r \in \mathbb{N}$

### Example

Group $\mathrm{GL}(n,F)$ of invertible $n \times n$ matrices is boundedly generated by the set of elementary matrices
(for all $n \in \mathbb{N}$ and every field $F$).



### Notation

$n \in \mathbb{N}$, $F$ field. $\quad \mathrm{SL}(n,F) = \{ T \in \mathrm{GL}(n,F) \mid \det T = 1 \}$

### Theorem (graduate Group Theory)

*$F$ infinite $\Rightarrow$ $G = \mathrm{SL}(n,F)$ is simple (modulo scalar matrices)*
*If $N$ is a proper, normal subgroup of $G$, then $N \subseteq F^{\times} \cdot \mathrm{Id}$.*

I.e., if $T \in \mathrm{SL}(n,F)$, and $T \notin F^{\times} \cdot \mathrm{Id}$, then
$\langle$conjugates $P^{-1}TP$ of $T\rangle = \mathrm{SL}(n,F)$.

### Corollary (first-order logic)

*Conjugates of $T$ boundedly generate $\mathrm{SL}(n,F)$.*

*Exer.* Examine pf of the thm and find bound $C$ on # conjugates.
Will be a lot of work!

Logic tells us that $C$ exists, without having to do extra work.



### First-order logic: bound exists (without additional work)

If certain types of conditions imply that
a function $f: A \to \mathbb{N}$ exists on all of $A$,
(# row operations needed, # conjugates needed, ...)
Then $f$ must be a bounded function: $f(a) \le C$ for all $a \in A$.

(We do not need to know how to prove the theorem.)

We will see how to prove bounded generation using:

- Compactness Theorem
- Ultraproducts
- Nonstandard analysis



## First-order logic

The only quantifiers are $\forall x$ and $\exists x$ (or also $\forall x \in y$ and $\exists x \in y$).

**You cannot write "$\forall x \subseteq A$" in a first-order sentence.**

Quantifiers range over the *elements* of the univ of discourse $\mathbb{U}$,
so $\forall x$ or $\exists x$ cannot assign a subset of $\mathbb{U}$ to the variable $x$ unless that subset happens to be an element of $\mathbb{U}$.

Second-order logics (and other higher-order logics) allow you to write sentences about *all* subsets of the universe of discourse.

**Definition**

A (first-order) *language* is a (finite or infinite) set $\mathcal{L}$ of:

- constant symbols $c_1, c_2, \ldots$,
- function symbols $f_1, f_2, \ldots$ ($k_i$-ary),
- relation symbols $R_1, R_2, \ldots$ ($k_i$-ary).

Also have:

- $=$ and $\in$,
- logical connectives: &, $\vee$ (or), $\Rightarrow$, $\Leftrightarrow$ and $\neg$ (not)
- variables $(x_1, x_2, \ldots)$,
- (bounded) quantifiers: $\forall x$, $\exists x$, $\forall x \in y$, $\exists x \in y$.

**Example**

- group theory: constant symbol 1 and binary operator $*$
- field theory: constants 0 and 1 and binary ops $+$ and $\times$

These suffice to write all of the axioms

- of group theory (e.g., $\forall x, \exists y,\ xy = 1$)
- or field theory (e.g., $\forall x, y, z, \quad x \cdot (y + z) = x \cdot y + x \cdot z$).



**Exercise**

*Write first-order sentence $\psi_r$ that says $n \times n$ matrix $[c_{i,j}]$ is in:*

1. $\langle$*elementary matrices*$\rangle_r$
2. $\langle$*conjugates of* $[a_{ij}]\rangle_r$

**Compactness Theorem of first-order logic**

Assume $\Phi$ and $\Psi$ are sets of first-order axioms, such that
for all structures that satisfy all of the axioms in $\Phi$,
at least one of the assertions in $\Psi$ is also true.
Then $\Psi$ can be replaced with a finite subset $\Psi_0$.

**Exercise**

*Finiteness cannot be expressed by first-order axioms:*
*If first-order axioms imply that a set is finite, then* $\exists C$,
*such that the axioms imply the cardinality of the set is* $\leq C$.

If a set of first-order axioms is satisfied by arbitrarily large finite structures, then it is satisfied by an infinite structure.



**Example**

$\mathrm{GL}(n, F)$ is boundedly generated by the set of elementary matrices (for all $n \in \mathbb{N}$ and every field $F$).

**Proof.**

- $\Phi = \{\text{field axioms}\} \cup \{[c_{ij}] \text{ is } n \times n \text{ invertible matrix}\}$.
- $\psi_r$: $\quad [c_{ij}] \in \langle \text{elem mats} \rangle_r$.

Linear Algebra: some $\psi_r$ is true.

Compactness Theorem: $\exists C$, some $\psi_{\leq C}$ is true.
(And $C$ does not depend on $F$, but does depend on $n$.) □



## Ultraproducts

**Remark**

Elementary matrices boundedly generate $\mathrm{GL}(n, F)$
$\Leftrightarrow$ elementary matrices generate $\mathrm{GL}(n, \times_{i=1}^{\infty} F)$

**Proof.**

$$\mathrm{GL}(n, \times_{i=1}^{\infty} F) \cong \times_{i=1}^{\infty} \mathrm{GL}(n, F).$$

$T_k \neq$ product of $k$ elem mats in $\mathrm{GL}(n, F)$,
$\Rightarrow (T_k)_{k=1}^{\infty} \neq$ prod of any # of elem mats in $\times_{i=1}^{\infty} \mathrm{GL}(n, F)$. □

Bounded generation $\rightsquigarrow$ ordinary generation
— but over a terrible ring (with lots of zero divisors).
Ultraproducts make the same reduction, but over a field.



**Definition**

A *nonprincipal ultrafilter* ($\mathcal{U}$ or $\mu$) on $\mathbb{N}$ is a finitely additive, $\{0,1\}$-valued measure on $I$ that has no atoms.

- Every set has measure 0 or 1,
- finite sets have measure 0, and
- the whole space ($\mathbb{N}$) has measure 1.

Axiom of Choice (Zorn's Lemma) implies:

**Proposition**

*There is a nonprincipal ultrafilter $\mathcal{U}$ on $\mathbb{N}$ (or any infinite set).*



**Definition**

Let $A_1, A_2, \ldots$ be a sequence of sets.

- Equivalence relation on $\prod_{i=1}^{\infty} A_i$:
  $(a_i)_{i=1}^{\infty} \sim (b_i)_{i=1}^{\infty} \iff a_i = b_i$ a.e.
  E.g., $a_i = b_i$ for all large $i$ (finite sets have measure 0)
- Ultraproduct: $\prod_{\mathcal{U}} A_i = \left(\prod_{i=1}^{\infty} A_i\right)/\sim$.

**Theorem**

*Suppose $\varphi(x, y)$ is a first-order formula and $a, b \in \prod_{\mathcal{U}} A_i$.*
*(So $a = (a_i)_{i=1}^{\infty}$ and $b = (b_i)_{i=1}^{\infty}$.)*
*Then $\varphi(a, b)$ is true in $\prod_{\mathcal{U}} A_i$*
$\iff$ *$\varphi(a_i, b_i)$ is true for a.e. $i$.*

**Example**

- $\varphi(x,y): x = y$ (definition of ultraproduct)
- General $\varphi$: proved by ind'n with $x = y$ as the base case.
- $\prod_{\mathcal{U}} G_i$ is abelian $\Leftrightarrow$ a.e. $G_i$ is abelian.
- $\prod_{\mathcal{U}} F_i$ is a field $\Leftrightarrow$ a.e. $F_i$ is a field.

**Example**

$\prod_{\mathcal{U}} \mathbb{Z}$ is an integral domain: $\forall x,y,\ xy = 0 \Rightarrow (x = 0 \vee y = 0)$.

**Proof.**

$xy = 0 \Rightarrow x_i y_i = 0$ a.e.
Let $X = \{\, i \mid x_i = 0 \}$ and $Y = \{\, j \mid y_j = 0 \,\}$.
Then $\mu(X) + \mu(Y) \geq \mu(X \cup Y) = \mu(\{ i \mid x_i y_i = 0\}) = 1 > 0 + 0$.
So $\mu(X)$ and $\mu(Y)$ cannot both be 0 — one must be 1.
Either $x_i = 0$ a.e. or $y_i = 0$ a.e.
I.e., either $x = 0$ or $y = 0$. □



**Exer.** Elem mats generate $\mathrm{GL}(n, \prod_{\mathcal{U}} F)$ (because $\prod_{\mathcal{U}} F$ is a field)
$\Rightarrow$ elementary matrices boundedly generate $\mathrm{GL}(n,F)$.

I.e., $\exists r,\ \mathrm{GL}(n,F) = \langle \text{elem mats} \rangle_r$ (product of $\leq i$ el'ts)

**Proof.**

Suppose not. Then $\exists T_i \notin \langle \text{elementary matrices} \rangle_i$.
Then $(T_i)_{i=1}^{\infty} \in \prod_{\mathcal{U}} \mathrm{GL}(n,F) \cong \mathrm{GL}(n, \prod_{\mathcal{U}} F)$.
But $(T_i)_{i \in \mathbb{N}} \notin \langle \text{elementary matrices} \rangle$
$(T_i)_{i \in \mathbb{N}} = A_1 A_2 \cdots A_r$
$\Rightarrow T_i = (A_1)_i (A_2)_i \cdots (A_r)_i \in \langle \text{elem mats} \rangle_r$.
and $\prod_{\mathcal{U}} F$ is a field (since the field axioms are first-order).
This is a contradiction. □

**Exer.** Use ultraproducts to prove the Compactness Theorem.

Therefore, anything that can be proved with the Compactness Theorem can also be proved with ultraproducts.



## Nonstandard analysis ("infinitesimals")

**Basic idea**

1. Fix a universe of discourse $\mathbb{U}$. E.g.
   - all grps, their el'ts, and the homos between them, or
   - all fields, all vector spaces, and all linear transformations.
2. For each $X \in \mathbb{U}$, associate "nonstandard model" ${}^*X \supseteq X$.
   - For a set $X$, let ${}^*X = \prod_{\mathcal{U}} X$.
   - For an individual $a$, let ${}^*a = a = (a,a,a,\ldots) \in {}^*A$.

**Example**

${}^*\mathbb{Z} = \prod_{\mathcal{U}} \mathbb{Z} = \{\, (n_1, n_2, n_3, \ldots) \mid n_i \in \mathbb{Z} \,\}$ contains:

- $1 = (1,1,1,\ldots)$,
- $2 = (2,2,2,\ldots) = 1 + 1$ $\qquad \mathbb{Z} \subsetneq {}^*\mathbb{Z}$
- $n = (n,n,n,\ldots)$
- $\omega = (1,2,3,\ldots) > n$ for all $n \in \mathbb{Z}$ ("infinitely large")
- $\omega^2 = (1^2, 2^2, 3^2, \ldots) > \omega$



${}^*\mathbb{Z}$ contains infinite numbers, but acts much like $\mathbb{Z}$:

- integral domain: $\forall x,y,\ xy = 0 \Rightarrow (x = 0 \vee y = 0)$.
- Division Algorithm:
  $\forall n, k \neq 0,\ \exists! q, r,\ (n = kq + r\ \ \&\ \ 0 \leq r < |k|)$.
- 2 el'ts have gcd:
  $\forall a,b,\ \exists m,n,\ ma + nb$ divides both $a$ and $b$
- Any first-order property.

But ${}^*\mathbb{Z}$ is not Euclidean domain (or PID or Noetherian or UFD).
(E.g., $p^k \mid (1, p, p^2, p^3, p^4, \ldots)$ for all $k \in \mathbb{N}$.)
(*Exer.* Every finitely generated ideal is principal.)

**Exercise**

*${}^*\mathbb{R}$ contains infinitely large $\omega$, and infinitesimal $\epsilon$*
$(\forall r \in \mathbb{R}^+, 0 < \epsilon < r)$.

Original motivation for nonstandard analysis [A. Robinson] was to make infinitesimals a legitimate foundation of Calculus.



**Theorem (Transfer principle)**

*A first-order assertion $\varphi$ is true in $X$*
*$\Leftrightarrow$ its $*$-transform is true in ${}^*X$.* ("Transfer principle")
*(Replace each constant symbol $c$ in $\varphi$ with ${}^*c$.)*

**Example**

Suppose $A, B \subseteq \mathbb{Z}$, such that $\forall a \in A, \exists b \in B, a^2 = b^3$.
Transfer principle: $\forall a \in {}^*A, \exists b \in {}^*B, a^2 = b^3$.

**Example**

Suppose $F$ is a field.
Then ${}^*F$ is a field (because field axioms are first order).
Therefore $\mathrm{SL}(n, {}^*F)$ is generated by elementary matrices.
$\therefore$ $\mathrm{SL}(n,F)$ is boundedly generated by elementary matrices.



**Proof.**

Recall: $\langle \text{elem mats} \rangle_r = \{\text{prod of } \leq r \text{ elem mats}\}$.
So $\mathrm{SL}(n, {}^*F) = \bigcup_{r \in \mathbb{N}} \langle \text{elem mats} \rangle_r \subseteq \langle \text{elem mats} \rangle_\omega$.
Obvious: $r < s \Rightarrow \langle \text{elem mats} \rangle_r \subseteq \langle \text{elem mats} \rangle_s$.
$\therefore$ $\mathrm{SL}(n, {}^*F)$ satisfies $\exists r \in {}^*\mathbb{N}, \forall x,\ x \in \langle \text{elem mats} \rangle_r$.
Transfer principle:
$\mathrm{SL}(n,F)$ satisfies $\exists r \in \mathbb{N}, \forall x,\ x \in \langle \text{elem mats} \rangle_r$. □

**Exercise**

*Suppose $S$ is a subset of a group $G$.*
*Show the following are equivalent:*

1. *$S$ boundedly generates $\langle S \rangle$.*
2. $\langle {}^*S \rangle = {}^*\langle S \rangle$.
3. $|{}^*\langle S \rangle : \langle {}^*S \rangle|$ *is finite (or $*$-finite).*

**Example (D. Carter, G. Keller, and E. Paige)**

Nonstandard analysis provides a simple proof that elementary matrices boundedly generate $\mathrm{SL}(3,\mathbb{Z})$.

**Idea of proof.**

There are (specific) first-order axioms $\Phi$ satisfied by $\mathbb{Z}$, such that if $R$ is a ring satisfying these axioms, then elementary matrices generate $\mathrm{SL}(3,R)$. □

The methods have also yielded new results:

**Corollary (D. Carter, G. Keller, and E. Paige)**

*Let $T$ be a noncentral matrix in $\mathrm{SL}(3,\mathbb{Z})$. Then the conjugates of $T$ boundedly generate a finite-index, normal subgroup.*



**Proof.**

**Theorem** (from 1960s). *Suppose*

- *$R$ is commutative ring with stable range condition $\mathrm{SR}_2$, and*
- *$N$ is a normal subgroup of $\mathrm{SL}(3,R)$ (not in center).*

*Then $\exists$ ideal $\mathcal{I}$ of $R$, such that $N$ contains*

$E(\mathcal{I}) := \{$*elem mats that are* $\equiv \mathrm{Id} \pmod{\mathcal{I}}\}$

$= \{$*elem mats*$\} \cap \mathrm{SL}(3,\mathbb{Z};\mathcal{I})$.

$S = \{\text{conjs of } T\}$. $N = \langle {}^*S \rangle = \langle \text{conjs of } T \text{ in } \mathrm{SL}(3, {}^*\mathbb{Z}) \rangle$.

Theorem gives us an ideal $\mathcal{I}$. (We may assume $\mathcal{I}$ is principal.)

Generalization of CKP Example: $\mathrm{SL}(3,{}^*\mathbb{Z};\mathcal{I}) / \langle E(\mathcal{I}) \rangle$ is finite.

Easy: for all $q \in \mathbb{Z}$, $\mathrm{SL}(3,\mathbb{Z}) / \mathrm{SL}(3,\mathbb{Z};q\mathbb{Z})$ is finite.

Transfer Principle: $\mathrm{SL}(3,{}^*\mathbb{Z}) / \mathrm{SL}(3,{}^*\mathbb{Z};\mathcal{I})$ is $*$-finite.

Therefore $\mathrm{SL}(3,{}^*\mathbb{Z}) / \langle E(\mathcal{I}) \rangle$ is $*$-finite.

So $\left| {}^*\langle S \rangle / \langle {}^*S \rangle \right| \le \left| \mathrm{SL}(3,{}^*\mathbb{Z}) / \langle E(\mathcal{I}) \rangle \right|$ is $*$-finite.

$\therefore$ Exercise tells us that $S$ boundedly generates. □



**Remark**

Nonstandard analysis puts every set in our universe inside a "finite" set:

Every $A \in \mathbb{U}$ is contained in a $*$-finite $B \in {}^*\mathbb{U}$:

$\exists n \in {}^*\mathbb{N}$, $\exists f \in {}^*\mathbb{U}$, $f \colon \{0,1,\ldots,n\} \twoheadrightarrow B$.

For this theorem, need to take ultraproduct with large index set, instead of $\mathbb{N}$.



## Further reading

**First-order logic and the Compactness Theorem**

See almost any textbook on mathematical logic, or:

J. Barwise,
An introduction to first-order logic, pp. 5–46
in *Handbook of Mathematical Logic.*
North-Holland Publishing Co., New York, 1977.
ISBN: 0-7204-2285-X, MR0457132

**Ultraproducts**

See almost any textbook on model theory, or:

P. C. Eklof,
Ultraproducts for algebraists, pp. 105–137
in *Handbook of Mathematical Logic.*
North-Holland Publishing Co., New York, 1977.
ISBN: 0-7204-2285-X, MR0457132



**Nonstandard analysis**

Several textbooks are available, such as:

M. Davis:
*Applied Nonstandard Analysis.*
Wiley-Interscience, New York, 1977.
ISBN: 0-471-19897-8, MR0505473

P. A. Loeb and M. Wolff, eds.:
*Nonstandard Analysis for the Working Mathematician.*
Kluwer, Dordrecht, 2000.
ISBN: 0-7923-6340-X, MR1790871



**Application to bounded generation of matrix groups**

D. Carter, G. Keller, and E. Paige:
Bounded expressions in $\mathrm{SL}(n,A)$,
unpublished (c. 1985).

D. W. Morris:
Bounded generation of $\mathrm{SL}(n,A)$
(after D. Carter, G. Keller, and E. Paige).
*New York J. Math.* 13 (2007), 383–421. MR2357719
`http://nyjm.albany.edu/j/2007/13_383.html`