DISTANCES OF GROUPS OF PRIME ORDER

PETR VOJTĚCHOVSKÝ

1. Introduction

Let G be a finite set with n elements, and $G(\circ)$, $G(*)$ two groups defined on G. Their (*Hamming*) *distance* is the number of pairs $(a, b) \in G \times G$ for which $a \circ b \neq a * b$. Let us denote this value by $dist(G(\circ), G(*))$.

It is not difficult to show that $dist(\_,\_)$ is a metric on the set of all groups defined on G. In fact, when G_n, G_m are two groups of different orders n and m, respectively, and $dist(G_n, G_m)$ is defined simply by $max\{n^2, m^2\}$, then $dist(\_,\_)$ is a metric on all finite groups (defined on some fixed sets).

Similar ideas were first introduced by L. Fuchs in [8]. He asked about the maximal number of elements, which can be deleted at random from a group multiplication table M, so that the rest of M determines M up to isomorphism, or even allows a complete reconstruction of M. These two numbers have been denoted by $k_1(M)$ and $k_2(M)$.

J. Dénes shows in [1] that $k_2(M) = 2n-1$, not including abelian groups of order 4 and 6. His proof (published also in [2]) was fixed by S. Frische in [7]. She also found correct values of $k_2(M)$ for abelian groups of order 4 and 6 — these are equal to 3 and 7. Surprisingly, the value of $k_2(M)$ does not depend on structure of M at all.

Definition 1.1. Let $G(\circ)$ be a group. Then

$$\delta(G(\circ)) = min\{dist(G(\circ), G(*)); G(*) \neq G(\circ)\}$$

is called *Cayley stability of* $G(\circ)$. In similar manner, put

$$\mu(G(\circ)) = min\{dist(G(\circ), G(*)); G(*) \simeq G(\circ) \neq G(*)\},$$
$$\nu(G(\circ)) = min\{dist(G(\circ), G(*)); G(*) \not\simeq G(\circ)\},$$

and call these numbers *Cayley stability of* $G(\circ)$ *among isomorphic groups*, *Cayley stability of* $G(\circ)$ *among non-isomorphic groups*, respectively. Note that $\nu(G(\circ))$ is defined only when n is not a prime.

Definition 1.2. Let $f : H \longrightarrow K$ be a mapping between two groups H, K. *Distance of* f *from a homomorphism* is the number m_f of pairs $(a, b) \in H \times H$ at which f does not behave as a homomorphism, i.e. $f(ab) \neq f(a)f(b)$.

When both operations $\circ$ and $*$ are fixed, and g is an element of G, we shall use $d(g)$ to denote the cardinality of $\{h \in G; g \circ h \neq g * h\}$.

While working on this paper the author has been partially supported by the University Development Fund of Czech Republic, grant number 1379/1998 .

2. Some known facts

Relatively few facts are known about $\nu(G(\circ))$. One can prove that $v(E_{2^n}) = 2^{2n-2}$, where E_{2^n} is the elementary abelian 2-group of order 2^n (see [5]). More generally, when $G(\circ)$, $G(*)$ are two groups of order n with $d(G(\circ), G(*)) < n^2/4$, then their Sylow 2-subgroups must be isomorphic (see [6]).

The Cayley stability is known for any group $G(\circ)$ of order $n \geq 51$ (main result of [4]), and is equal to $\delta_0(G(\circ))$, where, using words of [3],

$$\delta_0(G(\circ)) = \begin{cases} 6n-18 & \text{if } n \text{ is odd,} \\ 6n-20 & \text{if } G(\circ) \text{ is dihedral of twice odd order,} \\ 6n-24 & \text{otherwise.} \end{cases}$$

Cayley stability of $G(\circ)$ is less than or equal to $\delta_0(G(\circ))$ whenever $n \geq 5$ (for more details see 2.3). Moreover, the nearest group $G(*)$ must be isomorphic to $G(\circ)$. As 2.3 says, when $f : G(\circ) \longrightarrow G(*)$ is an isomorphism, then f is a transposition. This means that $\mu(G(\circ)) < \nu(G(\circ))$ holds for all groups of order at least 51. However, $\mu(G(\circ)) < \nu(G(\circ))$ is not true in general; the exceptions embrace the elementary abelian 2-group of order 8 and the group of quaternions of order 8. This is shown in [9], section 8. The biggest group found so far, for which $\delta(G(\circ)) \neq \delta_0(G(\circ))$ is the cyclic group of order 21 (see [9], p.36).

Our goal is to prove that $\delta(G(\circ)) = 6p-18$ for each prime p greater than 7 (note that $\delta(G(\circ)) \leq 6p-18$ holds for each $p > 7$). In order to achieve this we need the following propositions:

Lemma 2.1. *Suppose that $G(\circ)$, $G(*)$ are two groups of order n, and $a \circ b \neq a * b$ for some a, $b \in G$. Then $d(a) + d(b) + d(a \circ b) \geq n$.*

Proof. [9] lemma 2.10, or, more generally, [4] lemma 2.4. □

Proposition 2.2. *Let $G(\circ)$, $G(*)$ be two groups. Put $K = \{a \in G; d(a) < n/3\}$, and assume that $|K| > 3n/4$. Define a mapping $f : G \longrightarrow G$ by $f(g) = a * b$ for any $g \in G$, a, $b \in K$, $g = a \circ b$. Then f is an isomorphism of $G(\circ)$ onto $G(*)$, and $f(a) = a$ for each $a \in K$. Moreover, $f(g) \neq g$ for any $g \in G$ with $d(g) > 2n/3$.*

Proof. [4] proposition 3.1. □

Proposition 2.3. *Let $G(\circ)$ be a finite group of order $n \geq 5$. Then there exists a transposition f of $G(\circ)$ with $m_f = \delta_0(G(\circ))$. Furthermore, $m_f \geq \delta_0(G(\circ))$ for any transposition f of G. Finally, if $n \geq 12$, and f is such a permutation of G that $n > |\{g \in G; f(g) = g\}| > 2n/3$, then $m_f \geq \delta_0(G(\circ))$, and f is a transposition whenever $m_f = \delta_0(G(\circ))$.*

Proof. [4] proposition 7.1. □

Lemma 2.4. *Assume that $G(\circ)$, $G(*)$ are two isomorphic groups of order $n > 7$ satisfying $dist(G(\circ), G(*)) \leq 6n-18$. Then we have $1_{G(\circ)} = 1_{G(*)}$.*

Proof. Let $e = 1_{G(\circ)}$, $f = 1_{G(*)}$. Assume that $e \neq f$. We would like to prove that $d = dist(G(\circ), G(*)) > 6n-18$.

Put $E = \{(a,b) \in G \times G;\ \{e, f\} \cap \{a, b\} \neq \emptyset\}$. We show that $a \circ b \neq a * b$ for any $(a,b) \in E$. When $a = e$, we have $a \circ b = b$, and $a * b \neq b$, since $a \neq f$. All remaining cases follow from symmetry.

For any $a \in G$ denote by a^{-1}, a^* the inverse element of a in $G(\circ)$, $G(*)$, respectively. Define $I = \{a \in G;\ a^{-1} = a^*\}$.

We prove that $d(a) \geq 4$ for any $a \in I$, $a \notin \{e, f\}$. Let $M = \langle e,\ f,\ a^{-1},\ a^{-1} \circ f\rangle$ be an ordered set. Note that all elements of M are distinct. Hence also $a \circ M = \langle a,\ a \circ f,\ e,\ f\rangle$ and $a * M = \langle a * e,\ a,\ f,\ a * (a^{-1} \circ f)\rangle$ are four-element sets. Moreover, each two respective elements of $a \circ M$ and $a * M$ are different.

If $a \notin I$ and $b \in G$ are such that $a \circ b = a * b = c$, we have $a^* \circ c \neq a^* * c$. Otherwise $b = a^* * a * b = a^* * c = a^* \circ c \neq a^{-1} \circ c = b$, a contradiction. This means that $d(a) + d(a^*) \geq n$ for any $a \notin I$.

Let $i = |I|$. We need to consider three possible cases.

(i) Let $e \notin I$, $f \notin I$. If $i \geq n-4$, we have $d \geq 4(n-4)+2n = 6n-16 > 6n-18$. On the other hand, if $i \leq n-5$, then $d \geq (n-i)n/2 + 4i = n^2/2 + i(4-n/2)$. Since $n > 7$, we can conclude that $d \geq n^2/2 + (n-5)(4-n/2) = 13n/2 - 20 > 6n-18$.

(ii) Let $|\{e, f\} \cap I| = 1$. If $i \geq n-3$, then again (however, the reason is different) $d \geq 4(n-4)+2n$. For $i \leq n-4$, one can see that $d \geq (n-i)n/2 + 4(i-1) + n = n^2/2 + i(4-n/2) - 4 + n \geq n^2/2 + (n-4)(4-n/2) - 4 + n = 7n - 20 > 6n - 18$.

(iii) Finally, let $\{e, f\} \subseteq I$. If $i \geq n-2$, we have $d \geq 4(n-4)+2n$. If $i \leq n-3$, then $d \geq (n-i)n/2 + 4(i-2) + 2n = n^2/2 + i(4-n/2) - 8 + 2n \geq n^2/2 + (n-3)(4-n/2) - 8 + 2n = 15n/2 - 20 > 6n - 18$.

This proof can be found in [9]. □

Unfortunately, also some use of computers is needed in two special cases.

3. Basic estimates

From now on suppose that $G(\circ)$, $G(*)$ are two distinct groups of prime order $p > 7$. Let us denote by H the set of all rows in multiplication table of $G(\circ)$ at which operations $\circ$ and $*$ completely agree, i.e. $H = \{g \in G; d(g) = 0\}$. Assume that H is not empty, and a, b belong to H. Then $(a*b)\circ g = (a\circ b)\circ g = a\circ(b\circ g) = a \circ (b * g) = a * (b * g) = (a * b) * g = (a \circ b) * g$, which shows that H is a common subgroup of $G(\circ)$ and $G(*)$.

According to lemma 2.4, H is never empty, when $dist(G(\circ), G(*)) < 6p - 18$. Because there are no non-trivial subgroups in $\mathbb{Z}_p$, H must be the one element subgroup $1 = 1_{G(\circ)} = 1_{G(*)}$, since $G(\circ)$, $G(*)$ are distinct.

Put $m = min\{d(g); g \neq 1\}$. We know that $m > 0$. The case $m = 1$ is impossible, hence $m > 1$. In fact, as the following lemma shows, $m > 2$.

Lemma 3.1. *Let $G(\circ)$, $G(*)$ be two groups of odd order n. Then $d(g) \neq 2$ for any $g \in G$.*

Proof. Let $\pi : G \longrightarrow G$ be a left translation by g in $G(\circ)$, and $\sigma : G \longrightarrow G$ a left translation by g in $G(*)$. Then $g \circ a \neq g * a$ if and only if $\pi(a) \neq \sigma(a)$, i.e. $\pi^{-1} \circ \sigma(a) \neq a$.

Suppose that $d(g) = 2$. This means that $\pi^{-1} \circ \sigma$ is a transposition. In particular, $sgn(\pi^{-1} \circ \sigma) = -1$. But $sgn(\pi) = sgn(\pi)^n = sgn(\pi^n) = sgn(id) = 1$, and a similar argument shows that also $sgn(\sigma) = 1$, a contradiction. □

Suppose, for a while, that $m \geq 6$. Then $dist(G(\circ), G(*)) \geq 6(n-1) > 6n - 18$, and we can see that this case is not interesting.

Some additional theory is needed for $m = 3, 4, 5$.

We use symbol $\lceil x \rceil$ to denote the smallest integer k such that $x \leq k$.

Proposition 3.2. *Let $G(\circ)$, $G(*)$ be two distinct groups of order $n \geq 5$. Then either $dist(G(\circ), G(*)) \geq \delta_0(G(\circ))$, or*

$$dist(G(\circ), G(*)) \geq \lceil n/4 \rceil \lceil n/3 \rceil + (n - \lceil n/4 \rceil - 1)m.$$

Proof. Put $K = \{a \in G; d(a) < n/3\}$.

(i) Suppose that $|K| > 3n/4$. By 2.2 there is an isomorphism $f : G(\circ) \longrightarrow G(*)$ such that $f(a) = a$ for each $a \in K$. If $n < 12$, then we have $|K| > 3n/4 > n - 3$. Therefore f must be a transposition, and $dist(G(\circ), G(*)) = m_f \geq \delta_0(G(\circ))$ follows by 2.3. If $n \geq 12$, then $dist(G(\circ), G(*)) \geq \delta_0(G(\circ))$ follows at once from 2.3, because $n > |K| > 3n/4 > 2n/3$.

(ii) Now, let $|K| \leq 3n/4$. We show that there are at least $\lceil n/4 \rceil$ elements g with $d(g) \geq \lceil n/3 \rceil$. Assume the contrary, i.e. assume that there are at least $n - \lceil n/4 \rceil + 1$ elements g with $d(g) < \lceil n/3 \rceil$, so also with $d(g) < n/3$. However, $n - \lceil n/4 \rceil + 1 > 3n/4$, a contradiction with $|K| \leq 3n/4$. □

Proposition 3.3. *Let $G(\circ)$, $G(*)$ be as in previous proposition. Let's choose $h \in G$ such that $d(h) = m$, and $h_0, \dots, h_{m-1}$ are pairwise different elements satisfying $h \circ h_i \neq h * h_i$ for $i = 0, \dots, m-1$. Further suppose there is an l-element subset Y of $\{h_0, \dots, h_{m-1}\}$ such that $Y \cap h \circ Y = \emptyset$. Then either $dist(G(\circ), G(*)) \geq 6n - 18$, or we get*

(1) $\quad dist(G(\circ), G(*)) \geq l(n - m) + (n - 2l - 1)m$, *and*

(2) $\quad dist(G(\circ), G(*)) \geq l(n - m) + (\lceil n/4 \rceil - 2l)\lceil n/3 \rceil + (n - \lceil n/4 \rceil - 1)m$,

provided $\lceil n/4 \rceil - 2l \geq 0$.

Proof. Let us keep the notation of 3.2. If $|K| > 3n/4$, then $dist(G(\circ), G(*)) \geq \delta_0(G(\circ))$ follows in the same way as in 3.2. When $|K| \leq 3n/4$, we have at least $\lceil n/4 \rceil$ elements $g \in G$ for which $d(g) \geq \lceil n/3 \rceil$. Without loss of generality, put $Y = \{h_0, \dots, h_{l-1}\}$. According to 2.1, we get

$$d(h) + d(h_i) + d(h \circ h_i) \geq n, \text{or in other words}$$
$$d(h_i) + d(h \circ h_i) \geq n - m \text{ for each } i = 0, \dots, l-1.$$

This immediately proves (1). In order to prove (2), notice there are at least $\lceil n/4 \rceil - 2l$ rows in K not belonging to $Y \cup h \circ Y$. □

Corollary 3.4. *When $G(\circ)$ is a group of prime order $p > 31$, then $\delta(G(\circ)) = 6p - 18$.*

Proof. Let $G(*)$ be the nearest group to $G(\circ)$. Since $m \geq 3$, it is easy to see that we can always find a set Y (from 3.3) such that it has at least two elements. Inequality (2) gives

$$dist(G(\circ), G(*)) \geq 2(p - m) + (\lceil p/4 \rceil - 4)\lceil p/3 \rceil + (p - \lceil p/4 \rceil - 1)m.$$

Observe that its right hand side is increasing in m. For $m = 3$ we obtain

$$dist(G(\circ), G(*)) \geq 5p - 9 + (\lceil p/4 \rceil - 4)\lceil p/3 \rceil - 3\lceil p/4 \rceil,$$

and one can check that the expression on the r.h.s. is for $p > 31$ always greater than $6p - 18$ (consider p in form $12r + s$, say). □

4. Case $m = 5$

Estimate (1) from 3.3 turns out to be strong enough when $m = 5$. Let us denote, for convenience, the powers of any h in $G(\circ)$ by h^r. For example, $h^2 = h \circ h$.

Lemma 4.1. *Let $G(\circ)$, $G(*)$ be two distinct groups of prime order $p > 7$, and suppose that $m = 5$. Then $dist(G(\circ), G(*)) \geq 6p - 18$.*

Proof. Denote by h one of the rows for which $d(h) = 5$. Suppose that h^{i_0}, h^{i_1}, h^{i_2}, h^{i_3}, h^{i_4} are pairwise different elements with $h \circ h^{i_j} \neq h * h^{i_j}$, $j = 0, \ldots, 4$, where $i_0 < i_1 < i_2 < i_3 < i_4 < p$. We can suppose that $i_0 > 0$ (otherwise $dist(G(\circ), G(*)) \geq 6p - 18$ follows from 2.4).

We would like to find a 3-element subset Y of $\{h^{i_0}, h^{i_1}, h^{i_2}, h^{i_3}, h^{i_4}\}$ satisfying $Y \cap h \circ Y = \emptyset$. Clearly, $h^{i_0+1} \neq h^{i_2}$, h^{i_4}. As $i_0 > 0$, we have also h^{i_2+1}, $h^{i_4+1} \neq h^{i_0}$. Finally, $h^{i_2+1} \neq h^{i_4}$, and $Y = \{h^{i_0}, h^{i_2}, h^{i_4}\}$ is such a subset. By (1) we know that

$$dist(G(\circ), G(*)) \geq 3(p - 5) + (p - 7)5 = 8p - 50,$$

and $8p - 50$ is less than $6p - 18$ only when $p < 16$, i.e. $p \leq 13$.

But when $p \leq 13$ we have $dist(G(\circ), G(*)) \geq 5p - 5 \geq 6p - 18$. □

5. Cases $m = 4$, $m = 3$

Proposition 5.1. *For any two distinct groups $G(\circ)$, $G(*)$ of prime order $p > 19$ with $m = 4$ we have $dist(G(\circ), G(*)) \geq 6p - 18$.*

Proof. Assume there is a 3-element subset Y from 3.3. Then (1) yields

$$dist(G(\circ), G(*)) \geq 3(p - 4) + (p - 7)4 = 7p - 40,$$

and $7p - 40$ is less than $6p - 18$ only when $p < 22$, i.e. $p \leq 19$. We cannot improve this result by using estimate (2), since $\lceil p/4 \rceil \geq 2l = 6$ if and only if $p \geq 21$.

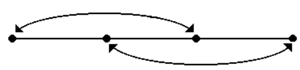
It is not always feasible to find a 3-element subset Y of $\{h^{i_0}, h^{i_1}, h^{i_2}, h^{i_3}\}$ with $Y \cap h \circ Y = \emptyset$. One can show by tedious elementary methods that this is not feasible if and only if $i_1 = i_0 + 1$ and $i_3 = i_2 + 1$. However, in such a case we can show that the transposition $f = (h^{i_1}, h^{i_3})$ is an isomorphism of $G(\circ)$ onto $G(*)$ (detailed proofs are given in [9] 4.18, 4.19). Our wanted estimate then follows from 2.3. □

There is no such estimate for $m = 3$. We need more information about the group operation $*$.

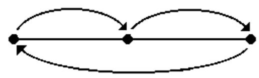
Lemma 5.2. *Let $G(\circ)$, $G(*)$ be two groups of odd order n, and let h be a common generator of $G(\circ)$, $G(*)$ with $d(h) = 4$. Denote by h^{i_0}, h^{i_1}, h^{i_2}, h^{i_3} the pairwise different elements for which $h \circ h^{i_j} \neq h * h^{i_j}$, $j = 0, \ldots, 3$, where $i_0 < i_1 < i_2 < i_3$. Then $h * h^{i_0} = h \circ h^{i_2}$, $h * h^{i_2} = h \circ h^{i_0}$, $h * h^{i_1} = h \circ h^{i_3}$, and $h * h^{i_3} = h \circ h^{i_1}$*

Proof. Let π, σ be as in the proof of 3.1. Then $\pi^{-1} \circ \sigma$ is either a 4-cycle, or a composition of two independent transpositions. In fact, $\pi^{-1} \circ \sigma$ cannot be a 4-cycle, because $sgn(\pi^{-1} \circ \sigma) = 1$. It is not difficult to observe that $\pi^{-1} \circ \sigma$ must be a permutation $(i_0, i_2)(i_1, i_3)$. □

We can depict the situation as follows:



For $m = 3$, the appropriate picture is (without proof):



Now we have enough information to write efficient computer programs in order to solve all remaining cases — we only need to consider situations when $m = 4$ and $7 < p < 19$, or $m = 3$ and $7 < p < 31$.

We will not give a concrete implementation of requested algorithms (which can be found in [9]), but we describe these algorithms in words instead.

Suppose that p is a prime between 7 and 19. We would like to modify the canonical multiplication table of $\mathbb{Z}_p = G(\circ)$ in all possible ways, such that the resulting table will be a multiplication table of some group $G(*)$ satisfying $m = 4$ (the other case $m = 3$ is similar), and then check that $dist(G(\circ), G(*)) \geq 6p - 18$.

By lemma 2.4, the first row and the first column of $G(\circ)$ remain unchanged. We choose some row $h \neq 0$ in G and modify it at four places $0 < i_0 < i_1 < i_2 < i_3 < p$. According to 5.2, this modification is given by permutation $(i_0, i_2)(i_1, i_3)$, otherwise we never get a group multiplication table.

It is worth to point out that we do not need to go through all choices of $h \in G$. In fact, we can fix only one row (a detailed explanation of this fact can be found in [9], 4.1). This trick speeds up the algorithm $p - 1$ times, and hence it is not essential.

Once we know one row of multiplication table of $G(*)$, we can build up $G(*)$ fully, because each non-zero element of $\mathbb{Z}_p$ is a generator.

6. Main result

The algorithm described in section 5 does not find any pair of groups $G(\circ)$, $G(*)$ with $dist(G(\circ), G(*)) < 6p - 18$, which, together with all previous results, means that:

Theorem 6.1. *Each group of prime order $p > 7$ has Cayley stability equal to $6p - 18$.*

Note that there are two groups $G(\circ)$, $G(*)$ of order 7 with $d(G(\circ), G(*)) = 18 < 24$ — consider isomorphism $f : G(\circ) \longrightarrow G(*)$ given by

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 \end{pmatrix},$$

so the estimate $p > 7$ in 6.1 cannot be improved. These two groups are the nearest possible groups of order 7 — in other words, $\delta(\mathbb{Z}_7) = 18$.

It is easy to check that $\delta(\mathbb{Z}_2) = 4$ and $\delta(\mathbb{Z}_3) = 9$. Computation reveals that $\delta(\mathbb{Z}_5) = 12$. Here, the group nearest to $\mathbb{Z}_5$ is obtained via transposition (2, 3), for example.

References

[1] J. Dénes, *On problem of L. Fuchs*, Acta Sci. Math. (Szeged) **23** (1962), 237–241

[2] J. Dénes, A. D. Keedwell, *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest, 1974.

[3] Diane Donnovan, Sheila Oates-Williams, Cheryl E. Praeger, *On the Distance between Distinct Group Latin Squares*, Journal of Comb. Designs **5** (1997), 235–248.

[4] Aleš Drápal, *How Far Apart Can the Group Multiplication Tables be?*, European Journal of Combinatorics **13** (1992), Academic Press Limited, 335–343
[5] ———, *On Distances of Multiplication Tables of Groups*, (to appear).
[6] ———, *Non-isomorphic groups coincide at most in three quarters of their multiplication tables*, (to appear).
[7] S. Frische, *Lateinische Quadrate*, diploma thesis, Vienna, 1988
[8] L. Fuchs, *Abelian Groups*, Akadémiai Kiadó, Budapest, 1958
[9] Petr Vojtěchovský, *On Hamming Distances of Groups*, Master Degree thesis (in Czech), Charles University, 1998

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, Prague, Czech Republic

Current address: Department of Mathematics, Iowa State University, Ames, IA, U.S.A.

E-mail address: `petr@iastate.edu`