European Journal of Combinatorics 33 (2012) 474–476

Contents lists available at SciVerse ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

On the distance between non-isomorphic groups

Gábor Ivanyos [a,1], François Le Gall [b], Yuichi Yoshida [c]

[a] Computer and Automation Research Institute of the Hungarian Academy of Sciences, Kende u. 13-17, H-1111 Budapest, Hungary

[b] Department of Computer Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan

[c] School of Informatics, Kyoto University, and Preferred Infrastructure, Inc., Yoshida-Honmachi, Kyoto 606-8501, Japan

ARTICLE INFO

Article history:
Received 1 July 2011
Received in revised form
24 October 2011
Accepted 24 October 2011
Available online 5 January 2012

ABSTRACT

A result of Ben-Or, Coppersmith, Luby and Rubinfeld on testing whether a map between two groups is close to a homomorphism implies a tight lower bound on the distance between the multiplication tables of two non-isomorphic groups.

In [3] Drápal showed that if $\circ$ and $*$ are two binary operations on the finite set G such that $(G, \circ)$ and $(G, *)$ are non-isomorphic groups then the Hamming distance between the two multiplication tables is greater than $\frac{1}{9}|G|^2$. In [5] there are constructed infinite families of non-isomorphic pairs of 3-groups at distance exactly $\frac{2}{9}|G|^2$.

In this note we show that $\frac{2}{9}|G|^2$ is a lower bound for the distance between arbitrary non-isomorphic group structures. The proof is a simple application of the following result from [2].

Fact 1. Let $(G, \circ)$ and $(K, *)$ be two groups and $f: G \to K$ be a map such that

$$\frac{\#\{(x, y) \in G \times G : f(x \circ y) = f(x) * f(y)\}}{|G|^2} > \frac{7}{9}.$$

Then there exists a group homomorphism $h: G \to K$ such that $\frac{\#\{x \in G: f(x) = h(x)\}}{|G|} \geq \frac{5}{9}$.

Fact 1 is a weak version of Theorem 1 in [2]. Here is a brief sketch of its proof. For every $x \in G$, $h(x)$ is defined as the value taken most frequently by the expression $f(x \circ y) * f(y)^{-1}$ where y runs over G. Then the first step is showing that for every $x \in G$, $\#\{y \in G : f(x \circ y) * f(y)^{-1} = h(x)\} > \frac{2}{3}|G|$. The homomorphic property of h and equality of $h(x)$ with $f(x)$ for $\frac{5}{9}$ of the possible elements x follow from this claim easily.

E-mail addresses: Gabor.Ivanyos@sztaki.hu (G. Ivanyos), legall@is.s.u-tokyo.ac.jp (F. Le Gall), yyoshida@kuis.kyoto-u.ac.jp (Y. Yoshida).

1 Tel.: +36 1 2796164; fax: +36 1 2095269.

0195-6698/$ – see front matter
doi:10.1016/j.ejc.2011.10.009

We apply Fact 1 to obtain a result on the distance between multiplication tables of groups of not necessarily equal size. It will be convenient to state it in terms of a quantity complementary to the distance. Let $(G, \circ)$ and $(K, *)$ be finite groups. We define the overlap between $(G, \circ)$ and $(K, *)$ as

$$\max_{\gamma:G\hookrightarrow S,\kappa:K\hookrightarrow S} \# \left\{ (x,y) \in G \times G : \exists (x',y') \in K \times K \text{ s.t. } \begin{array}{r} \gamma(x) = \kappa(x'), \\ \gamma(y) = \kappa(y'), \\ \gamma(x \circ y) = \kappa(x' * y') \end{array} \right\},$$

where S is any set with $|S| \geq \max(|G|, |K|)$.

Corollary 1. *If $|G| \leq |K|$ and $(G, \circ)$ is not isomorphic to a subgroup of $(K, *)$ then the overlap between $(G, \circ)$ and $(K, *)$ is at most $\frac{7}{9}|G|^2$.*

Proof. Assume that the overlap is larger than $\frac{7}{9}|G|^2$. Then there exist injections $\gamma : G \hookrightarrow S, \kappa : K \hookrightarrow S$ such that the set

$$Z = \left\{ (x,y) \in G \times G : \exists (x',y') \in K \times K \text{ s.t. } \begin{array}{r} \gamma(x) = \kappa(x'), \\ \gamma(y) = \kappa(y'), \\ \gamma(x \circ y) = \kappa(x' * y') \end{array} \right\}$$

has cardinality larger than $\frac{7}{9}|G|^2$. Put

$$G_0 = \{x \in G | \exists x' \in K \text{ such that } \gamma(x) = \kappa(x')\}.$$

Then $\kappa^{-1} \circ \gamma$ embeds G_0 into K and it can be extended to an injection $\phi : G \hookrightarrow K$. For $(x, y) \in Z$ we have

$$\phi(x \circ y) = \kappa^{-1}(\gamma(x \circ y)) = \kappa^{-1}(\gamma(x)) * \kappa^{-1}(\gamma(y)) = \phi(x) * \phi(y),$$

and therefore, by Fact 1, there exists a homomorphism $\psi : G \to K$ such that

$$\#\{x \in G : \psi(x) \neq \phi(x)\} < \frac{4}{9}|G|.$$

This, together with the injectivity of ϕ implies that the ψ is injective as well and its image is a subgroup of $(K, *)$ isomorphic to $(G, \circ)$. $\square$

We remark that the bound $\frac{2}{9}|G|^2$ on the distance for non-isomorphic group structures is only tight in the case of general (or general Abelian) groups. For 2-groups the tight bound is $\frac{1}{4}|G|^2$ (see [4]). In [5], a formula for p-groups is conjectured (and proved in the cases $p = 2$ and $p = 3$). Regarding homomorphism tests, for special classes of groups, the "error bound" $\frac{2}{9} = 1 - \frac{7}{9}$ of Fact 1 can also be improved (at the cost of getting a somewhat worse, but still meaningful "distance bound" in the conclusion). For the case of $G = (\mathbb{Z}/(2))^m$ and $K = \mathbb{Z}/(2)$, $\frac{2}{9}$ can be replaced with $\frac{45}{128} > \frac{1}{4}$ (see [1]). As the bound for distances between groups coincides with that for "errors" in homomorphism tests for general groups, it is natural to ask whether this happens to be the case for certain classes of groups as well. In particular, it would be interesting to know whether the bound $\frac{1}{4}$ of [4] remains valid in the context of testing homomorphisms between general 2-groups.

Acknowledgment

The authors are grateful to an anonymous referee for helpful remarks and suggestions.

References

[1] M. Bellare, D. Coppersmith, J. Hastad, M. Kiwi, M. Sudan, Linearity testing in characteristic two, IEEE Transactions on Information Theory 42 (1996) 1781–1795.
[2] M. Ben-Or, D. Coppersmith, M. Luby, R. Rubinfeld, Non-abelian homomorphism testing, and distributions close to their self-convolutions, Random Structures and Algorithms 32 (2008) 49–70.
[3] A. Drápal, How far apart can the group multiplication tables be? European Journal of Combinatorics 13 (1992) 335–343.

[4] A. Drápal, Non-isomorphic 2-groups coincide at most in three quarters of their multiplication tables, European Journal of Combinatorics 21 (2000) 301–321.
[5] A. Drápal, On distances of 2-groups and 3-groups, in: C.M. Campbell, E.F. Robertson, G.C. Smith (Eds.), Groups St. Andrews 2001 in Oxford: Volume 1, in: LMS Lecture Notes Series, vol. 304, Cambridge University Press, Cambridge, 2003, pp. 143–149.