Results on the Equivalence Problem for Finite Groups

Stanley Burris and John Lawrence

Abstract. The equivalence problem for a finite nilpotent group has polynomial time complexity, even when the terms have parameters from the group. The same result holds for the dihedral groups $\mathbf{D}_n$.

The *terms* for groups (in the language $\cdot, ^{-1}, e$) are defined inductively by:

(1) variables are terms
(2) e is a term
(3) t is a term implies t^{-1} is a term
(4) s, t are terms implies $s \cdot t$ is a term.

Given a group $\mathbf{G}$ we define the *polynomials* of $\mathbf{G}$ to be the terms obtained when we add names for the elements of $\mathbf{G}$ to our constant symbols, i.e.,

(1) variables are polynomials
(2) g is a polynomial for g denoting an element of $\mathbf{G}$
(3) p is a polynomial implies p^{-1} is a polynomial
(4) p, q are polynomials implies $p \cdot q$ is a polynomial.

The *term equivalence problem* for a group $\mathbf{G}$ is to determine, for any two terms p, q, if they define the same function on $\mathbf{G}$, i.e., if the identity $p \approx q$ holds on $\mathbf{G}$.

The *polynomial equivalence problem* for a group $\mathbf{G}$ is to determine, for any two polynomials p, q, if they define the same function on $\mathbf{G}$, i.e., if the identity $p \approx q$ holds on $\mathbf{G}$.

One can, of course, define these equivalence problems for any algebra. In Hunt & Stearns [4] (1990) it is proved that the polynomial equivalence problem for a finite nilpotent ring has polynomial time complexity. And Burris & Lawrence [3] (1992) show that for finite nonnilpotent rings the term equivalence problem is co-**NP**-complete.

It is easy to see that for any finite algebra $\mathbf{A}$ both the term and the polynomial equivalence problem are in co-**NP**. So if $\mathbf{P} = \mathbf{NP}$ then both problems for $\mathbf{A}$ have polynomial complexity. However it is widely believed that $\mathbf{P} \neq \mathbf{NP}$.

The classification of the equivalence problem for finite groups is begun in this paper. (The results were announced in [1].) We will show that the polynomial

Date: July 31, 2002.

Key words and phrases: evquivalence problem, finite groups, terms, polynomials, automated theorem proving, computational complexity.

We are grateful to Joel Berman for his comments on a earlier version of this paper. And both authors thank NSERC for funding which has supported this research.

equivalence problem for any finite nilpotent group, or any dihedral group $\mathbf{D}_{2k+1}$, is of polynomial time complexity.

Now we turn to finite nilpotent groups. A group $\mathbf{G} = \langle G, \cdot, ^{-1}, e\rangle$ is *nilpotent* if it satisfies a (left-normed) commutator identity

$$[x_0, \cdots, x_n] \approx e. \tag{1}$$

If $\mathbf{G}$ is nilpotent we say it is *nilpotent class* c if c is the smallest n such that (1) holds.

In the next definition we use $[\,,\,]$ as a binary operation symbol (for the commutator).

Definition 1. The collection PC of *pure commutator polynomials* is defined by:

(1) variables are in PC
(2) g is in PC for g denoting an element of $\mathbf{G}$
(3) p, q are in PC implies $[p, q]$ is in PC.

Definition 2. The *leaf count* function lc on PC is defined by:

- $lc(x) = 1$ for x a variable
- $lc(g) = 1$ for g naming an element of $\mathbf{G}$
- $lc([s, t]) = lc(s) + lc(t)$.

The leaf count function gives the number of leaves when a member of PC is viewed as a binary tree.

Lemma 3. *For $\mathbf{G}$ a nilpotent class c group and for p from PC we have*

(a) $lc(p) = c$ *implies* $\mathbf{G} \models p \cdot z \approx z \cdot p$
for z a variable not appearing in p, and
(b) $lc(p) > c$ *implies* $\mathbf{G} \models p \approx e$.

Proof. This follows from the basic commutator calculus—see Lemma 33.35, p. 86, of H. Neumann [6] (1967). □

Definition 4. Given a polynomial p let $\text{var}(p)$ be the set of variables occurring in p.

Lemma 5. *Let $\mathbf{G}$ be a finite nilpotent class c group and let $p(x_1, \cdots, x_k)$ be a polynomial of $\mathbf{G}$. Let $S_0, \cdots, S_m$ be an ordering of the subsets of $\{1, \cdots, k\}$ of size at most c, and such that $i < j \implies |S_i| \le |S_j|$. For $1 \le i \le k$ we assume $S_i \approx \{x_i\}$. Then one can find, for each S_i, a product γ_i of pure commutator polynomials p_{ij} such that*

(a) $\text{var}(p_{ij}) = \{x_s : s \in S_i\}$, *for all i, j, and*
(b) $\mathbf{G} \models p(x_1, \cdots, x_k) \approx \gamma_0 \cdots \gamma_m$.

Proof. This is our version of Theorem 33.45, p. 89, of H. Neumann [6] (1967). First put $p(x_1, \cdots, x_k)$ into the form $y_1 \cdots y_\ell$ where each y_i is in the set $\{x_1, \cdots, x_k\}$, or is the name of an element of $\mathbf{G}$. Then apply the following group identity

$$x \cdot y \approx y \cdot x \cdot [x, y] \tag{2}$$

to put $y_1 \cdots y_\ell$ in the form $g_0 \cdot {x_1}^{n_1} \cdots {x_k}^{n_k} \cdot s(x_1, \cdots, x_k)$, where $g_0 \in G$ and $s(x_1, \cdots, x_k)$ is a product of pure commutators p, with $lc(p) \leq c$ and $\text{var}(p) \geq 2$ for each such p. Then let $\gamma_0 = g_0$, and let $\gamma_i = {x_i}^{n_i}$ for $1 \leq i \leq k$.

Next apply the identity (2) to $s(x_1, \cdots, x_k)$ to pull the pure commutator terms involving exactly two variables to the left side, with appropriate grouping, to give $\gamma_{k+1}, \cdots, \gamma_{k+\binom{k}{2}}$. Etc. □

Lemma 6. *Let* $\mathbf{G}$ *be a nilpotent class c group, and let* $p(x_1, \cdots, x_k)$ *be a polynomial of* $\mathbf{G}$. *Let* $\gamma_0, \cdots, \gamma_m$ *be as in Lemma 5. Then*

$$\mathbf{G} \models p(x_1, \cdots, x_k) \approx e \qquad \textit{iff} \qquad \mathbf{G} \models \gamma_i \approx e \qquad \textit{for } 0 \leq i \leq m.$$

Proof. ($\Longrightarrow$) From Lemma 5 we know from $\mathbf{G} \models p \approx e$ that $\mathbf{G} \models \gamma_0 \cdots \gamma_m \approx e$. Putting all variables equal to e shows that $\gamma_0 = e$. Then putting all variables except x_i equal to e gives $\mathbf{G} \models \gamma_i \approx e$, for $1 \leq i \leq k$. Thus $\mathbf{G} \models \gamma_{k+1} \cdots \gamma_m \approx e$. Let $\text{var}(\gamma_{k+1}) = \{x_{i_1}, x_{i_2}\}$. Next by putting all variables except x_{i_1}, x_{i_2} equal to e we have $\mathbf{G} \models \gamma_{k+1} \approx e$. Etc.

The converse is obvious using Lemma 5. □

Proposition 7. *Let* $p(x_1, \cdots, x_k)$ *be a polynomial of a nilpotent class c group* $\mathbf{G}$. *Then*

$$\mathbf{G} \models p(x_1, \cdots, x_k) \approx e \qquad \textit{iff} \qquad \mathbf{G} \models p(\sigma x_1, \cdots, \sigma x_k) \approx e$$

for all σ *such that*

(a) $\sigma x_i \in \{x_i, e\}$, *and*
(b) $|\{i : \sigma x_i \neq e\}| \leq c$.

Proof. ($\Longrightarrow$) This is obvious.

($\Longleftarrow$) Let σ satisfy (a) and (b). Choose $S_0, \cdots, S_m$ and $\gamma_0, \cdots, \gamma_m$ as in Lemma 5, and let j be such that $S_j = \{i : \sigma x_i \neq e\}$. Then, from Lemma 5,

$$\mathbf{G} \models p(\sigma x_1, \cdots, \sigma x_k) \approx \prod_{S_i \subseteq S_j} \gamma_i,$$

so

$$\mathbf{G} \models \prod_{S_i \subseteq S_j} \gamma_i \approx e.$$

As we run over the possible σ we see that this last assertion holds for any $j \leq m$. Then, working through the S_j's in order, we see that, for $j \leq m$,

$$\mathbf{G} \models \gamma_j \approx e.$$

But then we can apply Lemma 6 to obtain

$$\mathbf{G} \models p(x_1, \cdots, x_k) \approx e.$$

□

Theorem 8. *Let* $\mathbf{G}$ *be a finite nilpotent group. Then the polynomial equivalence problem for* $\mathbf{G}$ *is of polynomial time complexity.*

Proof. Let $\mathbf{G}$ be nilpotent class c, and let $p(x_1, \cdots, x_k)$ be a polynomial of $\mathbf{G}$. Let

$$T = \{(a_1, \cdots, a_k) \, : \, |\{i : a_i \neq e\}| \leq c\}.$$

By Proposition 7 we see that

$$\mathbf{G} \models p(\vec{x}) \approx e \qquad \text{iff} \qquad p(\vec{a}) = e \qquad \text{for } \vec{a} \in T.$$

Now

- $|T| = \Sigma_{i \leq c} \binom{k}{i} (|G| - 1)^i$, so T is of polynomial size,
- finding T is a polynomial time procedure, and
- checking $p(\vec{a}) = e$ is a polynomial time procedure.

Thus we have a polynomial time procedure to determine if $\mathbf{G} \models p \approx e$. □

The idea of formulating the algorithm in terms of a polynomial size test set T is due to Joel Berman. It also applies to the results of Hunt & Stearns on finite nilpotent rings.

Next we will see that finite nilpotent groups are not the only ones with a polynomial equivalence problem of polynomial time complexity.

Theorem 9. *The polynomial equivalence problem for the dihedral group* $\mathbf{D}_n$ *is of polynomial time complexity, for* n *odd.*

Proof. First we look at the case that n is odd. Let $a, b \in D_n$ with $o(a) = n$, $o(b) = 2$. Then all elements of $\mathbf{D}_n$ can be written in the form $a^u b^v$, where u, v are integers. Now we have

$$(a^{u_1} b^{v_1})(a^{u_2} b^{v_2}) = a^{u_1 + (-1)^{v_1} u_2} b^{v_1 + v_2},$$

or, abbreviating $a^u b^v$ to (u, v), we have

$$(u_1, v_1) \cdot (u_2, v_2) = (u_1 + (-1)^{v_1} u_2, v_1 + v_2).$$

By induction this leads to

$$(u_1, v_1) \cdots (u_\ell, v_\ell) = (u_1 + (-1)^{v_1} u_2 + \cdots + (-1)^{v_1 + \cdots + v_{\ell - 1}} u_\ell, \ v_1 + \cdots + v_\ell). \quad (3)$$

Now a polynomial $p(x_1, \cdots, x_k)$ of $\mathbf{D}_n$ can be put, in polynomial time, into the form $y_1 \cdots y_\ell$, where each $y_i \in \{x_1, \cdots, x_k\} \cup D_n$. Let $\alpha : \{1, \cdots, \ell\} \implies \{1, \cdots, k\} \cup D_n$ be such that $y_i = x_{\alpha i}$ if y_i is a variable, and $y_i = \alpha i$ if $y_i = g \in D_n$. Replace each y_i by $(u_{\alpha i}, v_{\alpha i})$, meaning: (i) a pair of variables (over the integers) if $\alpha i \in \{1, \cdots, k\}$, or (ii) a pair of integers such that $g = a^{u_{\alpha i}} b^{v_{\alpha i}}$ if $\alpha i = g \in D_n$. This leads to $p(x_1, \cdots, x_n)$ corresponding to

$$(a^{u_{\alpha 1}} b^{v_{\alpha 1}}) \cdots (a^{u_{\alpha \ell}} b^{v_{\alpha \ell}}),$$

or, in our abbreviated notation,

$$(u_{\alpha 1}, v_{\alpha 1}) \cdots (u_{\alpha \ell}, v_{\alpha \ell}).$$

Then, by (3),

$$\mathbf{D}_n \models p(x_1, \cdots, x_k) \approx e$$

holds iff

$$\begin{aligned} u_{\alpha 1} + (-1)^{v_{\alpha 1}} u_{\alpha 2} + \cdots + (-1)^{v_{\alpha 1} + \cdots + v_{\alpha(\ell - l)}} u_{\alpha \ell} &\equiv 0 \bmod n \\ v_{\alpha 1} + \cdots + v_{\alpha_\ell} &\equiv 0 \bmod 2, \end{aligned}$$

and, by putting all, or all but one, of the variable $u_{\alpha i}$'s equal to 0, we see that these two equations hold iff

$$\begin{aligned} \Sigma_{\alpha i \in D_n} \ (-1)^{v_{\alpha 1} + \cdots + v_{\alpha(i-1)}} u_{\alpha i} &\equiv 0 \bmod n & (4) \\ \Sigma_{\alpha i = s} \ (-1)^{v_{\alpha 1} + \cdots + v_{\alpha(i-1)}} &\equiv 0 \bmod n, \text{ for } 1 \leq s \leq k & (5) \\ v_{\alpha 1} + \cdots + v_{\alpha_\ell} &\equiv 0 \bmod 2. & (6) \end{aligned}$$

Now each $v_{\alpha 1} + \cdots + v_{\alpha(i-1)}$ is a sum of variables and integers, so the equations (4) and (5) can be written in the form

$$\epsilon_1 \cdot (-1)^{a_{11} v_1 + \cdots + a_{1k} v_k} + \cdots + \epsilon_r \cdot (-1)^{a_{r1} v_1 + \cdots + a_{rk} v_k} \equiv 0 \bmod n, \quad (7)$$

where $\epsilon_i \in \{0, \cdots, n-1\}$, $a_{ij} \in \{0, 1\}$, and no two rows of the $r \times k$ matrix (a_{ij}) are the same. Let $\eta_i = (-1)^{v_i}$, and define a ring polynomial $q \in \mathbf{Z}_n[w_1, \cdots, w_k]$ by

$$q(w_1, \cdots, w_k) = \sum_{1 \leq i \leq r} \epsilon_i \cdot \prod_{1 \leq j \leq k} {w_j}^{a_{ij}}.$$

As the η_i can independently take on the values in $\{1, -1\}$, and no other values, the equation (7) is equivalent to

$$q \text{ vanishing in } \mathbf{Z}_n \text{ as the } w_i \text{ range over } \{1, -1\}. \quad (8)$$

Now the final part of the polynomial algorithm is to realize that (8) holds iff

$$q(w_1, \cdots, w_k) \text{ is simply the 0 polynomial.} \quad (9)$$

This can be proved by induction on k, namely show that if q is not the zero polynomial then for some assignment c_i of values of the w_i in $\{1, -1\}$ we have $q(c_1, \cdots, c_k) \neq 0$ in $\mathbf{Z}_n$.

The proof proceeds simply by writing $q(w_1, \cdots, w_k)$ in the form

$$q'(w_1, \cdots, w_{k-1}) + (1 - w_k) \cdot q''(w_1, \cdots, w_{k-1}),$$

and noting that if q is not the zero polynomial then choose a ± 1 assignment of $w_1, \cdots, w_{k-1}$ such that one of q' and q'' does not vanish in $\mathbf{Z}_n$. Then either $w_k = 1$ or $w_k = -1$ will yield a nonvanishing value of $q(w_1, \cdots, w_k)$ since we have assumed n is odd. Item (9) gives us a polynomial time algorithm to determine if the equations in (4) and (5) hold. And determining if (6) holds is quite easy.

This takes care of the case for n odd. To handle the general case let $n = 2^k \cdot m$, where m is odd. Then one can embed $\mathbf{D}_n$ into $\mathbf{D}_{2^k} \times \mathbf{D}_m$, and both $\mathbf{D}_{2^k}$ and $\mathbf{D}_m$ embed into $\mathbf{D}_n$. Thus one has a polynomial time algorithm for the polynomial equivalence problem for $\mathbf{D}_n$ as one has such for $\mathbf{D}_m$ by the above, and for $\mathbf{D}_{2^k}$ by Theorem 9 (as $\mathbf{D}_{2^k}$ is nilpotent). □

The result for $\mathbf{D}_n$ holds, by the same methods, for other finite groups which can be presented by defining relations of the form $o(a) = n$, $o(b) = m$, and $b^{-1}ab = a^j$, where $\gcd(\mathrm{j}, \mathrm{n}) = 1$ and $o(j) = 2$ in $\mathbf{Z}_n$. On the other hand Lawrence has proved that any finite nonsolvable group has a co-**NP**-complete term equivalence problem—hence the following question is appropriate.

Problem 1. Does every finite solvable group have a term [polynomial] equivalence problem of polynomial time complexity?

References

[1] S. Burris, *Computers and universal algebra: some directions.* Algebra Universalis **34** (1995), 61–71.

[2] S. Burris and J. Lawrence, *The equivalence problem for finite rings.* J. Symbolic Computation **15** (1993), 67–71.

[3] S. Burris and H.P. Sankappanavar, *A Course in Universal Algebra*. Springer-Verlag, 1981.

[4] H.B. Hunt III and R.E. Stearns *The complexity of equivalence for commutative rings.* J. Symbolic Computation **10** (1990), 411–436.

[5] O.G. Kharlampovich and M.V. Sapir, *Algorithmic problems in varieties.* Internat. J. Algebra Comput. **5** (1995), 379–602.

[6] H. Neumann, *Varieties of Groups.* Springer-Verlag, 1967.

Dept. of Pure Mathematics, University of Waterloo, Waterloo, Ont., Canada N2L 3G1

E-mail address: snburris@thoralf.uwaterloo.ca

Dept. of Pure Mathematics, University of Waterloo, Waterloo, Ont., Canada N2L 3G1

E-mail address: jwlawren@math.uwaterloo.ca