On the distance between non-isomorphic groups

Gábor Ivanyos* François Le Gall† Yuichi Yoshida‡

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 [2] 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 [3] it is shown that if $(G,\circ)$ and $(G,*)$ are non-isomorphic 3-groups then the distance is at least $\frac{2}{9}|G|^2$; and infinite families of non-isomorphic pairs of 3-groups with distance exactly $\frac{2}{9}|G|^2$ are given.

In this note we show that the lower bound $\frac{2}{9}|G|^2$ holds for arbitrary non-isomorphic group structures. The proof is a simple application of the following result from [1].

Fact 1. *Let $(G,\circ)$ and $(K,*)$ be two groups and $f\colon G \to K$ 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 $h\colon G\to K$ 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 [1]. 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.

We apply Fact 1 to obtain a result on the distance of 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

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

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

*Computer and Automation Research Institute of the Hungarian Academy of Sciences, Kende u. 13-17, H-1111 Budapest, Hungary. E-mail: `Gabor.Ivanyos@sztaki.hu`

†Department of Computer Science, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan. E-mail: `legall@is.s.u-tokyo.ac.jp`

‡School of Informatics, Kyoto University, and Preferred Infrastructure, Inc., Yoshida-Honmachi, Kyoto 606-8501, Japan. E-mail: `yyoshida@kuis.kyoto-u.ac.jp`

Corollary 1. *If* $|G| \le |K|$ *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

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

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

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

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 the ψ is injective as well and its image is a subgroup of $(K,*)$ isomorphic to $(G,\circ)$. $\square$

References

[1] 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.

[2] A. Drápal, How far apart can the group multiplication tables be?, European Journal of Combinatorics 13 (1992), 335–343.

[3] 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 (LMS Lecture Notes Series No. 304), Cambridge University Press, Cambridge, 2003, pp. 143–149.