Siberian Mathematical Journal, *Vol.* 53, *No.* 2, *pp.* 201–206, 2012

ECONOMICAL ADJUNCTION OF SQUARE ROOTS TO GROUPS

© **D. V. Baranov and Ant. A. Klyachko** UDC 512.543.7:512.542

Abstract: How do we have to extend a group so that in the resulting group all elements of the original group be squares? We give a rather precise answer to this question (the best possible upper bound differs from our estimate by at most a factor of two) and pose several open questions.

Keywords: equations over a group, adjunction of roots, wreath product

Introduction

A series of articles studies the solvability of equations over groups (see, e.g., [1–14] and the references therein). It is shown there that under certain conditions the equation $w(x) = 1$ with coefficients in a group G is *solvable over* G; thus, we can find a group H that includes G as a subgroup and an element $h \in H$ satisfying $w(h) = 1$. In this article we address the quantitative question: *How large must this group* H *be?* Even for simple equations whose solvability is known for a long time this question turns out rather difficult, and we restrict exposition to the simplest nontrivial equations $x^2 = g$.

Certainly, the answer depends strongly on the original group G. For instance, if the order of G is odd then for every $g \in G$ we can take as H the group G itself; if G is a cyclic group then for each $g \in G$ it suffices to take as H a group of twice the order of G, and so forth. It is most interesting, of course, to estimate the order of H in the worst case. We have managed to obtain an estimate that differs from the best in at most a factor of two in the following sense:

Main Theorem. *Each finite group* G *embeds into a group of order* $2|G|^2$ *in which all elements of* G *are squares. There exist infinitely many pairwise nonisomorphic finite groups* G_i *such that for some* $g_i \in G_i$ *the group including* G_i *as a subgroup and containing an element whose square equals* g_i *is of order at least* $|G_i|^2$.

Apart from the problem of solving one equation $x^2 = g$, we can consider the problem of solving simultaneously all equations of this form. It is clear from the main theorem that in this case a group of order $2|G|^2$ always suffices, while a group of order less than $|G|^2$ is not sufficient in general.

Much is known about the behavior of the set of solutions to equations in finite groups (see, e.g., [15–18] and the references therein). Unfortunately, we were unable to use these nontrivial results.

The first claim of the theorem is not new and can be established easily (see Section 1). In Section 2 we prove the second claim. In Section 3 we state several open questions on economical adjunction of solutions to equations to groups.

Our notation is standard in general. Note only that if $k \in \mathbb{Z}$, while x and y are elements of some group, then x^y, x^{ky}, and x^{-y} stand for $y^{-1}xy$, $y^{-1}x^ky$, and $y^{-1}x^{-1}y$ respectively. If X is a subset of some group then $|X|$, $\langle X\rangle$, and $\langle\langle X\rangle\rangle$ stand respectively for the cardinality of X, the subgroup generated by X, and the normal subgroup generated by X. Denote by $\mathbb{Z}$ the set of integers. Denote by $\mathbb{Z}_n$ the group or ring $\mathbb{Z}/n\mathbb{Z}$ of residues modulo n. Denote the multiplicative group of $\mathbb{Z}_n$ by $\mathbb{Z}_n^*$. Denote the automorphism group of G by $\operatorname{Aut} G$. Denote by D_p the dihedral group of order $2p$. Denote the stabilizer of a point a under the action of G by $\operatorname{St}_G(a)$. We refer as a *reflection* to an element of D_p lying outside its subgroup $\mathbb{Z}_p$.

The authors are grateful to the anonymous referee for valuable remarks.

The authors were supported by the Russian Foundation for Basic Research (Grant 11–01–00945).

Moscow. Translated from *Sibirskiĭ Matematicheskiĭ Zhurnal*, Vol. 53, No. 2, pp. 250–257, March–April, 2012. Original article submitted January 20, 2011.

1. Wreath Products and a Proof of the First Claim of the Theorem

The first claim of the theorem is well known [13]: the wreath product

$$G \wr \mathbb{Z}_2 = \left\{ \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \mid g_1, g_2 \in G \right\} \cup \left\{ \begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix} \mid g_1, g_2 \in G \right\}$$

of a group G and the cyclic group of order 2 is a group of order $2|G|^2$ and contains square roots of all elements of G assuming that G is embedded into the wreath product $G \wr \mathbb{Z}_2$ diagonally:

$$g \mapsto \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix}.$$

Indeed, $\begin{pmatrix} 0 & g \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix}$. This is the simplest particular case of Levin's theorem, whose full statement we present in Section 3.

2. Dihedral Groups and a Proof of the Second Claim of the Theorem

The second claim of the main theorem is immediate from the following claim.

Theorem 1. *Take a prime $p \in 4\mathbb{Z} + 3$ and a group $\widetilde{G}$ including a dihedral subgroup $G = D_p$. If a reflection $g \in G$ is a square of some element $x \in \widetilde{G}$ then $|\widetilde{G}| \geq |G|^2$.*

We need several easy lemmas.

Lemma 1. *Given two subgroups H_1 and H_2 of some group H, we have $|H| \geq \frac{|H_1||H_2|}{|H_1 \cap H_2|} = |H_1 H_2|$.*

Proof. This easy lemma is left to the reader.

Lemma 2. *Suppose that $D_p = G \subseteq \langle G, x \rangle = \widetilde{G}$ and $x^2 = g$, where $g \in G$ is a reflection. Then either $G \lhd \widetilde{G}$ or $G \cap G^x = \langle g \rangle$.*

Proof. It is obvious that $g \in G \cap G^x$. There exist only two subgroups of D_p containing g. If $G \cap G^x = \langle g \rangle$ then the claim is proved. If $G \cap G^x = G$ then $G = G^x$; but $G \lhd \widetilde{G}$ since $\langle G, x \rangle = \widetilde{G}$.

Lemma 3. *Suppose that $D_p = G \lhd \widetilde{G}$, where $p \in 3 + 4\mathbb{Z}$ is a prime. Then no reflection $g \in G$ is a square in $\widetilde{G}$.*

Proof. The subgroup $\mathbb{Z}_p \subset D_p = G \lhd \widetilde{G}$ is the commutant of G, and so $\mathbb{Z}_p$ is a characteristic subgroup of G and a normal subgroup of $\widetilde{G}$. The group $\widetilde{G}$ acts on $\mathbb{Z}_p$ by conjugation. Furthermore, the reflection g acts as $-1 \in \mathbb{Z}_p^* = \operatorname{Aut} \mathbb{Z}_p$, but -1 is not a square in $\mathbb{Z}_p^*$ if $p \in 3+4\mathbb{Z}$, which proves the lemma.

We proceed to prove Theorem 1. We may assume that $\widetilde{G} = \langle G, x \rangle$. Denote by K the set of all subgroups of $\widetilde{G}$ conjugate to G. Then $\widetilde{G}$ acts transitively on K by conjugation.

Lemma 4. $|\widetilde{G}| \geq |K| \cdot |G|$.

Proof. $|\widetilde{G}| = |K| \cdot |\operatorname{St}_{\widetilde{G}}(G)| \geq |K| \cdot |G|$ since $G \subseteq \operatorname{St}_{\widetilde{G}}(G)$.

Consider the complete undirected graph Γ with the vertex set K. Refer to an edge (G^{h_1}, G^{h_2}) as *green* whenever $|G^{h_1} \cap G^{h_2}| = 2$, as *yellow* whenever $|G^{h_1} \cap G^{h_2}| = p$, and as *red* whenever $|G^{h_1} \cap G^{h_2}| = 1$. It is clear that all edges are colored. If there is at least one red edge then the claim follows directly from Lemma 1. Thus, we assume henceforth that there are no red edges.

Lemma 5. *The vertices K and the yellow edges constitute a graph Y whose each connected component is a complete graph. All connected components contain the same number of vertices.*

Proof. The first claim of the lemma is immediate since D_p includes only one order p subgroup. Since $\widetilde{G}$ acts transitively on K and preserves the colors of the edges, it follows that all connected components contain the same number of vertices.

Lemma 6. *The number of green edges incident to a vertex of G is positive and divisible by p.*

PROOF. Each green edge incident to G corresponds to one of the p reflections $g \in G$. Therefore, the edges incident to G split into p classes. All of them contain the same number of edges since all reflections in G are conjugate, and consequently each of these classes goes into a given class under an automorphism of the graph. This means that the number of green edges incident to G is divisible by p.

One green edge in the graph certainly exists: this is the edge (G, G^x), where $x^2 = g \in G$ is a reflection. Indeed, $G^x \cap G \ni g$, but $G^x \neq G$ (otherwise G would be a normal subgroup of $\widetilde{G} = \langle G, x\rangle$, which is precluded by Lemma 3). Hence, $G^x \cap G = \langle g\rangle_2$, and the proof of the lemma is complete.

Continue proving the theorem. Suppose that at least $2p$ green edges are incident to G. Then the graph has at least $2p + 1$ vertices: $|K| > 2p$, and the claim follows since $|\widetilde{G}| \geq |K| \cdot |G| > 2p|G| = |G|^2$ by Lemma 4.

In view of Lemma 6, it remains to consider the case where every vertex of the graph is incident to exactly p green edges.

Denote by u the number of vertices in each connected component of Y (see Lemma 5), and by v, the number of these connected components. Then

$$p = (\text{the number of green edges incident to } G) = (v - 1)u$$

since every vertex not joined to G by a yellow edge is joined to G by a green edge.

Since p is a prime, $p = (v - 1)u$ means that either $v = 2$ and $u = p$ or $v = p + 1$ and $u = 1$.

In the first case $|K| = 2p$ and the claim follows since $|\widetilde{G}| \geq 2p|G| = |G|^2$ by Lemma 4.

In the second case $|K| = p + 1$ and the graph Γ amounts to a complete graph whose all edges are green. The group $\widetilde{G}$ acts on this graph; moreover, the action of G on the set of vertices different from G is isomorphic to the action of G by conjugation on the set of its order 2 subgroups (this isomorphism assigns the subgroup $G^h \cap G$ to each group G^h). In particular, conjugation by the reflection g amounts to a permutation of the vertices of the graph which leaves exactly two points fixed (G and the group G^h with $G \cap G^h = \langle g\rangle$), and consequently we can express it as the product of $\frac{p-1}{2}$ independent transpositions. This permutation is odd since $p \in 3 + 4\mathbb{Z}$, which contradicts the fact that g is a square in $\widetilde{G}$. The proof of the theorem is complete.

§ 3. Roots of Higher Degrees and Other Open Questions

The following question arises: What is actually the sharp estimate?

Question 1. *Is the set of finite groups G such that for some $g \in G$ every group including G as a subgroup and containing an element whose square equals g is of order at least $2|G|^2$ infinite?*

The following statement shows that for dihedral groups our theorem cannot be strengthened, while to answer Question 1 we should study groups close to simple.

Proposition 1. *Suppose that a finite group G and g in G satisfy at least one of the conditions:*
(a) *G is distinct from its commutator subgroup;*
(b) *G is distinct from the normal closure of g;*
(c) *G includes a nontrivial normal subgroup of odd order.*[1)]
Then G embeds into a group H of order at most $|G|^2$ in which g is a square.

PROOF. The following lemma shows that if condition (a) or (b) is fulfilled then we can take as H not the full wreath product $G \wr \mathbb{Z}_2$ (see Section 1), but its proper subgroup. If condition (c) is fulfilled then we can take as H a proper quotient group of this wreath product, as Lemma 8 shows (see below).

[1)] The Feit–Thompson theorem on the solvability of groups of odd order [19] implies that property (c) is equivalent to the presence in G of a nontrivial normal abelian subgroup of odd order.

Lemma 7. *In the wreath product $G \wr \mathbb{Z}_2$ the subgroup H generated by G embedded diagonally and the square root $\begin{pmatrix} 0 & g \\ 1 & 0 \end{pmatrix}$ of an element $g \in G$ is of the form*

$$H = \left\{ \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \mid g_1 g_2^{-1} \in [\langle\langle g \rangle\rangle, G] \right\} \cup \left\{ \begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix} \mid g_1 g_2^{-1} \in g\,[\langle\langle g \rangle\rangle, G] \right\},$$

where $[\langle\langle g \rangle\rangle, G]$ is the mutual commutator subgroup of the normal closure of g in G and the group G.

Proof. The epimorphism $\varphi : G \to G/\,[\langle\langle g \rangle\rangle, G]$ induces a homomorphism

$$\Phi : G \wr \mathbb{Z}_2 \to (G/\,[\langle\langle g \rangle\rangle, G]) \wr \mathbb{Z}_2.$$

The set on the right-hand side of the equality to be proved is $\Phi^{-1}(\Phi(H))$. Thus, it suffices to show that H includes the kernel of Φ. But $\ker \Phi$ is generated (as a subgroup) by the elements

$$\begin{pmatrix} [g^x, y] & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & [g^x, y] \end{pmatrix}, \quad \text{where } x, y \in G,$$

which lie in H as the equalities show:

$$\begin{pmatrix} x^{-1} & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 0 & g \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 0 & g^x \\ 1 & 0 \end{pmatrix},$$

$$\left[\begin{pmatrix} 0 & g^x \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \right] = \begin{pmatrix} 0 & 1 \\ g^{-x} & 0 \end{pmatrix} \begin{pmatrix} 0 & g^{xy} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & [g^x, y] \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & [g^x, y] \end{pmatrix} \begin{pmatrix} [g^x, y] & 0 \\ 0 & [g^x, y] \end{pmatrix}^{-1} = \begin{pmatrix} [g^x, y] & 0 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Lemma 8. *If N is a normal abelian subgroup of G then*

$$K = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in N \right\}$$

is a normal subgroup of $G \wr \mathbb{Z}_2$. If the order of N is odd then K trivially intersects G (embedded into the wreath product diagonally).

Conversely, each nontrivial normal subgroup of the wreath product which intersects G trivially includes a nontrivial normal abelian subgroup of this form.

Proof. It is obvious that K is a normal subgroup. It is clear that

$$K \cap G = \{x \in N \mid x^2 = 1\}.$$

Thus, K trivially intersects G when the order of N is odd.

It is known that every nontrivial normal subgroup X of the wreath product intersects the base nontrivially (see [20] for instance). Take

$$1 \neq u = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in X.$$

Then

$$\left[u, \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \right] = \begin{pmatrix} [x, y] & 0 \\ 0 & 1 \end{pmatrix} = v \in X \ni \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} v \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & [x, y] \end{pmatrix} = w,$$

and, consequently,

$$vw = \begin{pmatrix} [x, y] & 0 \\ 0 & [x, y] \end{pmatrix} \in X \cap G = \{1\}, \quad \text{i.e., } [x, y] = 1.$$

In this case

$$X \ni \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} u \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & x \end{pmatrix} = t;$$

hence,

$$ut = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} \in X \cap G = \{1\}, \quad \text{i.e., } xy = 1.$$

Therefore, the intersection of the subgroup X with the base of the wreath product is

$$K = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in N \right\},$$

where N is a subset of G. Certainly, this implies that N must be a normal abelian subgroup. The proof of the lemma is complete.

These lemmas establish Proposition 1 and, moreover, show that if a group G violates all conditions (a)–(c) (for instance, if G is a nonabelian simple group) then the wreath product $G \wr \mathbb{Z}_2$ lacks proper subgroups and proper quotient groups including G and containing the square root $\begin{pmatrix} 0 & g \\ 1 & 0 \end{pmatrix}$ of g.

Proceed now to roots of higher degrees and solutions to other equations. The starting point of our study is Levin's theorem whose full statement is as follows:

Levin Theorem [13]. *The wreath product $G \wr \mathbb{Z}_n$ of a group G and an order n cyclic group (being of order $n|G|^n$) contains solutions to all positive equations of degree n over G.*

By a *positive equation of degree n over G* we understand an equation of the form

$$g_1 x g_2 x \dots g_n x = 1, \quad \text{where } g_1, \dots, g_n \in G.$$

In this regard, the question arises: Does Levin's theorem yield an unimprovable estimate?

Question 2. *Is the set of finite groups G such that every group including G as a subgroup containing a solution to every positive equation of degree n over G is of order at least $n|G|^n$ infinite?*

We can put forth a bolder conjecture.

Question 3. *Is the set of finite groups G such that every group H including G as a subgroup every element of which is an nth power in H is of order at least $n|G|^n$ infinite?*

What can we say about economical adjunction of solutions to other (nonpositive) equations? For instance, the Gerstenhaber–Rothaus theorem [8] in combination with Malcev's theorem about residual finiteness of finitely generated linear groups [21] yields the statement:

Proposition 2 [8, 20]. *Each finite group G embeds into a finite group H containing solutions to all nondegenerate equations of length n over G.*

By a *nondegenerate equation of length n over* a group G we understand an equation of the form

$$g_1 x^{\varepsilon_1} g_2 x^{\varepsilon_2} \dots g_n x^{\varepsilon_n} = 1, \quad \text{where } g_i \in G,\ \varepsilon_i \in \{\pm 1\}, \text{ and } \sum \varepsilon_i \neq 0.$$

The proof of the Gerstenhaber–Rothaus theorem is beautiful but not constructive. Thus, it is difficult to write not only unimprovable, but even any explicit estimate on the order of H.

Question 4. *Can we estimate $|H|$ in terms of $|G|$ and n in claim 2?*

For $n = 1$ the answers to Questions 2–4 are obviously affirmative. A nondegenerate equation of length 2 is of the form $g_1 x^{\varepsilon} g_2 x^{\varepsilon} = 1$, where $\varepsilon \in \{\pm 1\}$, and a linear change of variables reduces it to $x^2 = g$; thus, the main result of this article yields the answer to "twice weakened" versions of these questions for $n = 2$. We do not know what happens for other values of n.

References

1. *Brodskiĭ S. D.*, "Equations over groups and one-related groups," Sibirsk. Mat. Zh., **25**, No. 2, 84–103 (1984).
2. *Klyachko A. A.,* "How to generalize known results on equations over groups," Math. Notes, **79**, No. 3, 377–386 (2006) (also see arXiv:math.GR/0406382).
3. *Klyachko Ant. A. and Prishchepov M. I.*, "The descent method for equations over groups," Moscow Univ. Math. Bull., **50**, No. 4, 56–58 (1995).
4. *Clifford A. and Goldstein R. Z.*, "Equations with torsion-free coefficients," Proc. Edinburgh Math. Soc., **43**, 295–307 (2000).
5. *Edjvet M. and Howie J.*, "The solution of length four equations over groups," Trans. Amer. Math. Soc., **326**, 345–369 (1991).
6. *Edjvet M. and Juhász A.*, "Equations of length 4 and one-relator products," Math. Proc. Cambridge Phil. Soc., **129**, 217–230 (2000).
7. *Fenn R. and Rourke C.*, "Klyachko's methods and the solution of equations over torsion-free groups," Enseign. Math., II Sèr., **42**, 49–74 (1996).
8. *Gerstenhaber M. and Rothaus O. S.*, "The solution of sets of equations in groups," Proc. Nat. Acad. Sci. USA, **48**, 1531–1533 (1962).
9. *Howie J.*, "The quotient of a free product of groups by a single high-powered relator. III: The word problem," Proc. London Math. Soc., **62**, No. 3, 590–606 (1991).
10. *Juhász A.*, "On the solvability of a class of equations over groups," Math. Proc. Cambridge Phil. Soc., **135**, No. 2, 211–217 (2003).
11. *Klyachko Ant. A.*, "A funny property of a sphere and equations over groups," Comm. Algebra, **21**, 2555–2575 (1993).
12. *Klyachko Ant. A.*, "Asphericity tests," Internat. J. Algebra Comput., **7**, No. 4, 415–431 (1997).
13. *Levin F.*, "Solutions of equations over groups," Bull. Amer. Math. Soc., **68**, 603–604 (1962).
14. *Lyndon R. C.*, "Equations in groups," Bol. Soc. Bras. Math., **11**, No. 1, 79–102 (1980).
15. *Strunkov S. P.*, "On the theory of equations in finite groups," Izv.: Math., **59**, No. 6, 1273–1282 (1995).
16. *Frobenius G.,* "Über einen Fundamentalsatz der Gruppentheorie," Berl. Sitz., 987–991 (1903).
17. *Hall Ph.*, "On a theorem of Frobenius," Proc. London Math. Soc., **40**, 468–501 (1936).
18. *Solomon L.*, "The solutions of equations in groups," Arch. Math., **20**, No. 3, 241–247 (1969).
19. *Feit W. and Thompson J. G.*, "Solvability of groups of odd order," Pacific J. Math., **13**, No. 3, 775–1029 (1963).
20. *Kargapolov M. I. and Merzlyakov Yu. I.*, Fundamentals of the Theory of Groups, Springer-Verlag, New York, Heidelberg, and Berlin (1979).
21. *Malcev A. I.*, "On isomorphic matrix representations of infinite groups," Mat. Sb., **8**, No. 3, 405–422 (1940).

D. V. Baranov; Ant. A. Klyachko
Moscow State University, Moscow, Russia
E-mail address: dimbaranov@mail.ru; klyachko@mech.math.msu.ru