On the Complexity of Some Problems on Groups Input as Multiplication Tables

David Mix Barrington Amherst
Peter Kadau Tübingen
Klaus-Jörn Lange Tübingen
Pierre McKenzie Montréal

Depth $\log\log n$ was missing

David Mix Barrington $\boxed{\text{Amherst}}$
Peter Kadau $\boxed{\text{Tübingen}}$
Klaus-Jörn Lange $\boxed{\text{Tübingen}}$
Pierre McKenzie $\boxed{\text{Montréal}}$

A neat trick (with applications)

David Mix Barrington $\boxed{\text{Amherst}}$

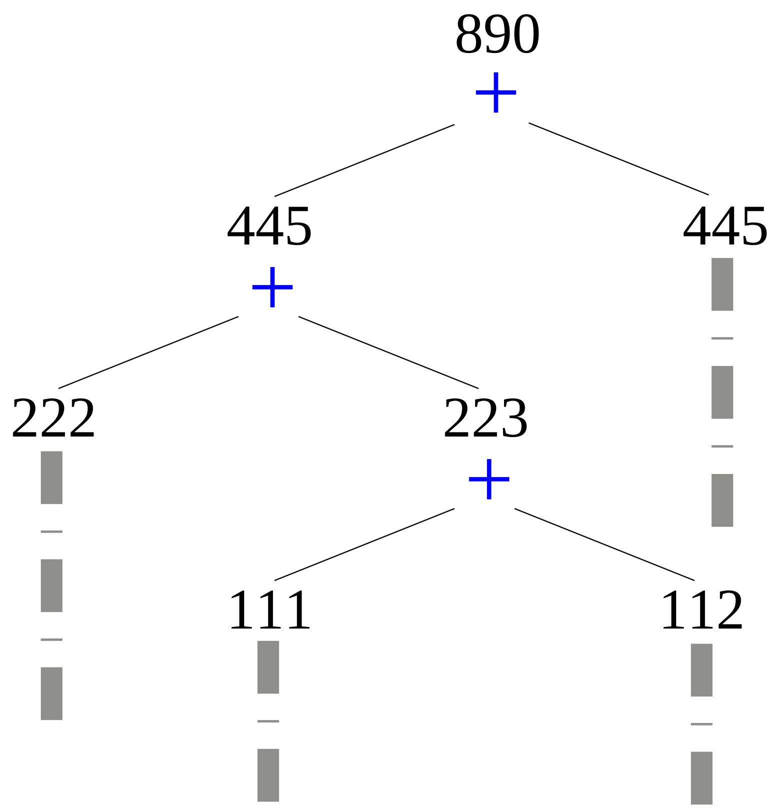
Peter Kadau $\boxed{\text{Tübingen}}$

Klaus-Jörn Lange $\boxed{\text{Tübingen}}$

Pierre McKenzie $\boxed{\text{Montréal}}$

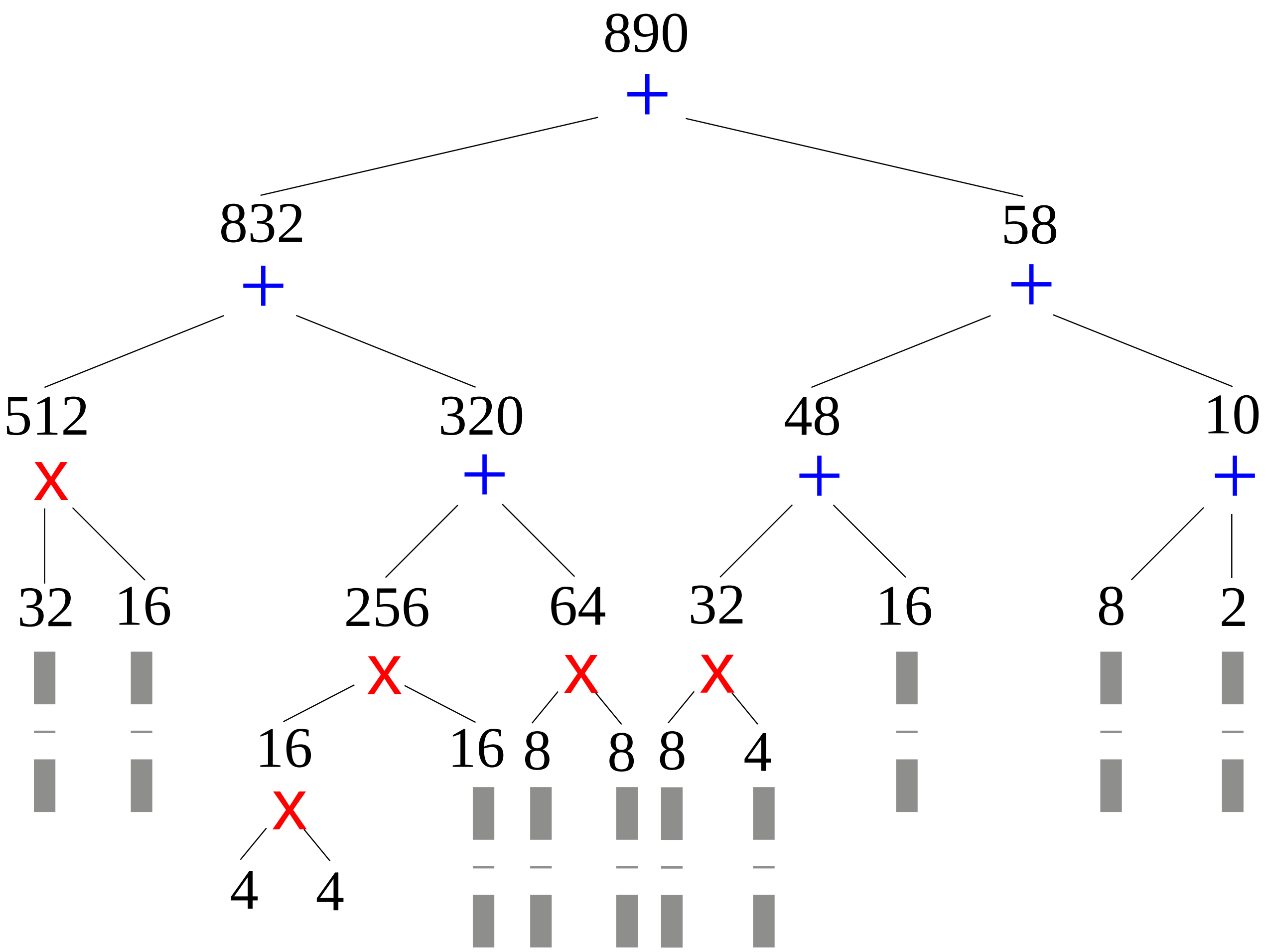
Warmup

How deep is a formula expressing n as a sum of ones?



Of course, any "+"-formula requires $\Omega(\log n)$ depth.

How deep is a "$+, \times$"-formula expressing n?



Fact: $O(\log\log n)$ depth suffices!

The neat trick

When you can, make use of "$+, \times$"-formulas instead of "$+$"-formulas!

Motivation

Group membership problem

Given: group G, subgroup H, $t \in G$

Decide: is t in H?

Cayley group membership problem (CGM)

Given: G in full as an $n \times n$ table, eg

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	5	4	6	1	3
3	3	4	2	5	6	1
4	4	6	5	1	3	2
5	5	1	6	3	2	4
6	6	3	1	2	4	5

H by generating elements $h_1, \ldots, h_r$

eg $H = \langle 2, 3 \rangle$, $t \in G$

Decide: is $t \in \langle h_1, \ldots, h_r \rangle$, eg do the elements $\{2, 3\}$ generate t?

Why care about CGM?

[JoLa 1977]

P-complete for arbitrary table.

[JoLiLa 1976]

NL-complete for associative table.

[BaMc 1991]

CGM in symmetric L

- graph on $\{1, 2 \ldots n\}$
- edge (i, j) iff $\exists$ generator h of H such that $ih = j$ or $hi = j$
- $t \in H$ iff path$(1, t)$

Is CGM hard for SL?

Is CGM(cyclic) hard for L?

Is CGM(cyclic) hard for NC^1?

Our results

- **CGM**(nilpotent), hence in particular **CGM**(cyclic), are provably not hard for TC^0, NC^1, L or NL.

- **CGM**(abelian), hence in particular **CGM**(cyclic), belongs to a peculiar class which we call **FOLL**.

- other group problems, like testing nilpotency or cyclicity of a table, share the above properties.

- testing $a^i \equiv b \mod m$, for $O(\log n)$-bit numbers, is in **FOLL**; by recent work [ChDaLi 2000, AlBa 2000], this has bearing on the uniformity of TC^0 circuits for integer division.

The road to FOLL

$$\exists x \ \forall y \ [(y \leq x) \wedge P_b\, x]$$

defines a language over an alphabet, say $\{a, b, c\}$, when x and y refer to positions within $w_1 w_2 \ldots w_n$ and $P_b\, x$ says that "b is the letter at position x"

Büchi-**FO**:

- Variables: $x, y, x, x_5, \ldots$
- Logical symbols: $\wedge, \vee, \neg, (,), \ldots$
- Predicates: $<, =, \leq, P_a, P_b, P_c$
- Quantifiers: $\exists, \forall$

Büchi-**FO** $\subset$ regular languages.

Definition of FOLL

FO

Büchi-FO with $+$ and $\times$ predicates

[BaImSt90]: **FO** $=$ AC^0, ie logtime-uniform unbounded fanin circuits of constant depth and poly size.

FO(log n)

FO with up to $O(\log n)$ syntactic iterations of quantifier blocks

[Im89,Im99]: **FO**(log n) $=$ AC^1
$=$ **FO** with predicates defined recursively up to depth $O(\log n)$.

FOLL

defined here as **FO**(log log n).

AC^1

LOGCFL $\cup$ DET

NL

L

parity $\notin$ **FOLL**

NC^1

TC^0

ACC^0

AC^0

Group tables in the FO framework

Recall: variables range over $\{1, 2, \ldots, n\}$

Available predicates:

- $x \cdot y = z$ in G
- h is a generating element of H
- t is the test element

Example. $\forall x : \forall y : \forall z : \exists u : \exists v : \exists w :$

$$x \cdot y = u \quad \wedge \quad u \cdot z = w \quad \wedge$$
$$x \cdot v = w \quad \wedge \quad y \cdot z = v$$

expresses that the table is associative.

Hence:
Testing associativity $\in$ **FO** $= \mathrm{AC}^0$.

NB: testing group properties also **FO**.

The $a = b^i$ predicate
(a recursive definition)

Ordinary variable i, ie $1 \leq i \leq n$.

We have $a = b^i$ if and only if

$$i = 1 \quad \wedge \quad a = b$$

or

$$\exists c : \exists d : \exists j : \exists k : \quad i = j + k \quad \wedge$$
$$a = c \cdot d \quad \wedge \quad c = b^j \quad \wedge \quad d = b^k.$$

Closes in $O(\log n)$ steps.
Hence: If predicate $a \cdot b = c \in$ **FO**, then $a^i = b \in$ **FO**$(\log n) =$ AC^1.

The $a = b^i$ predicate

(a better recursive definition: the trick!)

We also have $a = b^i$ iff

$$i = 1 \quad \wedge \quad a = b$$

or

$$\exists c : \exists d : \exists j : \exists k : \quad i = j + k \quad \wedge$$
$$a = c \cdot d \quad \wedge \quad c = b^j \quad \wedge \quad d = b^k$$

or

$$\exists c : \exists j : \exists k : \quad i = j \times k \quad \wedge$$
$$a = c^j \quad \wedge \quad c = b^k.$$

Closes in $O(\log \log n)$ steps!

Hence: Predicate $a^i = b \in$ **FOLL**.

Consequences for cyclic groups

Testing for cyclicity $\in$ **FOLL**

Proof: cyclic iff $\exists\omega : \forall b : \exists i : b = \omega^i$.

Also in **FOLL**:

- finding such an ω
- computing $\log_\omega g$ for any g
- computing $|\langle g\rangle|$ for any g

CGM(cyclic) $\in$ **FOLL**

Proof: $t \in \langle h_1, \ldots, h_r\rangle$ iff

$\gcd(\log_\omega h_1, \ldots, \log_\omega h_r, n) \mid \log_\omega t$.

Hence: **CGM**(cyclic) is provably not hard for ACC^0.

Also: **CGM**(cyclic) in L.

More general groups

G has the $f(n)$ power basis property iff, whenever $G = \langle g_1, \ldots, g_r \rangle$, each $g \in G$ is expressible as

$$g = g_{i_1}^{j_1} g_{i_2}^{j_2} \cdots g_{i_{f(n)}}^{j_{f(n)}}.$$

Proposition. If a family of groups closed under subgroups has the above property, then **CGM**(family) $\in$ **FO**($\log f$).

Proof: $t \in \langle h_1, \ldots, h_r \rangle$ iff $Q_{\lg f} t$, where $Q_0 x$ is defined as

$$\exists j : \exists k : \quad x = h_j^k$$

and $Q_i x$ is defined as

$$\exists a : \exists b : \quad x = a \cdot b \quad \wedge \quad Q_{i-1} a \quad \wedge \quad Q_{i-1} b.$$

Consequences for abelian groups

Lemma. Abelian groups have the $\lg n$ power basis property.

Proof: any generating set for a group of order n contains a minimal generating set of size $\leq \lg n$.
G abelian $\Rightarrow$ any expression over this minimal set can be rearranged.

Theorem. **CGM**(abelian) $\in$ **FOLL**, hence not hard for ACC^0.

OPEN: Is **CGM**(abelian) in L?

Direct products of p-groups

Known fact: A finite group is nilpotent iff for all primes p, the set of p-elements in G forms a group.

Corollary: Testing nilpotency $\in$ **FOLL**.

Thm: **CGM**(nilpotent)$\in$ **FO**$((\log\log n)^2)$, hence is not hard for ACC^0.

Proof: **CGM** for groups of solvability class $d(n)$ is in $\in$ **FO**$(d(n)\log\log n)$, and nilpotent groups have [Th 1978] $d(n) \leq \log\log n$.

OPEN: Where is **CGM**(solvable)?

Another application: arithmetic

• Chinese Remaindering uses polynomially many $\log n$-bit numbers to break down n-bit computations.

• The multiplicative group of the integers modulo an odd prime power is cyclic.

Let a, b, c, i, m be $O(\log n)$-bit numbers.

Fact: $a \cdot b \equiv c \mod m$ is in **FO**.

Corollary: $a \equiv b^i \mod m$ is in **FOLL**.

[ChDaLi 2000, AlBa 2000]: the only additional numerical predicate required to perform integer division in FO+MAJ (truly uniform TC^0) is $a \equiv b^i \mod m$.

Conclusion

The case for **FOLL**

Groups

- Do all groups have the $(\log n)^d$ power basis property?
- Is **CGM**(nilpotent) in **FOLL**?
- Where are **CGM**(solvable) and **CGM**?

Integer arithmetic: the final frontier

- is $a \equiv b^i \mod m$ in TC^0 for $\log n$-bit numbers?

Other applications

- We can compute the accessibility of slightly larger graphs in **FOLL**.
- What else? What implications?