Acta Sci. Math. (Szeged) 63 (1997) 341–351

ON THE MINIMAL DISTANCE BETWEEN GROUP TABLES

Sophie Frisch

Abstract. We examine the minimal distance (number of differing entries) between different group tables of the same order n. Here group table means a matrix of order n with entries from a fixed set of n symbols, which (with suitable border elements) is the multiplication table of a group. (The border elements are not considered part of the table. A group is defined up to isomorphism by its multiplication table without border elements.) With the exception of some pairs of groups of orders 4 and 6, which are listed explicitly, different group tables of order n differ in at least $2n$ places; and with the exception of some pairs of groups of orders 4, 6, 8 and 9, which are listed explicitly, tables of non-isomorphic groups of order n always differ in strictly more than $2n$ places.

1. Introduction

We use the notion of group table, or Cayley table of a group, that is set forth in [2]: for every natural number n we consider all binary operations defined on the set $\underline{n} = \{1, \ldots, n\}$ that satisfy the group axioms; a group table is a multiplication table of such a group $(\underline{n}, \cdot)$. By the existence of an identity, some column contains the elements in the same order as they appear on the vertical border of the table and some row is equal to the horizontal border. The border is not regarded as part of the table, however. The abstract group defined (up to isomorphism) by the multiplication table is uniquely determined by the remaining $n \times n$ matrix, since any row and column can be used as borders: the resulting operations define isomorphic groups. A group table is necessarily a *Latin square*, that is, a matrix whose every row and every column contains every symbol from $\underline{n}$ exactly once. Given a group table $A = (a_{i,j})$ of order n, the set of all tables arising from the same abstract group is the orbit of A under $S_n \times S_n \times S_n$, acting on Latin squares by permuting rows, columns and names of entries: $(\pi, \sigma, \rho)A = (a'_{i,j})$ with $a'_{i,j} = \rho(a_{\pi(i),\sigma(j)})$.

In [1] J. Dénes investigates how many entries can be deleted from a group table such that it remains uniquely reconstructible, and claims [1; Theorem 1 and Corollary] that two arbitrary group tables of order $n \neq 4$ differ in at least

1991 Mathematics Subject Classification: 05B15, 20N05, 20A99.

$2n$ places. In contrast to this we exhibit a pair of tables of the cyclic group of order 6 of distance 9 (By "distance," we always mean Hamming distance, or number of differing entries.).

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ 4 & 5 & 6 & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ 5 & 6 & 4 & \mathbf{3} & \mathbf{1} & \mathbf{2} \\ 6 & 4 & 5 & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{array} \qquad \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ 4 & 5 & 6 & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ 5 & 6 & 4 & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ 6 & 4 & 5 & \mathbf{3} & \mathbf{1} & \mathbf{2} \end{array}$$

Dénes makes two statements: 1) two different group tables of the same group G of order n differ in at least $2n$ places [1; Lemma 2], and, 2) group tables of non-isomorphic groups of order $n \neq 4$ differ in at least $2n$ places [1; Lemma 3]. These are reproduced in [2] and also in [3], where 1) is acknowledged to be false, but no corrected version is given. While 1) is incorrect, (Dénes' proof wrongly assumes that any table of a group can be transformed into any other by permuting rows and columns), 2) is correct and its proof can be adapted to cover the case of different tables of the same group. We shall show that exceptions to 1) occur only between tables of the cyclic group of order 4 and between tables of the cyclic group of order 6. By suggestion of the referee we will also classify all pairs of non-isomorphic groups that admit tables of distance $2n$ or less. Note that every group of order $n > 1$ has tables that differ in exactly $2n$ places: one can get such, for instance, by interchanging two rows in a table.

2. Results.

Theorem 1. *Different tables of groups of order n differ in at least $2n$ places, except for the following three pairs of groups, for which we give the minimal distance between different tables below:*

$\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$: minimal distance 4,

$\mathbb{Z}_4$ and $\mathbb{Z}_4$: minimal distance 7,

$\mathbb{Z}_6$ and $\mathbb{Z}_6$: minimal distance 8.

Corollary. *Different tables of groups of order $n \notin \{4, 6\}$ differ in at least $2n$ places.*

Theorem 2. *Tables of non-isomorphic groups of order n always differ in strictly more than $2n$ places, except for the pair $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ that has tables of distance 4 and the following pairs of groups, for which the minimal distance between tables is $2n$:*

$\mathbb{Z}_6$ and D_3; $\mathbb{Z}_8$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$; any pair of non-cyclic groups of order 8; and $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Corollary. *Tables of non-isomorphic groups of order $n > 9$ differ in more than $2n$ places.*

Tables of groups of order n of distance less than $2n$

Tables of $\mathbb{Z}_2 \times \mathbb{Z}_2$ (left) and $\mathbb{Z}_4$ (the other three tables), where the table of $\mathbb{Z}_2 \times \mathbb{Z}_2$ is of distance 4 from each table of $\mathbb{Z}_4$, while different tables of $\mathbb{Z}_4$ differ in 7 places (these are all possible group tables of order 4 with first row and first column in natural order):

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
2	1	4	3
3	4	2	1
4	3	1	2

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

Two tables of $\mathbb{Z}_6$ of distance 8:

1	2	3	4	5	6
2	1	4	3	6	5
3	4	**6**	**5**	1	2
4	3	**5**	**6**	2	1
5	6	1	2	**4**	**3**
6	5	2	1	**3**	**4**

1	2	3	4	5	6
2	1	4	3	6	5
3	4	**5**	**6**	1	2
4	3	**6**	**5**	2	1
5	6	1	2	**3**	**4**
6	5	2	1	**4**	**3**

Tables of non-isomorphic groups of distance $2n$

Tables of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (upper left), Q_8 (upper right), $\mathbb{Z}_2 \times \mathbb{Z}_4$ (lower left) and D_4 (lower right) of distance 16 from each other. (Differences from the table of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are marked):

1	2	3	4	5	6	7	8
2	1	4	3	6	5	8	7
3	4	1	2	7	8	5	6
4	3	2	1	8	7	6	5
5	6	7	8	1	2	3	4
6	5	8	7	2	1	4	3
7	8	5	6	3	4	1	2
8	7	6	5	4	3	2	1

2	**1**	3	4	5	6	7	8
1	**2**	4	3	6	5	8	7
3	4	1	2	7	8	**6**	**5**
4	3	2	1	8	7	**5**	**6**
5	6	**8**	**7**	1	2	3	4
6	5	**7**	**8**	2	1	4	3
7	8	5	6	**4**	**3**	1	2
8	7	6	5	**3**	**4**	2	1

2	**1**	3	4	5	6	7	8
1	**2**	4	3	6	5	8	7
3	4	1	2	7	8	**6**	**5**
4	3	2	1	8	7	**5**	**6**
5	6	7	8	**2**	**1**	3	4
6	5	8	7	**1**	**2**	4	3
7	8	**6**	**5**	3	4	1	2
8	7	**5**	**6**	4	3	2	1

2	**1**	3	4	5	6	**8**	**7**
1	**2**	4	3	6	5	**7**	**8**
4	**3**	1	2	7	8	**6**	**5**
3	**4**	2	1	8	7	**5**	**6**
5	6	7	8	1	2	3	4
6	5	8	7	2	1	4	3
7	8	5	6	3	4	1	2
8	7	6	5	4	3	2	1

Tables of D_3 (left) and $\mathbb{Z}_6$ of distance 12:

1	2	3	4	5	6
2	3	1	6	4	5
3	1	2	5	6	4
4	**5**	**6**	**1**	**2**	3
5	**6**	**4**	**3**	**1**	2
6	**4**	**5**	**2**	**3**	1

1	2	3	4	5	6
2	3	1	6	4	5
3	1	2	5	6	4
4	**6**	**5**	**2**	**1**	3
5	**4**	**6**	**1**	**3**	2
6	**5**	**4**	**3**	**2**	1

Tables of $\mathbb{Z}_8$ (left) and $\mathbb{Z}_2 \times \mathbb{Z}_4$ of distance 16:

1	2	3	4	5	6	7	8
2	1	4	3	6	5	8	7
3	4	2	1	7	8	6	5
4	3	1	2	8	7	5	6
5	6	7	8	**3**	**4**	**2**	**1**
6	5	8	7	**4**	**3**	**1**	**2**
7	8	6	5	**2**	**1**	**4**	**3**
8	7	5	6	**1**	**2**	**3**	**4**

1	2	3	4	5	6	7	8
2	1	4	3	6	5	8	7
3	4	2	1	7	8	6	5
4	3	1	2	8	7	5	6
5	6	7	8	**1**	**2**	**3**	**4**
6	5	8	7	**2**	**1**	**4**	**3**
7	8	6	5	**3**	**4**	**2**	**1**
8	7	5	6	**4**	**3**	**1**	**2**

Tables of $\mathbb{Z}_3 \times \mathbb{Z}_3$ (left) and $\mathbb{Z}_9$ of distance 18:

1	2	3	4	5	6	7	8	9
2	3	1	5	6	4	8	9	7
3	1	2	6	4	5	9	7	8
4	5	6	**7**	**8**	**9**	1	2	3
5	6	4	**8**	**9**	**7**	2	3	1
6	4	5	**9**	**7**	**8**	3	1	2
7	8	9	1	2	3	**4**	**5**	**6**
8	9	7	2	3	1	**5**	**6**	**4**
9	7	8	3	1	2	**6**	**4**	**5**

1	2	3	4	5	6	7	8	9
2	3	1	5	6	4	8	9	7
3	1	2	6	4	5	9	7	8
4	5	6	**8**	**9**	**7**	1	2	3
5	6	4	**9**	**7**	**8**	2	3	1
6	4	5	**7**	**8**	**9**	3	1	2
7	8	9	1	2	3	**6**	**4**	**5**
8	9	7	2	3	1	**4**	**5**	**6**
9	7	8	3	1	2	**5**	**6**	**4**

3. A few Lemmata.

Lemma 1. *Let A and A' be group tables of order n such that some pair of corresponding rows is of distance d. If every pair of corresponding rows is of distance less than $\frac{n-d}{3}$ then the groups are isomorphic.*

Proof. Let A and A' be tables of groups G and G' as indicated, of distance d in row x. Let π be the permutation that, applied to the columns of A, would arrange the elements in row x in the same order as they appear in row x of in A', then π moves exactly d letters. Viewed as a permutation of the elements in row x of A', the i-th row of A is $\psi_i\pi$ and the i-th row of A' is φ_i, where $P' = \{\varphi_1, \ldots, \varphi_n\}$ is a regular permutation representation of G' and $P = \{\psi_1, \ldots, \psi_n\}$ is one of G. We claim that $f\colon P \longrightarrow P'$, $f(\psi_i) = \varphi_i$ is an isomorphisms of groups. Since φ_i differs from $\psi_i\pi$ and φ_j from $\psi_j\pi$ in less than $(n-d)/3$ places each, $\varphi_i\varphi_j^{-1}$ differs from $\psi_i\psi_j^{-1} = \psi_i\pi(\psi_j\pi)^{-1}$ in less than $2(n-d)/3$ places. Therefore $\varphi_i\varphi_j^{-1}$, which occurs in some row of A', differs from $\psi_i\psi_j^{-1}\pi$, which occurs in some row of A, in $e < d + 2(n-d)/3$ places.

Since $\psi_i\psi_j^{-1}\pi$ has $n - e > (n-d)/3$ values in common with $\varphi_i\varphi_j^{-1}$ these elements must occupy corresponding rows, since $\psi_i\psi_j^{-1}\pi$ would differ from every other element of P' in at least $n - e > (n-d)/3$ places, and we know that corresponding rows are of distance less than $(n-d)/3$. This means $f(\psi_i\psi_j^{-1}) = \varphi_i\varphi_j^{-1}$ for all i, j. Now it is an easy exercise that every function between groups that satisfies $f(ab^{-1}) = f(a)f(b)^{-1}$ is a homomorphism. $\square$

Regular permutations of small distance. Consider multiplying a permutation φ from the left by a permutation π that fixes all but a few letters, $\pi\varphi = \psi$. Every letter whose image under φ is not moved by π has the same image under ψ, and every letter that is not moved by π has the same pre-image under ψ as under φ. Therefore every block of letters in the cycle representation of φ starting with a letter x moved by π and reaching up to the next letter moved by π also occurs as a block of adjacent letters in the cycle representation of ψ. We can multiply φ by π by considering only the letters moved by π and treating each block $\bar{x}$ (starting with the letter x moved by π) just like the letter x. Cycles of φ that do not contain elements moved by π of course remain completely unchanged. We illustrate this by an example:

$$(a\,b\,c\,d)\cdot(a\,b\,c)(d) = (a\,c\,b\,d), \quad \text{therefore} \quad (a\,b\,c\,d)\cdot(\bar{a}\,\bar{b}\,\bar{c})(\bar{d})\,\langle\ldots\rangle = (\bar{a}\,\bar{c}\,\bar{b}\,\bar{d})\,\langle\ldots\rangle,$$

where $\bar{x}$ represents the block of digits starting with x and $\langle\ldots\rangle$ stands for possible additional cycles not containing any of the letters moved by $\pi = (a\,b\,c\,d)$.

(For multiplication with π from the right, one uses the blocks of letters that end with a letter moved by π, beginning just after the previous occurrence of a letter moved by π in each cycle of φ.)

Lemma 2. *Here $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$ represent non-empty blocks of digits, and $\langle\ldots\rangle$ denotes possible additional cycles, which the permutations in question have in common. The pairs of regular permutations are unordered pairs.*
(I) Every pair of regular permutations of distance 2 is of the form $(\bar{a})(\bar{b})$ and $(\bar{a}\,\bar{b})$, where $\bar{a}$ and $\bar{b}$ are blocks equal length (and therefore $2 \mid n$).

(II) Every pair of regular permutations of distance 3 is of the form
(1) $(\bar{a}\,\bar{b}\,\bar{c})\langle\ldots\rangle$ and $(\bar{a}\,\bar{c}\,\bar{b})\langle\ldots\rangle$ or
(2) $(\bar{a})(\bar{b})(\bar{c})$ and $(\bar{a}\,\bar{b}\,\bar{c})$ (in which case $3 \mid n$).

(III) Every pair of regular permutations φ and ψ, where $\varphi = \pi\psi$ with π a product of two disjoint transpositions, is of one of the following types
(1) $(\bar{a})(\bar{b})(\bar{c})(\bar{d})$ *and* $(\bar{a}\,\bar{b})(\bar{c}\,\bar{d})$ *(in which case* $4 \mid n$*)*
(2) $(\bar{a}\,\bar{c})(\bar{b}\,\bar{d})\langle\ldots\rangle$ *and* $(\bar{a}\,\bar{d})(\bar{b}\,\bar{c})\langle\ldots\rangle$
(3) $(\bar{a}\,\bar{c}\,\bar{b}\,\bar{d})\langle\ldots\rangle$ *and* $(\bar{a}\,\bar{d}\,\bar{b}\,\bar{c})\langle\ldots\rangle$
(4) $(\bar{a})(\bar{b}\,\bar{c})(\bar{d})$ *and* $(\bar{a}\,\bar{b}\,\bar{d}\,\bar{c})$ *(in which case* $3 \mid n$*).*

(IV) Every pair of regular permutations φ and ψ, where $\varphi = \pi\psi$ with π a 4-cycle, is of one of the following types
(1) $(\bar{a})(\bar{b})(\bar{c})(\bar{d})$ *and* $(\bar{a}\,\bar{b}\,\bar{c}\,\bar{d})$ *(in which case* $4 \mid n$*)*
(2) $(\bar{a}\,\bar{b}\,\bar{c}\,\bar{d})$ *and* $(\bar{a}\,\bar{c})(\bar{b}\,\bar{d})$
(3) $(\bar{a}\,\bar{b}\,\bar{c})(\bar{d})$ *and* $(\bar{a}\,\bar{c}\,\bar{b}\,\bar{d})$
(4) $(\bar{a}\,\bar{b})(\bar{c}\,\bar{d})$ *and* $(\bar{a}\,\bar{c})(\bar{b})(\bar{d})$ *(in which case* $6 \mid n$*).*

Sketch of proof. We discuss case III, the others are similar. Consider all products $(a\,b)(c\,d)\varphi = \psi$, where φ runs through all elements of the symmetric group on the letters a, b, c and d. If we replace these letters by $\bar{a}$, $\bar{b}$, $\bar{c}$ and $\bar{d}$, respectively, in the cycles of φ and ψ and represent possible additional cycles which remain unchanged by $\langle\ldots\rangle$, we get a list of all possible ways in which multiplication by $(a\,b)(c\,d)$ from the left can transform a permutation $\bar{\varphi}$ into another permutation $\bar{\psi}$. We identify the cases that only differ by a renaming of letters or by interchanging $\bar{\varphi}$ and $\bar{\psi}$.

We omit the cases that are incompatible with the requirement that φ and ψ be regular, such as $(a\,b)(c\,d) \cdot (\bar{a}\,\bar{b})(\bar{c})(\bar{d})\,\langle\ldots\rangle = (\bar{a})(\bar{b})(\bar{c}\,\bar{d})\,\langle\ldots\rangle$. (If φ is regular, the length of $\bar{a}$ is smaller than that of $\bar{c}$, and greater if ψ is regular.)

We also omit the mention of additional cycles $\langle\ldots\rangle$ common to $\bar{\varphi}$ and $\bar{\psi}$, if the length of cycles is different in φ and ψ, since common cycles cannot exist between regular permutations of different cycle lengths. In this way we arrive at the list of types given. □

We have already displayed group tables of the distances claimed to be minimal in the exceptional cases of Theorems 1 and 2. It now remains to show that group tables of order n differ in at least $2n$ places, unless the groups are listed in Theorem 1 as an exception, (in which case we must show that the distance is at least the claimed minimum); and further, that tables of order n and distance $2n$ belong to isomorphic groups or to one of the pairs of non-isomorphic groups listed in Theorem 2.

To avoid unnecessary clutter in a proof that is already fraught with case distinctions, we relegate some of the computational details to a separate section following the body of the proof.

4. Proof of the Theorems.

Let A and A' be tables of groups G and G' of order n. For $n = 1$ or 2 the assertions are evident; we assume $n \geq 3$.

Case I: *A and A' differ in every row and every column.*
Since two different permutations differ in at least 2 places, A and A' differ in at least $2n$ places. If there are exactly $2n$ differences, then every pair of corresponding rows is of distance 2 (and similarly for the columns) and Lemma 1 implies that the groups are isomorphic if $n > 8$. Also, $2n$ is greater or equal than the minimal distance claimed for pairs of non-isomorphic groups of order $n < 8$ and for most pairs of non-isomorphic groups of order 8; it only remains to check that $\mathbb{Z}_8$ does not have a table that differs from a table of a non-cyclic group of order 8 other than $\mathbb{Z}_2 \times \mathbb{Z}_4$ in exactly two places in every row and column, see (1) below.

Case II: *A and A' agree in some row or column.*
Suppose A and A' agree in row x. (We talk about rows, but the argument works *mutatis mutandis* for columns.) The rows of A and A', interpreted as permutations of the elements in row x, give regular permutation representations $P = \{\varphi_1, \dots, \varphi_n\}$ of G and $P' = \{\psi_1, \dots, \psi_n\}$ of G'. Let $H = P \cap P'$. If the elements of H do not each occur in the same row in both tables then we can permute the rows of one table to bring matching elements into corresponding rows without increasing the distance of the tables: Consider the rows where either A or A' has an element of H and the other table has something different; then the number of differences between A and A' in each of these rows is n, so permuting them cannot increase the distance. We may therefore assume that every element of H occurs in the same position in both tables. Now let s be the number of rows in which A and A' agree, then $s = |H|$ and in particular $s \mid n$.

Two Latin squares of order 3 that have a row in common consist of the same 3 rows in different order and therefore differ at 6 places. All regular permutation groups of order 4 are given by the rows of the four tables of order 4 displayed earlier, the possible distances between tables that agree in a row are easily found by considering the distances between the non-identity permutations of these groups, and we assume $n > 4$ from now on.

Case 1: *There are no rows of distance* 2.
Case 1.1: $s \leq \frac{n}{4}$.
$d(A, A') \geq 3(n - \frac{n}{4}) = \frac{9}{4}n > 2n.$

Case 1.2: $s = \frac{n}{3}$.
In this case, $3 \mid n$. $d(A, A') \geq 3(n - \frac{n}{3}) = 2n$. If all distances between different corresponding rows are 3, then, since there are rows of distance $d = 0$, the groups must be isomorphic by Lemma 1 when $n > 9$. If the tables differ in at least 4 places in some row, then $d(A, A') \geq 3(n - \frac{n}{3}) + 1 > 2n$. (The pairs of non-isomorphic groups of orders 6 and 9 do admit tables of distance $2n$.)

Case 1.3: $s = \frac{n}{2}$.
Note that n is even in this case. Every row of distance d gives elements $\varphi \in P$ and $\psi \in P'$ with $\varphi = \pi\psi$, where π moves exactly d elements $x, y, \dots$ and the cycle representations of φ and ψ contain the same d (non-empty) blocks of digits $\bar{x}$, $\bar{y}, \dots$ in different order, as described in the remark before Lemma 2. If the length of some block is at least 3, say $\bar{x} = x_1 \dots x_k$ with $k \geq 3$, then $\varphi^2(x_1) = \psi^2(x_1)$ while $\varphi^2(x_{k-1}) \neq \psi^2(x_{k-1})$. This is impossible: since the index of H in P' is 2, $\psi^2 \in H = P \cap P'$, so ψ^2 and φ^2 are both elements of the regular permutation group G. Therefore the blocks moved by π must be of length at most 2, which implies $d \geq \frac{n}{2}$. This holds for every row in which A and A' differ, so $d(A, A') \geq \frac{n^2}{4}$. (In general we get, by the same principle, that $d(A, A') \geq (n - s)s$, where $s = |H|$.)

For $n \geq 8$ the distance between A and A' is therefore at least $2n$, and for $n > 8$ it is more than $2n$. We have to check non-isomorphic groups of order 8 and groups of order 6 separately, see (2) and (3).

Case 2: *Rows of distance 2 exist.*
There exist $\varphi = (i_1 \dots i_n) \in P$ and $\sigma = (i_1 \dots i_{n/2})(i_{(n/2)+1} \dots i_n) \in P'$. (Note that n is even in this case, and that at least one of the groups is cyclic.) We have $P = [\varphi]$, $[P' : [\sigma]] = 2$ and $P \cap [\sigma] = \{id\}$ (because every cycle of a nontrivial power of φ contains both i_m with $m \leq n/2$ and i_l with $l > n/2$), therefore $|P \cap P'| \leq 2$. Besides φ^{-1} and σ^{-1} there is no further pair of permutations of this type, when $n \neq 4$. (If $\varphi^k = (j_1 \dots j_n) \in P$, $1 < k < n - 1$, and $\rho = (j_1 \dots j_{n/2})(j_{(n/2)+1} \dots j_n) \in P'$ then each cycle of ρ contains both i_m with $m \leq n/2$ and i_l with $l > n/2$, therefore $[\sigma] \cap [\rho] = \{id\}$, which is impossible if $n \neq 4$.) Only if both P and P' are cyclic can there be an additional pair $(j_1 \dots j_n) \in P'$ and $(j_1 \dots j_{n/2})(j_{(n/2)+1} \dots j_n) \in P$, a maximum of 4 rows of distance 2 in all. We get $d(A, A') \geq 3(n - 6) + 4 \cdot 2 = 3n - 10$, and even $d(A, A') \geq 3(n - 4) + 2 \cdot 2 = 3n - 8$, if not both groups are cyclic. For $n > 8$, this means $d(A, A') > 2n$ for non-isomorphic groups, and $d(A, A') \geq 2n$ for two cyclic groups. It remains to check the cases $n \in \{6, 8\}$, see (4). $\square$

5. The Gory Details

(1) We show that $\mathbb{Z}_8$ does not have a table that differs from a table of a non-cyclic group of order 8 in exactly two places in every row and column. Suppose otherwise. In the first row, the differences are in columns x and y, say. We exchange columns x and y in A and get a table B of G that agrees with A' in the first row. The rows of B and A', considered as permutations of the elements in the first row, form a regular permutation representation $P = \{\varphi_1, \ldots, \varphi_8\}$ of $G = \mathbb{Z}_8$ and $P' = \{\psi_1, \ldots, \psi_8\}$ of G'. Since there are precisely two differences between A and A' in every column, either B and A' agree in one further row, or there are two rows of distance 3. In both cases, ψ_i and φ_i differ by multiplication with a product of two disjoint transpositions in all further rows, $\psi_i = \pi_i \varphi_i$, where $\pi_i = (a_i\, b_i)(c_i\, d_i)$. Among these rows there would be one with φ_i an 8-cycle and ψ_i of some other cycle structure. By Lemma 2, III this is impossible, as $3 \nmid 8$.

(2) We show that there are no tables of $\mathbb{Z}_8$ and a non-cyclic group other than $\mathbb{Z}_2 \times \mathbb{Z}_4$, that agree in four rows and are of distance 4 in each of the remaining rows.

Suppose otherwise. The regular permutation representation of $\mathbb{Z}_8$ consists of the powers of $\varphi = (a_1\, a_2\, b_1\, b_2\, c_1\, c_2\, d_1\, d_2)$, and $H = \{\mathrm{id}, \varphi^2, \varphi^{-2}, \varphi^4\}$. If ψ is a regular permutation of distance 4 from φ then the 4 blocks of digits that occur in different positions in the cycle representation of ψ and φ are each of length 2.

Using Lemma 2, we see that the possible regular permutations of distance 4 from φ are $\alpha = (a_1\, a_2)(b_1\, b_2)(c_1\, c_2)(d_1\, d_2)$, $\beta = (a_1\, d_2)(b_1\, a_2)(c_1\, b_2)(d_1\, c_2)$, $\gamma = (a_1\, a_2\, c_1\, c_2)(b_1\, b_2\, d_1\, d_2)$ and $\delta = (a_1\, b_2\, c_1\, d_2)(b_1\, c_2\, d_1\, a_2)$. For φ^{-1}, the possibilities are exactly the inverses of these permutations. The regular permutations of distance 4 from φ^3 are $\alpha' = (a_1\, b_2)(b_1\, c_2)(a_2\, d_1)(c_1\, d_2)$, $\beta' = (a_1\, c_2)(b_1\, d_2)(c_1\, a_2)(d_1\, b_2)$ and also γ and δ; for φ^{-3} they are the inverses of these elements. $G' \setminus H$ cannot contain only elements of order 4, because $H \cup \{\gamma, \gamma^{-1}, \delta, \delta^{-1}\}$ is not a group. We show that if $G' \setminus H$ contains an element of order 2, it also contains an element of order 4.

If α is in a row with φ, then δ^{-1} or γ^{-1} must be in a row with φ^{-1}, since $\alpha\beta$ cannot occur in a regular permutation group containing φ^2, and similarly for β in a row with φ. (The case of any of the other 8-cycles and an element of order 2 next to it, is up to conjugation the same as the one we considered). Now that G' has more than 2, but less than 6 elements of order 4, it can only be $\mathbb{Z}_2 \times \mathbb{Z}_4$.

(3) Two tables of $\mathbb{Z}_6$ can indeed agree in 3 rows and be of distance 3 each in the remaining rows, as show in an example earlier. By considering a regular permutation representation of D_3 and the possibilities to complete the subgroup of order 3 to a cyclic group of order 6, one checks easily that tables of $\mathbb{Z}_6$ and D_3 that agree in 3 rows differ in exactly 4 places in each of the remaining rows. If two tables of D_3 agree in three rows, the remaining rows are of distance at least 4 each, because the only regular permutation that a product of transpositions could have distance 3 to is a 6-cycle.

(4) Two tables of the cyclic group of order 8 do not admit more than 2 rows of distance 2: If $(1\,2\,3\,4\,5\,6\,7\,8) \in P$, $(1\,2\,3\,4)(5\,6\,7\,8) \in P'$ then there is no 8-cycle in P' of distance 2 to either $(1\,3\,5\,7)(2\,4\,6\,8)$ or $(1\,7\,5\,3)(2\,8\,6\,4)$, because it would have to contain 4 odd numbers in a row, which is incompatible with its square being $(1\,2\,3\,4)(5\,6\,7\,8)$ or $(1\,4\,3\,2)(5\,8\,7\,6)$, so that $d(A, A') \geq 3n - 8$ in this case too. Between a table of $\mathbb{Z}_8$ and one of a non-cyclic group there are at most 2 rows of distance 3, since each would involve one of the elements of order 4 of $\mathbb{Z}_8$, so $d(A, A') \geq 18$.

Tables of $\mathbb{Z}_6$ and D_3 differ by at least 12 entries in the case where rows of distance 2 occur: If there are two rows of distance 2, then there are no rows of distance 3, because every row of distance 3 would either involve a 6-cycle of $\mathbb{Z}_6$ or a product of 3-cycles in D_3, and these are all spent for the rows of distance 2. If there is only one row of distance 2, then the inverses of the elements in this row, which differ in 2 places, and therefore agree in 4, do not occur in the same position and produce two rows of distance 4. Since $|H| \leq 2$, the distances add up to at least 12. Tables of $\mathbb{Z}_6$ of distance $3n - 10 = 8$ do exist, as shown earlier.

References

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

[2] J. Dénes and A. D. Keedwell, *Latin Squares and Their Applications,* Academic Press, New York, 1974.

[3] J. Dénes and A. D. Keedwell, *Latin Squares (New Developments in the Theory and Applications),* North Holland, Amsterdam, 1991.

Institut für Mathematik C
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
e-mail: frisch@blah.math.tu-graz.ac.at