Problem C NAW 5/21 nr. 1 maart 2020

Jaap Spies

April 2020

The problem

Let $n \geq 4$ be an integer and A be an abelian group of order 2^n. Let σ be an automorphism of A such that the order of σ is a power of 2. Then the order of σ is at most 2^{n-2}.

Solution

Let p be prime We will use a well known result, Lemma: A cyclic group of order p^r has an automorfism group of order $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$ where ϕ is Euler's totient function.

Furthermore an abelian group of order n contains an element of order p if p is a prime dividing n.

A finite abelian group is a direct product of its Sylow subgroups. Here we only have $p = 2$, so we know that we can write A as a direct product of cyclic groups C_i:

$A = C_1 \times C_2 \times \cdots C_k$ for some k, with invariants 2^{e_i}, $e_1 = 1$ and $\sum_i e_i = n$.

We arrange $e_1 \leq e_2 \leq \cdots \leq e_k$ and let $e_1 = \cdots = e_r = 1$ for some $r \leq n$.

We associate with each direct product a tuple of the exponents e_i of its invariants: $(e_1, e_2, \cdots, e_k)$ and we arrange the tuples for a fixed n from $(1, n-1)$ down to $(1, 1, \cdots, 1)$ in a partial ordered set. For a fixed n we call the collection of tuples T_n

A representation of T_6:

$$
\begin{array}{ccccc}
 & & (1,5) & & \\
 & \swarrow & & \searrow & \\
 (1,1,4) & & & & (1,2,3) \\
 \downarrow & & \searrow & & \downarrow \\
 (1,1,2,2) & & & & (1,1,1,3) \\
 & \searrow & & \swarrow & \\
 & & (1,1,1,1,2) & & \\
 & & \downarrow & & \\
 & & (1,1,1,1,1,1) & &
\end{array}
$$

For larger n the representations will be more complex!

Now for the most difficult case: $r = n = 4$ with tuple $(1, 1, 1, 1)$. Show there is no automorphism σ of order $2^3 = 8$.

Let $\{b_i\}$ be a basis of A. All b_i are of order 2. A permutation of the b_i corresponds to an automorphism of A. We will use some graph theory here. We only consider derangements, no b_i is taken to itself. The number of derangements is $D_4 = per((J_4 - I_4)$, the permanent of a square matrix with 0's on the diagonal and 1's elsewhere. This permanent can be calculated with the Formula of Spies if you like :-) (see [2]): $D_4 = 9$. More general you get (see [3])

$$D_n = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^r (n-r-1)^{n-r}$$

We have permutations P_i with $1 \leq i \leq 9$. As we can easily see all permutations/automorphisms are of order at most $2^2 = 4$. See for example the cycle $b_1 \to b_2 \to b_3 \to b_4 \to b_1$ is of order 4. With permutation matrix:

$$P_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

For $n = 5$, $n = 6$ and $n = 7$ there are no cycles of length power of 2 other than of maximal order 4. If $n = 8$ we can make cycles of length at most $2^3 = 8$. If the order of automorphism σ is a power of 2, then the order is strictly less than $2^{n-2} = 2^6$.

This reasoning can be repeated for higher values of n.

To finish the case $n = 4$, we observe that tuple $(1, 3)$ leads with Lemma 1 to an order $2^2 = 4$ of the automorphism group. With elementary counting the tuple $(1, 1, 2)$ leads to order $2 \cdot 2 = 4$ for our σ.

Under the assumption that the order of σ is 2^u for some u we define functions $O_n(t)$ on the tuples $t \in T_n$ with value the maximum of 2^u in the decomposition belonging to that tuple. We call an automorphism of A allowed if its order is a power of 2.

If $k = 2$ applying the Lemma for $r = n - 1$ and $p = 2$, we see that the order of $Aut(A)$ is equal to 2^{n-2}. We start with

$$O_n((1, n-1)) = 2^{n-2}$$

Descending the representation of T_n is "splitting" a C_i in "parts": Tuples $t = (e_1, \cdots, a, \cdots, e_k)$ and $s = (e_1, \cdots, a_1, a_2, \cdots, e_{k+1})$ with $a_1 + a_2 = a$. Special case $t = (e_1, \cdots, a)$ and $s = (e_1, \cdots, a_1, a_2)$.

We distinguish two cases, first $a_1 = a_2$. Replacing C_i of order 2^a by the direct product of two equal cyclic groups of order $2^{a_1} = 2^{a_2}$ will have no influence on the number of allowed automorphisms. Second, if $a_1 < a_2$ we see with the Lemma: $2^{a-1} \geq 2^{a_1-1} \cdot 2^{a_2-1} = 2^{a-2}$. In this case we conclude that the number of allowed automorfisms will never increase.

In any case we can verify that $O_n(t) \geq O_n(s)$. That completes the story.

The order of σ is at most 2^{n-2}.

References

[1] Marshall Hall, Jr. The Theory of Groups, Macmillan, New York, 1959.

[2] https://nl.wikipedia.org/wiki/Permanent_(wiskunde)#Formule_van_Spies

[3] Brualdi and Ryser, Combinatorial Matrix Theory, Cambridge University Press, 1991