mathematics

MDPI

Article

A Moore Graph of Diameter 2 and Degree 57 Cannot Be Constructed Using a Group of Derangements

Derek H. Smith [1,*] and Roberto Montemanni [2]

[1] Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1DL, Wales, UK
[2] Department of Sciences and Methods for Engineering, University of Modena and Reggio Emilia, Via Amendola 2, 42122 Reggio Emilia, Italy; roberto.montemanni@unimore.it
* Correspondence: derek.smith@southwales.ac.uk

Abstract

In 1960, Hoffman and Singleton studied the possible existence of Moore graphs of degree k and diameter 2. A Moore graph is a regular graph with these parameters and the maximum possible number of vertices. They proved by algebraic means that the only possible cases are $k = 2$ (the pentagon), $k = 3$ (the Petersen graph), $k = 7$ (the Hoffman–Singleton graph) and possibly $k = 57$ (the unresolved case). Deciding this unresolved case $k = 57$ has proved to be an elusive challenge ever since. If the graph exists, it must have girth 5, that is, with no cycles of length 3 or 4. A construction can start from a tree with $1 + k^2$ vertices, with further edges to be inserted between leaf vertices being described by permutations. The permutations associated with the first branch can, without loss of generality, be assumed to be identity permutations. The remaining permutations must all be derangements, which have no fixed points. As many products of these derangements must also be derangements, it is tempting to use a group of derangements. In a recent paper, it was shown that the use of a cyclic group of derangements is impossible. In this paper, it is shown more generally that a construction via any group of derangements is not possible.

Keywords: graph theory; Moore graphs; diameter; girth

MSC: 05C12; 05C38

1. Introduction

The question of whether there exists a Moore graph of degree 57 and diameter 2 has been a source of frustration for graph theorists since the seminal paper of Hoffman and Singleton [1] appeared in 1960. Hoffman and Singleton showed by algebraic means that a Moore graph of diameter 2 and degree k exists if $k = 2$ (the pentagon), $k = 3$ (the Petersen graph), $k = 7$ (the Hoffman–Singleton graph) and possibly $k = 57$ (the unresolved case). This unresolved case is often referred to as the "missing Moore graph" or as sometimes the "Aschbacher graph". A Moore graph is a regular graph of a given diameter and degree with the maximum possible number of vertices. In the case of diameter 2, for any vertex w, there will be k vertices adjacent to w and $k(k-1)$ vertices at distance 2 from w. It follows that there cannot be cycles of length 3 or 4, so in other words, the graph has $1 + k^2$ vertices and girth 5. This allows a construction to start from a tree with $|\Gamma_1(w)| = k$ and $|\Gamma_2(w)| = k(k-1)$. Girth 5 then implies that the remaining edges to be added are adjacent to leaf vertices of different branches. In fact, for any two branches, the edges adjacent to their leaf vertices form a perfect matching which can be described by a permutation. Without loss of generality, it is possible for the permutations involving the first branch to be identity permutations,

Check for updates

Academic Editor: Janez Žerovnik

Received: 19 October 2026
Revised: 15 November 2026
Accepted: 18 November 2026
Published: 24 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

and then it can be shown that the remaining permutations are derangements (permutations with no fixed points). As it can be shown that many products of these derangements are also derangements, the use of a group of derangements for the set of permutations is suggested. The study of the use of a group of derangements for a Moore graph of diameter 2 and degree 57 was begun in [2], where it was shown that a construction using a cyclic group of derangements is not possible. The aim of this paper is to demonstrate that no construction is possible using any group of derangements.

Information on Moore graphs and the diameter 2, degree 57 case can be found in [3–5]. Much of the progress that has been made limits the amount of symmetry the graph could possess if it exists. The graph cannot be distance-transitive [6], cannot be vertex-transitive [7], and the size of the automorphism group cannot exceed 375 [8] (see also [9]). Smith and Montemanni [10] adopted an optimization approach to the construction of the missing Moore graph. The deficit in the number of edges obtainable by this approach was sufficiently large as to make existence seem unlikely. Smith and Montemanni [11] studied potential subgraphs of the missing Moore graph induced by a set of t branches. Subgraphs of girth 5 and maximum degree 57 could be obtained up to $t = 20$ but could not be found for larger values of t.

Section 2 outlines the construction method. Section 3 gives conditions on the branch/branch permutations to avoid cycles of length 3 or 4. Section 4 introduces the use of groups of derangements and presents a standard result on the order of semi-regular groups, together with a proof that the derangements at a single branch are all distinct. Section 5 shows how some modified transversals and a link to cliques can be applied to the existence problem. In Section 6, the system GAP (Groups, Algorithms, and Programming) is used to generate Cayley tables of the 13 possible groups of order 56. Two maximum clique algorithms, together with supporting evidence, are then used to show that the necessary modified transversals for a construction almost certainly do not exist. This strongly suggests that a construction via a group of derangements is impossible. Section 7 presents a theoretical proof, suggested by a Generative AI starting from the previous experimental study, as an alternative to the calculations in Section 6. Finally, the Conclusion summarises the outcome of the work and ideas for the future.

2. The Initial Tree and Branch/Branch Permutations

The Moore graph under consideration is regular of degree k = 57, has diameter d = 2 and the maximum number $1 + k^2 = 3250$ of vertices. Thus, construction of a Moore graph of diameter 2 and degree 57 can start from a tree, as shown in Figure 1.

Any vertex can be chosen as the root vertex w. $|\Gamma(w)| = |\Gamma_1(w)| = k$. The tree structure arises because $\Gamma_2(w)$ must have $k(k-1)$ vertices if the maximum number $1 + k^2$ of vertices is to be achieved. As this is true for any choice of w, the graph has girth 5, so further conditions must exclude cycles of length 3 or 4.

The remaining edges to be added to the graph must be of the form (ab) with a and b leaf vertices of distinct branches to avoid creating cycles of length 3. Further, to achieve degree k and avoid cycles of length 4, every leaf vertex of a branch must be adjacent to precisely one leaf vertex of every other branch.

Vertices of $\Gamma_1(w)$ will be labeled as $w_1, w_2, \ldots, w_k$, and the leaf vertices $\Gamma_2(w)$ will be labeled v_{ij} with $i \in \{1, 2, \ldots, k\}$ and $j \in \{0, 1, \ldots, k-2\}$. Vertex w_i is adjacent to all $k-1$ vertices $v_{ij'}$ with $j' \in \{0, 1, \ldots, k-2\}$. For any two branches i_1 and i_2, edges incident with two

vertices of $\Gamma_2(w)$ describe permutations $\Pi_{i_1 i_2}$ of $(0, 1, \ldots, k-2)$. Let $\phi(i_2, v_{i_1 j})$ be the vertex $v_{i_2 j'}$ adjacent to $v_{i_1 j}$.

$$\Pi_{i_1 i_2} = \begin{pmatrix} v_{i_1 0} & v_{i_1 1} & \ldots & v_{i_1 k-2} \\ \phi(i_2, v_{i_1 0}) & \phi(i_2, v_{i_1 1}) & \ldots & \phi(i_2, v_{i_1 k-2}) \end{pmatrix}$$

, and $\Pi_{i_2 i_1} = \Pi^{-1}_{i_1 i_2}$. Permutations will be composed in the order they are presented.

Considering first the permutations $\Pi_{1 i_2}$, leaf vertices of branches $2 \ldots k$ can be permuted so that, without loss of generality, all $\Pi_{1 i_2}$ are identity permutations. This assumption will be important in the proofs that follow.

This paper will focus, as in [2], on the set of permutations $\{\Pi_{i_1 i_2}\}$.

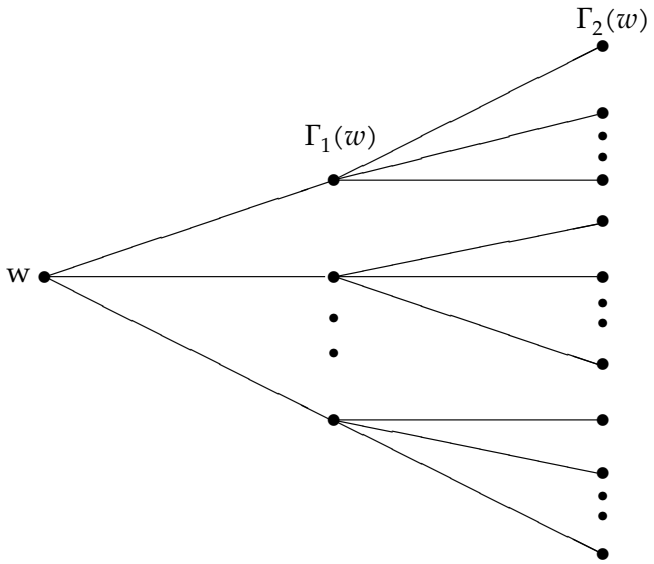


Figure 1. Starting tree for the Moore graph. The number of vertices is $1 + k^2$.

3. Conditions on Branch/Branch Permutations

Recall the following definition:

Definition 1. *A **Derangement** is a permutation with no fixed points. A **Group of Derangements** is a group in which all elements except the identity are derangements.*

Then, using the fact that Π_{1i} is the identity permutation for all i with $1 < i \leq k$, the following conditions hold to avoid cycles of length 3 or 4:

$$\Pi_{i_1 i_2} (2 \leq i_1 < i_2 \leq k) \text{ is a derangement.} \tag{1}$$

This follows as if q' was a fixed point, and then a cycle of length 3 $(1, q')$, (i_1, q'), (i_2, q'), $(1, q')$ would be obtained. Similarly, the inverse permutation $\Pi_{i_2 i_1}$ is a derangement.

$$\Pi_{i_1 i_2} \Pi_{i_2 i_3} (k \geq i_1 > 1, k \geq i_2 > 1, k \geq i_3 > 1, i_1 \neq i_2, i_1 \neq i_3, i_2 \neq i_3) \text{ is a derangement.} \tag{2}$$

This follows as if q' was a fixed point, and then a cycle of length 4 $(1, q')$, (i_1, q'), (i_2, q''), (i_3, q'), $(1, q')$ would be obtained. Similarly, the inverse of the product is a derangement.

Now for the branches 2,3,...,k, the following two conditions hold:

$$\Pi_{i_1 i_2} \Pi_{i_2 i_3} \Pi_{i_3 i_1} (k \geq i_1 > 1, k \geq i_2 > 1, k \geq i_3 > 1, i_1 \neq i_2, i_1 \neq i_3, i_2 \neq i_3) \text{ is a derangement.} \tag{3}$$

This follows as if q' was a fixed point, and then a cycle of length 3 (i_1, q'), (i_2, q''), (i_3, q'''), (i_1, q') would be obtained. Similarly, the inverse of the product is a derangement.

For $(k \geq i_1 > 1, k \geq i_2 > 1, k \geq i_3 > 1, k \geq i_4 > 1)$

$$\Pi_{i_1 i_2}\Pi_{i_2 i_3}\Pi_{i_3 i_4}\Pi_{i_4 i_1}(i_1 \neq i_2, i_1 \neq i_3, i_1 \neq i_4, i_2 \neq i_3, i_2 \neq i_4, i_3 \neq i_4) \text{ is a derangement.} \quad (4)$$

This follows as if q' was a fixed point, and then a cycle of length 4 (i_1, q'), (i_2, q''), (i_3, q'''), (i_4, q''''), (i_1, q') would be obtained. Similarly, the inverse of the product is a derangement.

If derangements could be assigned to ordered branch/branch pairs so that these conditions are all satisfied, and a Moore graph of diameter 2 would be obtained.

4. Groups of Derangements

The conditions in Section 3 can be viewed as conditions on an assignment of derangements and the identity permutation to oriented edges of a complete graph K_k. Label the vertices of this complete graph as $v_1, v_2, \ldots, v_k$, with v_i corresponding to branch i. The identity permutation is assigned to all pairs (v_1, v_i) and to no other pairs. Here, we are considering the case when the derangements are elements of a group of derangements of degree $k - 1 = 56$.

A permutation group is called *semiregular* if the only permutation fixing any selected point is the identity [12]. Thus, the definitions of a semiregular group and a group of derangements are identical. A proof of Proposition 1 is well known and can be found in [12].

Proposition 1. *The order of a semiregular group is a divisor of its degree.*

Proposition 2. *For any $i_1, i_2, i_3 \in \{2, 3, \ldots, k\}$ with $i_1 \neq i_2, i_1 \neq i_3, i_2 \neq i_3$ $\Pi_{i_1 i_2} \neq \Pi_{i_1 i_3}$.*

Proof. Assume that $\Pi_{i_1 i_2} = \Pi_{i_1 i_3}$ and recall that $\Pi_{i_2 i_1} = \Pi_{i_1 i_2}^{-1}$. As both Π_{1i} and Π_{i1} are the identity permutation for all $2 \leq i \leq k$, $\Pi_{1 i_2}\Pi_{i_2 i_1}\Pi_{i_1 i_3}\Pi_{i_3 1} = \Pi_{1 i_2}\Pi_{i_2 i_1}\Pi_{i_1 i_2}\Pi_{i_3 1} = \Pi_{1 i_2}\Pi_{i_1 i_2}^{-1}\Pi_{i_1 i_2}\Pi_{i_3 1} = \Pi_{1 i_2}\Pi_{i_3 1} = \Pi_{1 i_2}\Pi_{1 i_3}$ is the identity permutation. Choosing any fixed point q' of this identity permutation, vertices $(1, q')$, (i_2, q'), (i_1, q''), (i_3, q'), $(1, q')$ would form a cycle of length 4. This gives a contradiction. □

It can be seen from Propositions 1 and 2 that the group of derangements must have order $k - 1 = 56$.

5. Transversals and Cliques in the Group of Derangements Case

Definition 2. *A **transversal** in the Cayley table (multiplication table) of a group is a set of entries such that there is one entry in each row, one entry in each column, and all the group elements in the transversal are distinct [13].*

Definition 3. *A **partial transversal** in the Cayley table (multiplication table) of a group of order $k - 1$ is a set of $\ell < k - 1$ entries such that there is at most one entry in each row, at most one entry in each column, and all the group elements in the transversal are distinct.*

In the work that follows, we shall choose a specific non-identity element of a group of derangements and refer to it as the *selected element*.

Definition 4. *For a particular group and a selected element, remove the rows and columns corresponding to the identity element and the selected element. The remaining table will be referred to here as a **reduced Cayley table**.*

https://doi.org/10.3390/math14234318

Definition 5. *A **specified transversal** in a reduced Cayley table is a set of all entries consisting of distinct elements of the group, excluding the identity element and the selected element, with one entry in each remaining row and one entry in each remaining column.*

Now, consider vertices $v_2, v_3, \ldots v_k$ of the complete graph K_k with non-identity elements of a group of derangements of order $k-1$ assigned to ordered pairs of distinct vertices. In view of Proposition 2, all non-identity elements in the group must be used, and so any non-identity element can be chosen as the selected element and assigned to an ordered pair $(v_i, v_j), i \neq j$ of vertices.

Theorem 1. *For any selected element assigned to an ordered pair (v_i, v_j) of vertices with $i \geq 2, j \geq 2, i \neq j$, the products $\Pi_{i\ell}\Pi_{\ell j}$ (with $i \geq 2, \ell \geq 2, j \geq 2, i \neq j, i \neq \ell, j \neq \ell$) must be the $k-3 = 54$ entries of a specified transversal in the reduced Cayley table of the chosen group of derangements.*

Proof. Consider ordered triples (v_i, v_ℓ, v_j) for all ℓ with $i \geq 2, \ell \geq 2, j \geq 2, i \neq j, i \neq \ell, j \neq \ell$. None of the permutations considered here can be the identity as a result of Equations (1) and (2). From Proposition 2, the derangements assigned to pairs (v_i, v_j) and all (v_i, v_ℓ) are all distinct, and in a similar way, the derangements assigned to pairs (v_i, v_j) and all (v_ℓ, v_j) are distinct. Now, consider the products of derangements $\Pi_{i\ell}\Pi_{\ell j}$ assigned to pairs (v_i, v_ℓ) and (v_ℓ, v_j) for any $\ell \geq 2, \ell \neq i, \ell \neq j$. These are distinct from Π_{ij}, or a product $\Pi_{i\ell}\Pi_{\ell j}\Pi_{ij}^{-1}$ would be the identity giving rise to $k-1$ cycles of length 3. Also, if $\Pi_{i\ell_1}\Pi_{\ell_1 j} = \Pi_{i\ell_2}\Pi_{\ell_2 j}$ then $\Pi_{i\ell_1}\Pi_{\ell_1 j}\Pi_{\ell_2 j}^{-1}\Pi_{i\ell_2}^{-1}$ would be the identity giving rise to $k-1$ cycles of length 4, it follows that for this selected element, the products $\Pi_{i\ell}\Pi_{\ell j}$ must be elements of a specified transversal in the reduced Cayley table of the chosen group of derangements. □

For the Moore graph of degree 57 and diameter 2 to be constructed in this way from some group of derangements, there must be a group of derangements of order 56 such that for every non-identity element chosen as the selected element, a specified transversal in the reduced Cayley table (with 54 elements) must exist.

Definition 6. *A* clique *C of a graph G is a subset of the vertices of G with every pair of vertices of C adjacent.*

Construct a graph G where the vertices correspond to entries in the reduced Cayley table, excluding those that are either the identity or the selected element of the group of derangements. Two vertices are adjacent if they correspond to different group elements, and the entries represented are in different columns and in different rows. A specified transversal in the reduced Cayley table corresponds to a clique in G with 54 vertices and must be a maximum clique in the graph G. Thus, the construction indicated in Section 2 using a group of derangements is only possible if, for every selected element, the graph G has a maximum clique with 54 vertices.

6. Calculation of Cliques

In this section, all possible groups of order 56 will be considered, and for all selected elements in each group, a maximum clique in the graph G will be sought. Use will be made of the system GAP (Groups, Algorithms, and Programming) [14] and two maximum clique algorithms HTS2 [15] and SBTS [16].

There are 13 groups of order 56, and GAP was used to generate a Cayley table of each group. The order in which GAP presents these groups, and the order in which group elements are presented, is unimportant here, except that the cyclic group is Group 2, and the fifth element (which appears as the fourth position in Figure 2) is the only involution

(non-identity self-inverse element). For each group, there are 55 possible selected elements, so $13 \times 55 = 715$ clique calculations are necessary. In these cases, the graph G has 2808 or 2809 vertices. Although these problems are too large for an exact algorithm, both the algorithms HTS2 [15] and SBTS [16] have been shown to be able to find optimal solutions when a tight upper bound is available for problems of a similar size. This suggests that the cliques found are almost certainly maximum cliques, and further evidence for this will be presented below. In fact, these clique problems appear to be relatively easy in comparison with the standard benchmarks on which HTS2 and SBTS were tested [15,16]. A clique with 53 or 54 vertices was found almost immediately by HTS2, and 53 never improved in a very long run. Each HTS2 search normally ran for about 30 min without improvement, although some longer runs will be presented below. The results of the HTS2 runs are shown in a compact form in Figure 2. The selected elements run from element 2 to element 56 in the order presented in the Cayley table by GAP. A 0 denotes a clique of size 53 (so maximality would imply that no specified transversal exists for the selected element), and a 1 denotes a clique of size 54 which must be maximum (so a specified transversal does exist for the selected element). Recall that a specified transversal must exist for every selected element, so only a complete row of 1s would allow the group to be used to construct the Moore graph. The results are a long way short of this for any of the 13 groups.

Group 1	00100000010000000100000001000000010000000100000000100000
Group 2	00010000000000000000000000000000000000000000000000000000
Group 3	00110000011000000110000001100000011000000110000000100000
Group 4	00010000001000000010000000100000001000000010000000000000
Group 5	00110000011000000110000001100000011000000110000000100000
Group 6	00010000001000000010000000100000001000000010000000000000
Group 7	00110000011000000110000001100000011000000110000000100000
Group 8	00000000000000000000000000000000000000000000000000000000
Group 9	00010000000000000000000000000000000000000000000000000000
Group 10	00010000000000000000000000000000000000000000000000000000
Group 11	01110000111000000010000000000000000000000000000000000000
Group 12	00010000001000000010000000100000001000000010000000000000
Group 13	00000000000000000000000000000000000000000000000000000000

Figure 2. Clique sizes found for the 13 groups of order 56. Row and column 1 of the Cayley table (corresponding to the identity element) are always removed. If row and column j $\{j \in 2 \ldots 56\}$ are also removed, then the clique size found is shown in the positions $\{2 \ldots 56\}$, with the first position being 2. A 0 denotes a clique of size 53, and a 1 denotes a clique of size 54. Thus, for Group 2 (the cyclic group), a clique of order 54 only arises if row and column 5 are removed. In the GAP order, this is the cyclic shift by 28 positions (an involution). Although these clique sizes are strictly lower bounds, evidence suggests that they are maximum clique sizes.

To aid the reproducibility of the results in Figure 2, some material on GAP, HTS2, and SBTS is included in the Appendices A–C.

The results derived from the compressed form in Figure 2 arise from heuristic algorithms and so strictly are lower bounds. To show that they are likely to be correct sizes of maximum cliques, without providing a formal proof, three approaches were used. Unfortunately, the graph coloring upper bound for the graph G is not always a tight bound. A vertex coloring of G is an assignment of colors to the graph G such that adjacent vertices must have different colors, thus a clique in G can only have one vertex from each color class, and the number of colors is an upper bound for the number of vertices in the clique. Algorithmic attempts to find vertex colourings with less than 54 colors failed, and this is explained by the following proposition.

Proposition 3. *The number of colors in a minimum vertex coloring of G is always 54.*

Proof. In a reduced Cayley table, the elements other than the identity and the selected element can be referred to as the *required elements*. In the corresponding graph G, with vertices corresponding to entries in the reduced Cayley table which are required elements, two vertices are adjacent if the entries they correspond to are in different rows, different columns and are different required elements. Thus, two vertices can be in the same color class if the entries are in the same row, or in the same column, or are the same required element. There are three immediate colorings:

1. Color classes are vertices corresponding to all required elements in a row.
2. Color classes are vertices corresponding to all required elements in a column.
3. Color classes are vertices corresponding to all entries that are the same required element.

Each of these colorings has $k - 3 = 54$ colors. If a coloring with less than 54 colours is to exist, alternative color classes must be found. Clearly, subsets of these classes will not lead to a smaller number of colors. Each of the color classes described above has at least 52 vertices. It will be shown that any alternative (mixed) color classes will have fewer vertices and so cannot lead to a smaller number of color classes. The argument that follows deals with a row case. A similar argument applies in the other two cases. Assume first that there are at least three entries in some row, and attempt to add entries in another row. It can be in the same column as one of three entries, can be the same element as another entry, but cannot be in the same column or be the same element as a third entry. Thus, no new color class of this type is possible. Now assume that there are exactly two entries in some row. Two further entries can each be in the same column as one of the initial two entries and be the same element as the other. Then, as they are in different columns and are different elements, they must be in the same row. Then, it can be seen that no further entries are available to give vertices in the color class. A color class with four vertices cannot lead to a smaller number of colors. The only case not covered by the row and column arguments is when a color class has one entry in each row and one entry in each column. But then all entries must be of the same required element, and this is simply a color class of the third type specified initially and so is not a larger color class.

Now consider the summation

$$\sum_j i_j j = 2808 \text{ or } 2809$$

where i_j is the number of color classes with j vertices, and the number of vertices in G is 2808 or 2809. Each of the color classes defined initially has 52, 53 or 54 vertices. Thus,

$$i_{52}.52 + i_{53}.53 + i_{54}.54 = 2808 \text{ or } 2809 \text{ with } \sum_j i_j = 54$$

As it has been shown that all alternative color classes must have a smaller number of vertices, $\sum_j i_j$ cannot decrease, and in fact must increase. Thus, the graph coloring upper bound can never be improved from 54 to 53. □

As a first check, for each group, the HTS2 clique search with the first non-identity element in the GAP ordering as the selected element was run for over 12 h with no improvement. In fact, each of the 13 results of 53 was always obtained almost immediately and never improved.

A further check of correctness was carried out by running the clique search algorithm SBTS [16] for all 13 groups and all selected elements, again requiring 715 maximum clique calculations. SBTS works on significantly different principles to HTS2, and so these can be considered as complementary calculations. Precisely the same results were obtained as those presented in Figure 2.

A theoretical check is also possible using Group 2 (the cyclic group).

Theorem 2. *A specified transversal in a reduced Cayley table of a cyclic group of order 56 can only exist if the selected element is a cyclic shift by 28 positions.*

Proof. Consider ordered triples (v_i, v_ℓ, v_j) for all ℓ, with $i \geq 2, \ell \geq 2, j \geq 2, i \neq j, i \neq \ell, j \neq \ell$. Recall that the derangements assigned to pairs (v_i, v_j) and all (v_i, v_ℓ) are all distinct, and the derangements assigned to pairs (v_i, v_j) and all (v_ℓ, v_j) are distinct. Recall also that the products of derangements $\Pi_{i\ell}\Pi_{\ell j}$ assigned to pairs (v_i, v_ℓ) and (v_ℓ, v_j) for any $\ell \geq 2, \ell \neq i, \ell \neq j$ are distinct. For the cyclic group, define variables x_{ij}, where $x_{ij} = c$ $(c \in \{0, 1, \ldots, (k-2)\})$ if Π_{ij} maps $\{0, 1, \ldots, k-2\}$ to $\{c, 1+c, \ldots, k-2+c\}$ mod $(k-1)$ (a cyclic shift by $c \leq k-2$ positions). Thus, the permutation Π_{ij} is represented by x_{ij}. Then, for any $x_{ij} = \tau (\tau > 0)$, if $z_{i\ell j} \equiv (x_{i\ell} + x_{\ell j})$ mod $(k-1)$ $(\ell > 1, \ell \neq i, \ell \neq j)$, the $z_{i\ell j}$ are all distinct and distinct from x_{ij}. Then, if $L = \{\ell > 1, \ell \neq i, \ell \neq j\}$,

$$\sum_{\ell \in L} z_{i\ell j} \equiv \left(\sum_{\ell \in L} x_{i\ell} + \sum_{\ell \in L} x_{\ell j} \right) \bmod (k-1)$$

As $x_{i\ell} \neq \tau, x_{\ell j} \neq \tau, z_{i\ell j} \neq \tau$ (to avoid creating cycles of length 3 or 4), each of these three summations is $\sum_{h=1, h\neq\tau}^{k-2} h \equiv \frac{(k-1)(k-2)}{2} - \tau \bmod (k-1)$ so $\frac{(k-1)(k-2)}{2} - \tau \equiv 0 \bmod (k-1)$. For $k = 57$, $1540 - \tau \equiv 0 \bmod (56)$ and $\tau = x_{ij}$ can only be 28 (a cyclic shift by 28 positions). This is an involution which is shown as 1 in the 4th position of row 2 of Figure 2, so a specified transversal does exist. An alternative specified transversal in this case is displayed in Figure 3. Note that the conditions used in this proof are the same as the conditions required for a specified transversal. It follows that the results for Group 2 in Figure 2 are correct indications of maximum clique sizes. □

row	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
column	37	54	33	5	49	19	44	31	41	12	8	15	22	18	6	21	45	27
element	37	55	35	8	53	24	50	38	49	21	18	26	34	31	20	36	5	44
row	20	21	22	23	24	25	26	27	28	30	31	32	33	34	35	36	37	38
column	53	39	7	36	25	40	43	47	42	4	52	9	10	16	13	35	17	23
element	15	2	27	1	47	7	11	16	12	32	25	39	41	48	46	13	52	3
row	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
column	48	32	50	3	55	24	30	34	20	14	28	38	2	51	11	46	26	56
element	29	14	33	43	40	10	17	22	9	4	19	30	51	45	6	42	23	54

Figure 3. A specified transversal in a reduced Cayley table of a cyclic group of order 56 with selected element $\tau = 28$. The Cayley table in this example is not the table generated by GAP, but a more natural table given by *group element* = (*row number* + *column number* − 2) mod 56.

While there was already little doubt that the results in Figure 2 were correct, it seems implausible that there could be no incorrect results for the cyclic group, but there could be at least 33 incorrect results for one of the other groups, which would be necessary if a row of 1s in Figure 2 were to exist. Correctness demonstrates that the possibility of a construction using a group of derangements is excluded. A formal proof of this will be presented in the next section.

7. A Theoretical Alternative to Section 6 Suggested by Generative AI

As an alternative to the calculations in Section 6, a theoretical proof suggested by a Generative AI, starting from the foundations in Sections 2–5, is presented in this section. The theory presented will be accessible to the reader with the necessary background in group theory. This provides a proof that no group of order 56 can satisfy the requirement of Theorem 1 for every non-identity selected element. This completes an analytical, self-contained proof of non-existence without requiring the maximum clique searches of

Section 6. The proof strategy for Theorem 3 and side results were initially drafted with the assistance of the AI language model Google Gemini [17]. Subsequently, the proof was independently checked, corrected, substantially modified to make it more accessible, and finalized by the authors.

7.1. Algebraic Preliminaries: Derived Subgroups and Abelianization

To make the proof more accessible, the foundational algebraic concepts used in the derivation will be outlined.

Definition 7. *Let G be a finite group. For any two elements $a, b \in G$, their **commutator** is defined as $[a, b] = a^{-1}b^{-1}ab$. Then, we have the following:*

- *If a and b commute ($ab = ba$), then $[a, b] = a^{-1}b^{-1}ba = e$, where e is the identity element.*
- *If a and b do not commute, $[a, b] \neq e$ measures the degree to which commutativity fails.*

*The **derived subgroup** (or **commutator subgroup**), denoted $G' = [G, G]$, is the subgroup generated by all commutators in G:*

$$G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle.$$

Definition 8. *The derived subgroup G' is always a normal subgroup of G ($G' \lhd G$). The quotient group $\overline{G} = G/G'$ is called the **abelianization** of G. Then, we have the following:*

- *The elements of $\overline{G}$ are the cosets $\overline{x} = xG'$ for $x \in G$.*
- *Passing to the quotient $\overline{G}$ forces all commutators to equal the identity coset $\overline{e} = 0 \in \overline{G}$, making $\overline{G}$ a commutative (abelian) group under addition: $\overline{x} + \overline{y} = \overline{y} + \overline{x}$.*
- *Let $\pi : G \to \overline{G}$ denote the canonical projection mapping $x \mapsto \overline{x}$.*

7.2. The Main Invariant and Non-Existence Theorem

Lemma 1. *If a group G of order 56 admits a specified transversal in its reduced Cayley table with respect to a selected element $g \in G \setminus \{e\}$, then its coset $\overline{g} \in \overline{G}$ must satisfy:*

$$\overline{g} = T \quad \text{in } \overline{G},$$

where $T = \sum_{x \in G} \overline{x} \in \overline{G}$ is the sum of the images of all elements of G.

Proof. Let $g \in G \setminus \{e\}$ be a selected element. By Definition 5, a specified transversal in the reduced Cayley table of G with respect to g consists of two bijections $x, y : \{1, 2, \ldots, 54\} \to G \setminus \{e, g\}$ such that the elementwise product $z(l) = x(l)y(l)$ is also a bijection from $\{1, 2, \ldots, 54\}$ onto $G \setminus \{e, g\}$.

Projecting the relation $x(l)y(l) = z(l)$ via the canonical homomorphism π into the additive quotient group $\overline{G} = G/G'$ yields:

$$\overline{x}(l) + \overline{y}(l) = \overline{z}(l) \quad \text{in } \overline{G} \text{ for each } l \in \{1, 2, \ldots, 54\}.$$

Summing this identity over all $l = 1, 2, \ldots, 54$:

$$\sum_{l=1}^{54} \overline{x}(l) + \sum_{l=1}^{54} \overline{y}(l) = \sum_{l=1}^{54} \overline{z}(l) \quad \text{in } \overline{G}.$$

Because x, y, z are all bijections onto $G \setminus \{e, g\}$, each sum represents the sum of all elements in $G \setminus \{e, g\}$ projected into $\overline{G}$:

$$\sum_{h \in G \setminus \{e,g\}} \overline{h} = \left(\sum_{h \in G} \overline{h} \right) - \overline{e} - \overline{g} = T - 0 - \overline{g} = T - \overline{g}.$$

Substituting this back into the sum of projected equations gives:

$$(T - \overline{g}) + (T - \overline{g}) = (T - \overline{g}) \quad \text{in } \overline{G}.$$

Subtracting $(T - \overline{g})$ from both sides yields:

$$T - \overline{g} = 0 \implies \overline{g} = T \quad \text{in } \overline{G}.$$

This completes the proof of Lemma 1. □

Theorem 3. *A Moore graph of diameter 2 and degree 57 cannot be constructed using any group of derangements.*

Proof. Suppose such a Moore graph exists using a group of derangements G. By Propositions 1 and 2, G must be a group of order 56. By Theorem 1, *every* non-identity element $g \in G \setminus \{e\}$ must act as a selected element admitting a specified transversal.

Hence, by Lemma 1, *every* non-identity element $g \in G \setminus \{e\}$ must satisfy:

$$\overline{g} = T \quad \text{in } \overline{G} = G/G'.$$

We analyze this requirement across all possible isomorphism types for groups of order 56:

Case 1: G is non-abelian ($G' \neq \{e\}$). The order of G is $|G| = 56 = 2^3 \cdot 7$. By Burnside's $p^a q^b$ Theorem [18], any finite group whose order is divisible by at most two distinct primes is solvable.

For a nontrivial finite solvable group G, the derived subgroup $G' = [G, G]$ is strictly a *proper* normal subgroup ($G' \subsetneq G$). Furthermore, because G is non-abelian, G' contains non-identity elements ($G' \neq \{e\}$). Thus, the order of the commutator subgroup satisfies $1 < |G'| < 56$.

The quotient group $\overline{G} = G/G'$ therefore has order $|\overline{G}| = |G|/|G'| \geq 2$, partitioning G into at least two distinct cosets:

1. The identity coset $\overline{e} = 0 = G'$ contains the identity e and all non-identity elements $g \in G' \setminus \{e\}$. For all these elements, $\overline{g} = 0$.
2. The non-identity cosets contain elements $h \in G \setminus G'$ with $\overline{h} \neq 0$.

Now, we evaluate the constraint $\overline{g} = T$:

- If $T \neq 0$ in $\overline{G}$, then any element $g \in G' \setminus \{e\}$ (which exists, since $G' \neq \{e\}$) satisfies $\overline{g} = 0 \neq T$, violating Lemma 1.
- If $T = 0$ in $\overline{G}$, then any element $h \in G \setminus G'$ (which exists, since $G' \subsetneq G$) satisfies $\overline{h} \neq 0 = T$, violating Lemma 1.

Thus, no non-abelian group of order 56 can satisfy $\overline{g} = T$ for all non-identity elements $g \in G \setminus \{e\}$.

Case 2: G is abelian ($G' = \{e\}$). When G is abelian, $G' = \{e\}$, and $\overline{G} = G$. The projection maps elements directly to themselves ($\overline{g} = g$), so the condition $\overline{g} = T$ simplifies to:

$$g = T \quad \text{in } G.$$

Since $T = \sum_{h \in G} h$ evaluates to a single fixed element of G, the equality $g = T$ can hold for *at most one* element $g \in G$. Therefore, at least 54 of the 55 non-identity elements in $G \setminus \{e\}$ satisfy $g \neq T$, violating Lemma 1.

Because no group G of order 56 can satisfy $\overline{g} = T$ for all 55 non-identity elements $g \in G \setminus \{e\}$, specified transversals cannot universally exist. Consequently, a construction via any group of derangements is mathematically impossible. □

Example 1. *In the cyclic group* $G = C_{56} = \mathbb{Z}_{56}$*, the total sum is* $T = \sum_{h=0}^{55} h = \frac{55 \cdot 56}{2} = 1540 \equiv 28 \pmod{56}$*. Thus,* $g = T$ *holds strictly for* $g = 28$ *(the unique involution), explaining why transversals exist solely for this single element as observed in Theorem 2.*

8. Conclusions

The unresolved existence question for the missing Moore graph remains. Now that a construction via a group of derangements is excluded, it is necessary to consider further steps in attempting to exclude any construction via the approach described in Section 2. It is interesting to note that in the construction of the Hoffman–Singleton graph for $k = 7$, the derangements used are all involutions. There are only 15 involutions available, which is equal to the number required. For $k = 57$, the number of involutions is massively larger, so their application would be much more complex. However, if the involutions applied to both orientations of edges were regarded as colors, the assignment of involutions to edges would be an edge coloring with additional conditions. This might be a fruitful area for further study.

It was suggested in [2] that the derangements Π_{ij} labeling oriented edges of K_{k-1} be replaced by sets of derangements

$$S_{ij}^{r} = \{\text{Derangements mapping } 0 \text{ to } r \mid r \in \{1, 2, \ldots k-2\}\}$$

There are $k-2$ such sets, and a result similar to Proposition 2 might be proved. Without a group structure to exploit, massive challenges would remain in completing this idea to a proof of non-existence.

Supplementary Materials: The following supporting information can be downloaded at https://www.mdpi.com/article/10.3390/math14234318/s1

Author Contributions: Conceptualization, D.H.S. and R.M.; methodology, D.H.S. and R.M.; validation, D.H.S.; formal analysis, D.H.S. and R.M.; investigation, D.H.S. and R.M.; resources, D.H.S. and R.M.; writing—original draft preparation, D.H.S.; writing—review and editing, D.H.S. and R.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors acknowledge the use of Gemini (Google) [17] for providing suggestions regarding the proof of Theorem 3. All mathematical derivations and results were independently validated and confirmed by the authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. The 13 Groups of Order 56 and GAP

The structure descriptions of the 13 groups are given by the GAP command List(AllSmallGroups(56),StructureDescription) in the following order, which is the order used in Figure 2.

1 "C7 : C8"
2 "C56"
3 "C7 : Q8"
4 "C4 × D14"
5 "D56"
6 "C2 × (C7 : C4)"
7 "(C14 × C2) : C2"

8 "C28 × C2"
9 "C7 × D8"
10 "C7 × Q8"
11 "(C2 × C2 × C2) : C7"
12 "C2 × C2 × D14"
13 "C14 × C2 × C2"

It is only necessary to use a GAP command such as

g := SmallGroup(56 , 3);mat := MultiplicationTable(g); (for group 3)

to obtain a Cayley table. The graph G can then be created from the Cayley table and reformatted for HTS2 or for SBTS.

Further information on using the GAP system can be found in [19].

Appendix B. Parameters Used for HTS2 Runs

The HTS2 software used in Section 6, which has two minor updates, can be found in the Supplementary Material. The HTS2 parameter file HTS2_PARAMETER_FILE.txt used for HTS2 runs was

```
58                      //Target
50                      //Objective_value - immediate output when reached
999999999               //Limit for k in Algorithm 1 - does not terminate
FALSE                   //output for ts iterations?
20                      //Tabutenure
TRUE                    //Use non-default (custom) value of Tssetmin
40                      //Tssetmin
TRUE                    //Use non-default value of theta and lambda parameters
52                      //Threshold_For_One_Opt (θ1)
52                      //Threshold_For_Two_Opt (θ2)
52                      //Threshold_For_Three_Opt (θ3)
52                      //Threshold_For_Ts_Opt (θts)
80                      //Exact_Search_Threshold1 (λ1)
60                      //Exact_Search_Threshold2 (λ2)
// NOW NAMES OF INPUT AND OUTPUT FILES
56_3_2.per              //name of input .per file for group 3, selected element 2
HTS2_output_56_3_2.log  //name of output text file
```

Appendix C

SBTS solves the maximum clique problem by solving the equivalent maximum independent set problem in the complement graph. Thus, it must be supplied with the complement of the graph G as input. SBTS has just two parameters. For group 3 with selected element 2, the call to SBTS was:

Sbts.exe 56_3_2.mis 56_3_2.txt 54 7

References

1. Hoffman, A.J.; Singleton, R.R. On Moore graphs with diameters 2 and 3. *IBM J. Res. Dev.* **1960**, *4*, 497–504. [CrossRef]
2. Derek, H.S.; Roberto, M. The Moore Graph of Diameter 2 and Degree 57 via Cyclic Derangements. *Axioms* **2026**, *15*, 332. [CrossRef]
3. Norman, B. *Algebraic Graph Theory*; Cambridge Tracts in Mathematics, No. 67; Cambridge University Press: Cambridge, UK, 1974.

4. Mirka, M.; Jozef, Š. Moore graphs and beyond: A survey of the degree/diameter problem. *Electron. J. Comb.* **2013**, *20*, DS14. [CrossRef]
5. Cristina, D. A survey on the missing Moore graph. *Linear Algebra Appl.* **2019**, *569*, 1–14. [CrossRef]
6. Aschbacher, M. The nonexistence of rank three permutation groups of degree 3250 and subdegree 57. *J. Algebra* **1971**, *19*, 538–540. [CrossRef]
7. Cameron, P.J. Automorphism groups of graphs. In *Selected Topics in Graph Theory 2*; Beineke, L.W., Wilson, R.J., Eds.; Academic Press: London, UK, 1983; pp. 89–127.
8. Makhnev, A.A.; Paduchikh, D.V. Automorphisms of Aschbacher graphs. *Algebra Log.* **2001**, *40*, 69–74. [CrossRef]
9. Martin, M.; Jozef, Š. Search for properties of the missing Moore graph. *Linear Algebra Appl.* **2010**, *432*, 2381–2398. [CrossRef]
10. Derek, H.S.; Roberto, M. The missing Moore graph as an optimization problem. *EURO J. Comput. Optim.* **2023**, *11*, 100060. [CrossRef]
11. Derek, H.S.; Roberto, M. Potential subgraphs of the missing Moore graph. *Symmetry* **2024**, *16*, 1563. [CrossRef]
12. Helmut, W. *Finite Permutation Groups*; Academic Press: New York, NY, USA, 1964.
13. Ian M.W. Transversals in Latin squares. *Quasigroups Relat. Syst.* **2007**, *15*, 169–190.
14. The GAP Group. GAP—Groups, Algorithms, and Programming, Version 4.16.1. 2026. Available online: https://www.gap-system.org (accessed on 23 September 2026).
15. Derek, H.S.; Roberto, M.; Stephanie, P. The Use of an Exact Algorithm within a Tabu Search Maximum Clique Algorithm. *Algorithms* **2020**, *13*, 253. [CrossRef]
16. Jin, Y.; Hao, J.-K. General swap-based neighborhood tabu search for the maximum independent set problem. *Eng. Appl. Artif. Intel.* **2015**, *37*, 20–33. [CrossRef]
17. Google Gemini 3.1 Pro. Available online: https://gemini.google.com (accessed on 15 October 2026).
18. Burnside, W. On groups of order $p^{\alpha}q^{\beta}$. *Proc. Lond. Math. Soc.* **1904**, *2*, 388–392.
19. GAP—A Tutorial, Release 4.16.1. 23 August 2026. Available online: https://docs.gap-system.org/doc/tut/manual.pdf (accessed on 6 November 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.