Solvability in Uniquely Divisible Groups[HLR]

Chris J. Hillar, Lionel Levine and Darren Rhea

MSRI, MIT, UC Berkeley

1 Uniquely Divisible Groups

- A group G is called *uniquely divisible* if for every $B \in G$ and each positive integer m, there exists a unique $X \in G$ such that

$$X^m = B.$$

- Examples:
  - the group of positive units of a real closed field
  - unipotent matrix groups
  - noncommutative power series with unit constant term.
- A *word equation* is an expression of the form

$$w(X, A) = B$$

  where w is a finite word in the alphabet $\{X, A\}$.
- $A, B \in G$ are coefficients, and $X \in G$ is the unknown.

2 Word Equations Solvable By Radicals

- Certain word equations, such as

$$XAXAX = B$$

  have solutions in terms of radicals:

$$X = A^{-1/2}(A^{1/2}BA^{1/2})^{1/3}A^{-1/2}$$

  and are therefore solvable in every uniquely divisible group.

Definition 1. *A word w in the alphabet $\{X, A\}$ is totally decomposable if it is the image of the letter X under a composition of maps of the form*

- $w \mapsto (wA^k)^m w$ *for $m \geq 1$, $k \geq 0$;*
- $w \mapsto wA$*;*
- $w \mapsto Aw$.

Lemma 2.1. *If w is totally decomposable, then the word equation*

$$w(X, A) = B$$

is solvable by radicals in any uniquely divisible group.

3 Conjectured Classification

- We prove that certain equations, such as

$$X^2AX = B$$

  have **no solution in terms of radicals**.
- In fact, we construct uniquely divisible groups in which they have no solution at all.

Conjecture 3.1. *Let w be a finite word in the alphabet $\{X, A\}$. The following are equivalent.*

1. *w is totally decomposable.*
2. *$w(X, A) = B$ has a solution in terms of radicals.*

4 Our Main Result

Theorem. There exists a uniquely divisible group G with the following property: For all finite words w in the alphabet $\{X, A\}$, if the equation

$$P_w(x^2, y^2) = 0$$

has a solution $(x_p, y_p) \in (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ for all but finitely many primes p, then there exist elements $A, B \in G$ for which the word equation

$$w(X, A) = B$$

has no solution $X \in G$.

5 The Word Polynomial

- Given a word

$$w = A^{a_0}XA^{a_1}X \cdots A^{a_{n-1}}X,$$

  we define

$$P_w(x, y) = y^{a_0} + xy^{a_0+a_1} + x^2y^{a_0+a_1+a_2} + \cdots + x^{n-1}y^{a_0+\cdots+a_{n-1}}.$$

- If u and w are words in the alphabet $\{X, A\}$, the composition $u \circ v$ is the word obtained by replacing each occurrence of the letter X in u by the word w.

Lemma 5.1. *(Word Polynomial Of A Composition) Let m, n be respectively the number of letters in w equal to A, X. Then*

$$P_{u \circ w}(x, y) = P_u(x^ny^m, y)P_w(x, y).$$

Lemma 5.2. *(Word Polynomial Arises From Matrix Substitution) Let x, y, z be commuting indeterminates. Then*

$$w\left(\begin{bmatrix} x & z \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} x^ny^m & P_w(x, y)z \\ 0 & 1 \end{bmatrix}.$$

6 Proof Sketch

- The group G is constructed from an infinite collection of pq-groups $G_1, G_2, \ldots$

$$G = \prod_{i=1}^{\infty} G_i \Big/ \bigoplus_{i=1}^{\infty} G_i.$$

- The orders of the G_i are chosen using Dirichlet's theorem on primes in arithmetic progressions so that any prime p divides $\#G_i$ for only finitely many i.
- This gives a uniquely divisible group because of the following simple observation.

Lemma 6.1. *Let G be a finite group of order n. If m and n are relatively prime, then every element of G has a unique m-th root.*

- Using some classical results in number theory (related to the Weil Conjectures) we can convert the main result into an efficiently testable condition.

7 An Effective Condition

Corollary. *If w is a word in the alphabet $\{X, A\}$ beginning with X, and if $P_w(x^2, y^2)$ has a factor $f \in \mathbb{Z}[x, y]$ such that f is irreducible in $\mathbb{C}[x, y]$, then w is not universal.*

- The word $w = X^2AX$ has word polynomial

$$P_w(x^2, y^2) = 1 + x^2 + x^4y^2,$$

  which is irreducible over $\mathbb{C}$. It follows that $X^2AX = B$ is not solvable by radicals.
- In contrast, the word $v = XAXAX$ has

$$P_v(x^2, y^2) = 1 + x^2y^2 + x^4y^4 = (1 + xy + x^2y^2)(1 - xy + x^2y^2).$$

  Each factor on the right side is irreducible over $\mathbb{Z}$ but factors over $\mathbb{C}$.
- v is totally decomposable, so $XAXAX = B$ is solvable by radicals.

8 The End

By showing that the word polynomial P_w has a factor $f \in \mathbb{Z}[x, y]$ which is irreducible over $\mathbb{C}[x, y]$, we obtain certain infinite families of word equations not solvable by radicals.

The following words are not solvable in terms of radicals:

X^nAX^m,	$m, n \geq 1,\ m \neq n$;
$XA^{m+2n}XA^{m+n}XA^mX$,	$m \geq 0, n \geq 1$;
XAX^nAX,	$n \geq 3$;
$X^2(AX)^nX$,	$n \geq 2$.

To our knowledge, these are the first such infinite families known.

References

[HLR] C. Hillar, L. Levine, and D. Rhea. equations solvable by radicals in a uniquely divisible group. *submitted.*