axioms

MDPI

Article

The Moore Graph of Diameter 2 and Degree 57 via Cyclic Derangements

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

[1] Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1DL, 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

The possible existence of a regular Moore graph of diameter 2 and degree 57 with the maximum number 3250 of vertices has been an open question for over 65 years. One approach to a construction focuses on the set of permutations that describe the 1-factors that give the adjacencies between leaf vertices of pairs of branches of a tree. Most of these permutations are derangements, that is they are permutations with no fixed points. As many products of 2, 3, or 4 of these derangements must also be derangements, it is tempting to use a group of derangements, that is a group of permutations in which every non-identity element is a derangement. The first case to consider is when the group of derangements is a cyclic group of permutations. In this paper it is proved that a construction using only a cyclic group of permutations is impossible. This leaves only the possibility of using some other group of derangements, or a set of derangements that do not form a group. The prospects for extending the work to these cases is considered at the end of the paper.

Keywords: graph theory; Moore graphs; diameter; girth

MSC: 05C12; 05C38

1. Introduction

A Moore graph of degree k and diameter d is a simple regular graph with V vertices achieving equality in the Moore upper bound. The bound is

$$|V| \leq 1 + k\sum_{i=1}^{d}(k-1)^{i-1}.$$

and is obtained by counting the maximum possible number of vertices at distance i from any vertex u. The reader is referred to [1,2] for surveys on Moore graphs.

In 1960, Hoffman and Singleton [3] proved that a regular Moore graph of diameter 2 and degree k only exists if $k = 2$ (the pentagon), $k = 3$ (in which case the Petersen graph with 10 vertices is the unique Moore graph), $k = 7$ (in which case the Hoffman-Singleton graph with 50 vertices is the unique Moore graph, or possibly $k = 57$ (the open case which would have the maximum number of 3250 vertices). This last case is often referred to as the "missing Moore graph". In [4], Biggs noted that "many claims of its non-existence have been made" but none have proved publishable, a situation that has continued. Information on the missing Moore graph can be found in [2,5,6]. The main progress that has been made is to limit the possible size of the automorphism group. The graph cannot be distance

Check for updates

Academic Editor: Ivan Gutman

Received: 6 February 2026
Revised: 8 April 2026
Accepted: 27 April 2026
Published: 1 May 2026

transitive [7], cannot be vertex transitive [8], and the automorphism group could not have order greater than 375 [9]. These results, together with the optimization approach in [5], strongly suggest non-existence, but a proof remains elusive.

In this paper a description using permutations is considered. The choice of permutations is split into three cases, and for degree 57 the first case, where the permutations are selected from a cyclic group, is excluded.

2. Structure of the Moore Graph of Diameter 2

For a vertex u, denote by $\Gamma(u)$ the set of neighbours of u. Also, denote by $\Gamma_2(u)$ the set of vertices at distance two from u. Irrespective of the choice of u, a construction of a Moore graph can start from a tree with $|\Gamma(u)| = k$ and $|\Gamma_2(u)| = k(k-1)$ as shown in Figure 1. Then the edges to be added must all be incident with two vertices of $\Gamma_2(u)$.

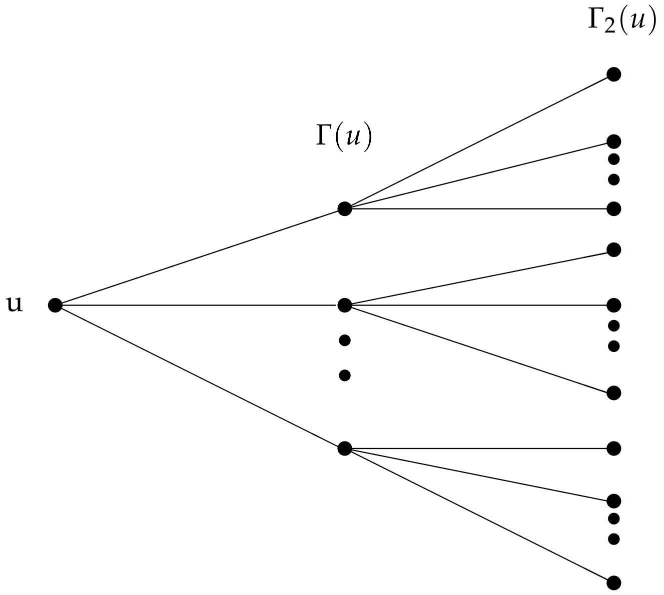

Figure 1. Indicative structure of a starting tree with $1 + k^2$ vertices. Vertex u and all vertices of $\Gamma(u)$ have degree k. It is necessary to add edges incident with two leaf vertices in $\Gamma_2(u)$ so that they also have degree k. This must be done in such a way that no cycles of length 3 or 4 are created and the diameter becomes 2.

For any choice of u a cycle including vertex u must have length at least 5, so the Moore graph must have girth 5. The remaining edges of the Moore graph, must connect leaf vertices of two distinct branches in order to avoid creating cycles of length 3. A leaf vertex of one branch cannot be adjacent to two leaf vertices of another branch, or a cycle of length 4 would be created. As every vertex has degree k, this vertex must be adjacent to exactly one vertex of every other branch. It follows that for a pair of branches, the edges connecting the leaf vertices form a perfect matching. Here, this perfect matching will be represented by a permutation.

In [5], an optimization algorithm was used to generate a graph with 3250 vertices, maximum degree 57, girth 5 and the largest number of edges achievable by the algorithm. The *deficit* was defined as the required number of edges minus the number of edges actually achieved. The best deficit found was 41482. This was later slightly improved to 41391 [10]. Some evidence was presented to suggest that the algorithm was effective. This strongly suggested non-existence of the Moore graph of degree 57, but an actual proof is still required.

3. Vertex Labelling and t-Subgraphs

Starting from the tree represented in Figure 1, label the vertices of $\Gamma(u)$ as $w_1, w_2, \ldots, w_k$ and label the leaf vertices as v_{ij} with $i \in \{1, 2, \ldots, k\}$ and $j \in \{0, 1, \ldots, k-2\}$. As in Figure 1, vertex w_i is adjacent to all $k-1$ vertices $v_{ij'}$ with $j' \in \{0, 1, \ldots, k-2\}$. Denote a Moore graph of diameter 2 and degree k by G.

Definition 1. *A t-subgraph G_t of G $(1 \leq t \leq k)$ is the subgraph induced by the t vertices $w_1, w_2, \ldots, w_t$ and by vertices v_{ij} with $i \in \{1, 2, \ldots, t\}$ and $j \in \{0, 1, \ldots, k-2\}$. As the Moore graph G has girth 5, t-subgraphs do not contain cycles of length 3 or 4.*

Irrespective of the existence of a Moore graph of diameter 2 and degree k, a graph satisfying the conditions for a t-subgraph can be referred to as a potential t-subgraph, as in [11]. In a potential subgraph, vertices of $\Gamma(u)$ have degree k, all other vertices have degree t, and the girth is 5.

4. Construction Using Permutations

A leaf vertex $v_{i_1 j}$ of branch i_1 must be adjacent to a leaf vertex of every other branch, and to precisely one leaf vertex of any branch i_2, or else a cycle of length 4 would be created. If $i_1 < i_2$ let $q(i_2, v_{i_1 j})$ be the vertex $v_{i_2 j'}$ adjacent to $v_{i_1 j}$. A permutation $\Phi_{i_1 i_2}$ of $(0, 1, \ldots, k-2)$ is described by these edges:

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

and $\Phi_{i_2 i_1} = \Phi_{i_1 i_2}^{-1}$.

By permuting leaf vertices of individual branches, it can, without loss of generality, be assumed (as in [5]) that Φ_{1i} is the identity permutation $1 < i \leq k$. As cycles of length 3 or 4 must be avoided, the following conditions hold, with $i_1 \leq k$, $i_2 \leq k$, $i_3 \leq k$, $i_4 \leq k$ in all cases:

$$\Phi_{i_1 i_2} (2 \leq i_1 < i_2) \text{ has no fixed points.} \tag{1}$$

(Assume a fixed point p' of $\Phi_{i_1 i_2}$ exists. A cycle of length 3 would be formed by vertices $(1, p'), (i_1, p'), (i_2, p'), (1, p')$.)

Condition (1) is assumed in the following three conditions.

$$\Phi_{i_1 i_2} \Phi_{i_2 i_3} (i_1 > 1, i_2 > 1, i_3 > 1, i_1 \neq i_2, i_1 \neq i_3, i_2 \neq i_3) \text{ has no fixed points.} \tag{2}$$

(Assume a fixed point p' of $\Phi_{i_1 i_2} \Phi_{i_2 i_3}$ exists. Then vertices $(1, p'), (i_1, p'), (i_2, p''), (i_3, p'), (1, p')$ would form a cycle of length 4.)

$$\Phi_{i_1 i_2} \Phi_{i_2 i_3} \Phi_{i_3 i_1} (i_1 > 1, i_2 > 1, i_3 > 1, i_1 \neq i_2, i_1 \neq i_3, i_2 \neq i_3) \text{ has no fixed points.} \tag{3}$$

(Assume a fixed point p' of $\Phi_{i_1 i_2} \Phi_{i_2 i_3} \Phi_{i_3 i_1}$ exists. Then vertices $(i_1, p'), (i_2, p''), (i_3, p'''), (i_1, p')$ would form a cycle of length 3.)

For $(i_1 > 1, i_2 > 1, i_3 > 1, i_4 > 1)$

$$\Phi_{i_1 i_2} \Phi_{i_2 i_3} \Phi_{i_3 i_4} \Phi_{i_4 i_1} (i_1 \neq i_2, i_1 \neq i_3, i_1 \neq i_4, i_2 \neq i_3, i_2 \neq i_4, i_3 \neq i_4) \text{ has no fixed points.} \tag{4}$$

(Assume a fixed point p' of $\Phi_{i_1 i_2} \Phi_{i_2 i_3} \Phi_{i_3 i_4} \Phi_{i_4 i_1}$ exists. Then vertices $(i_1, p'), (i_2, p''), (i_3, p''')$, (i_4, p''''), (i_1, p') would form a cycle of length 4.)

If these conditions are all satisfied, a Moore graph is obtained.

5. Cyclic Derangements

In the literature permutations with no fixed point are referred to as *derangements*. As the products of permutations listed in the conditions in Section 4 must be derangements, the use of a group of derangements (a group of permutations in which every non-identity element is a derangement) is suggested. Then the permutation approach can usefully be split into three sub-cases:

(1) The derangements $\Phi_{i_1 i_2} (2 \leq i_1 < i_2 \leq k)$ are non-identity elements taken from a cyclic group.

(2) The derangements $\Phi_{i_1 i_2} (2 \leq i_1 < i_2 \leq k)$ are non-identity elements taken from another group of derangements.

(3) The derangements $\Phi_{i_1 i_2} (2 \leq i_1 < i_2 \leq k)$ are not a set of non-identity elements taken from a group of derangements.

The first case is the main focus of this paper. In the case of the cyclic group it is only necessary to show that the relevant products are not equal to the identity of the group.

Define variables x_{ij} where $x_{ij} = a$ $(a \in \{0, 1, \ldots, (k-2)\})$ if Φ_{ij} $(i < j)$ maps $\{0, 1, \ldots, k-2\}$ to $\{a, 1+a, \ldots, k-2+a\}$ mod $(k-1)$ (a cyclic shift by $a \leq k-2$ positions). As Φ_{1i} is the identity we have

$$x_{1i} = x_{i1} = 0 \qquad \forall i \in \{2, 3, \ldots, k\} \tag{5}$$

and from Condition (1) it follows that $x_{ij} \neq 0 \quad \forall i, j \in \{2, 3, \ldots, k\}, i \neq j$. It follows from $\Phi_{ji} = \Phi_{ij}^{-1}$ that

$$x_{ji} = -x_{ij} \tag{6}$$

For $3 \leq p \leq k$ the requirement that cycles of length 3 do not exist represented by Conditions (2) and (3) imply that:

$$x_{pi} + x_{ij} + x_{jp} \not\equiv 0 \bmod (k-1) \tag{7}$$

where $p, i, j \in \{1, 2, \ldots, k\}$, $p > i, p > j, i < j$.

Similarly, for $4 \leq p \leq k$ the requirement that cycles of length 4 do not exist implies that:

$$x_{pi} + x_{ij} + x_{jl} + x_{lp} \not\equiv 0 \bmod (k-1) \tag{8}$$

where $p, i, j, l \in \{1, 2, \ldots, k\}$, $p > i, p > j, p > l, i \neq j, j \neq l, i < l$.

In [11], it was shown using these constraints and the constraint satisfaction software CP-SAT [12] that for degree 57 potential t-subgraphs exist for $t \leq 20$. Existence could not be settled for larger values of t due to the increased number of variables and constraints.

6. The Moore Graph of Diameter 2 and Degree 57 Cannot Be Constructed Using Cyclic Derangements

If the Moore graph exists, it can be constructed using appropriate permutations as in Section 4. It will now be shown that this cannot be done if the permutations (excluding the identities Φ_{1i}) are restricted to cyclic derangements.

Theorem 1. *The Moore graph of diameter 2 and degree 57 cannot be constructed by the method of Section 5 using cyclic derangements.*

Proof. Assume that the Moore graph is constructed using a cyclic group of derangements as in Section 5.

It was noted in Section 4 that leaf vertices of each branch $2, 3, \ldots, k$ can be permuted so that Φ_{1i} is the identity permutation $2 \leq i \leq k$. Then, as in Condition (5), it can be assumed without loss of generality that

$$x_{1i} = x_{i1} = 0 \quad \forall i \in \{2, 3, \ldots, k\}. \tag{9}$$

Independently of this permutation of leaf vertices, branches $3, 4, \ldots, k$ can be permuted so that x_{2k} takes a specific value in $\{x_{23}, x_{24}, \ldots x_{2k}\}$. This will be done later in the proof.

It follows from Equation (9) that

$$x_{ij} \in \{1, 2, 3, \ldots, k-2\}, \forall i, j \in \{2, 3, \ldots, k\} \text{ with } i < j, \tag{10}$$

for if $x_{ij} = 0$ then $x_{1i} + x_{ij} + x_{j1} \equiv 0 \bmod (k-1)$. It would follow that contrary to Condition (3), $\Phi_{1i}\Phi_{ij}\Phi_{j1}$ would be the identity permutation. For any choice of fixed point p' of this identity permutation, vertices $(1, p'), (i, p'), (j, p'), (1, p')$ would form a cycle of length 3, as noted in Section 5. Note also that the x_{2i} $(i \in \{3, 4, \ldots, k\})$ are $k-2$ distinct values, for if $x_{2i} = x_{2j}$ then $x_{2i} - x_{1i} + x_{1j} - x_{2j} \equiv 0 \bmod (k-1)$. It would follow that contrary to Condition (4), $\Phi_{2i}\Phi_{i1}\Phi_{1j}\Phi_{j2}$ would be the identity permutation. For any choice of fixed point p' of this identity permutation, vertices $(2, p'), (i, p''), (1, p''), (j, p''), (2, p')$ would form a cycle of length 4. By a similar argument, the x_{ik} $(i \in \{2, 3, \ldots, k-1\})$ are $k-2$ distinct values. Now assume that the branches of the tree have been permuted as noted above so that $x_{2k} = 1$. Then, x_{2i} $(i \in \{3, 4, \ldots, k-1\})$ are $k-3$ distinct values in $\{2, 3, \ldots, k-2\}$ and x_{ik} $(i \in \{3, 4, \ldots, k-1\})$ are $k-3$ distinct values in $\{2, 3, \ldots, k-2\}$.

Define $z_{2ik} = (x_{2i} + x_{ik}) \bmod (k-1)$ $(i \in \{3, 4, \ldots, k-1\})$. As $x_{2k} = 1$ these values cannot be 1 or $x_{2i} + x_{ik} - x_{2k} \equiv 0 \bmod (k-1)$ creating cycles $(2, p'), (i, p''), (k, p'''), (2, p')$ of length 3. Also, they must be $k-3$ distinct values in $\{2, 3, \ldots, k-2\}$ or if they are repeated for two values i_1 and i_2 then $x_{2i_1} + x_{i_1k} - x_{i_2k} - x_{2i_2} \equiv 0 \bmod (k-1)$ creating cycles $(2, p'), (i_1, p''), (k, p'''), (i_2, p'''', (2, p')$ of length 4. If these values are summed over i:

$$\sum_{i=3}^{k-1} z_{2ik} = \left(\sum_{i=3}^{k-1} x_{2i} + \sum_{i=3}^{k-1} x_{ik} \right) \bmod (k-1)$$

Each of these three summations is:

$$\sum_{\ell=2}^{k-2} \ell \equiv (k-3)k/2 \bmod (k-1)$$

so $(k-3)k/2 \equiv 0 \bmod (k-1)$. In the case $k = 57$ this gives $27 \equiv 0 \bmod 56$ which is a contradiction. Thus the construction using cyclic derangements is impossible. □

It can be observed that $(k-3)k/2 \equiv 0 \bmod (k-1)$ can only be satisfied if $k = 3$. For $k = 7$ the possibility of a cyclic construction is already excluded by the uniqueness of the Hoffman-Singleton graph [3]. The exclusion of the construction for all other values of k apart from $k = 57$ is essentially made redundant by the results of Hoffman and Singleton [3].

7. Discussion

For the case $k = 3$ not excluded by Theorem 1 the Petersen graph (shown in Figure 2) can be rather trivially obtained by the cyclic construction used here. If it is redrawn to highlight the tree pictured in Figure 1, as in Figure 3, it can be seen using the labelling of Section 4 that the only non-identity permutations are cyclic $\Phi_{23} = \Phi_{32} = (01)$.

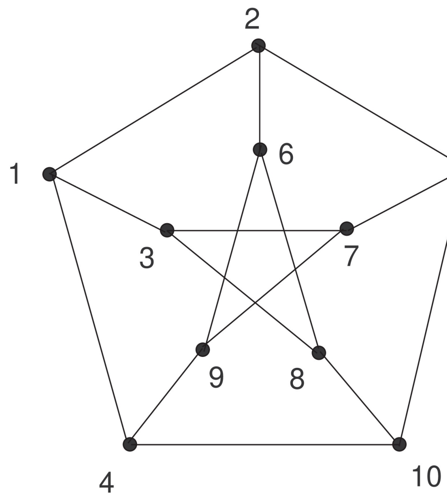

Figure 2. The Petersen Graph as it is usually drawn.

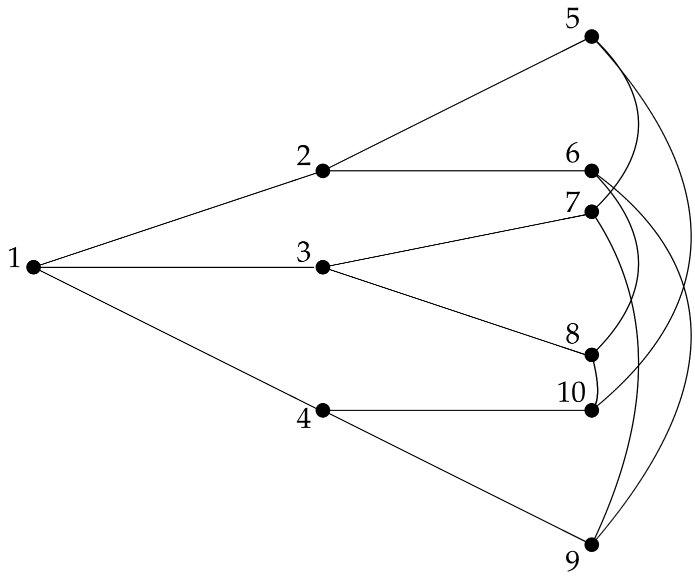

Figure 3. A redrawing of the Petersen graph to show the starting tree. The slightly re-ordered vertices 5, 6, 7, 8, 10, 9 can be re-labelled as $v_{10}, v_{11}, v_{20}, v_{21}, v_{30}, v_{31}$, as in Section 3. Then, it can be seen from the edges incident with two vertices in $\Gamma_2(1)$ that Φ_{12} and Φ_{13} are both the identity permutation, so $x_{12} = x_{13} = 0$. Also, $\Phi_{23} = (01)$ so $x_{23} = 1$.

The cyclic construction has also proved useful, as it has allowed the construction of the largest known potential t-subgraph (with $t = 20$) in [11]. CP-SAT was able to find this potential t-subgraph, but could not find or exclude a potential t-subgraph with $t = 21$. However, a heuristic algorithm similar to that described in [5] but assuming a cyclic construction also suggested that $t = 20$ was the largest value of t for which a potential t-subgraph could be obtained by a cyclic construction (see Figure 4).

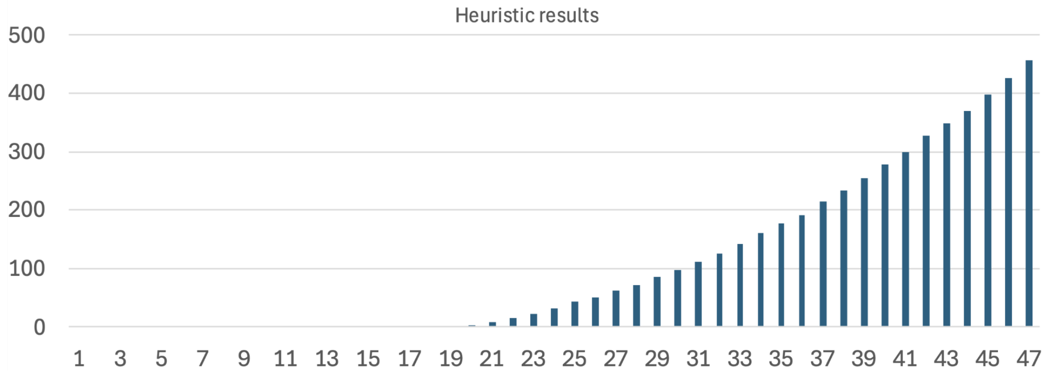

Figure 4. A heuristic attempt to construct a potential t-subgraph for $k = 57$. The horizontal axis shows the values of t. The vertical axis shows the number of x_{ij} values that cannot be found without creating cycles of length 3 or 4. To obtain the deficit this value is multiplied by 56.

The horizontal axis shows the values of t. The vertical axis shows the number of x_{ij} values that cannot be found without creating cycles of length 3 or 4. If an x_{ij} value is missing all the edges incident with leaf vertices in branches i and j are missing. Then the deficit is obtained by multiplying this value by 56. It can be seen that zero deficit is obtained up to $t = 19$. For $t = 20$ there is one missing x_{ij} value, so the deficit is 56. Thus the heuristic is not quite as strong as the exact algorithm in CP-SAT, but still allows us to formulate the following conjecture:

Conjecture 1. *No potential t-subgraph of a Moore graph of diameter 2 and degree 57 can be obtained by the cyclic construction for $t \geq 21$.*

However, Theorem 1 shows that the Moore graph cannot be obtained by the cyclic construction and so removes much of the incentive for attempting to prove Conjecture 1.

More generally, an attempt to construct a potential t-subgraph of a Moore graph of diameter 2 and degree 57 without assuming a cyclic construction or any group of derangements can be made using the algorithm described in [5]. The algorithm only needs minor adjustments to account for the different vertex degrees. The smallest deficit that has been obtained is 915 [10], which suggests a more general conjecture:

Conjecture 2. *No potential t-subgraph of a Moore graph of diameter 2 and degree 57 can be obtained for $t \geq 21$.*

Conjecture 2 would imply the non-existence of the Moore graph, and so a proof cannot be easily obtained. However, the conjecture does at least suggest a smaller graph for a non-existence proof than the Moore graph itself.

The work in this paper is the first part of an approach to divide the problem of the existence of the Moore graph into a number of distinct problems. The next case to consider is when the derangements used in Section 4 are taken from any group of derangements. A permutation group is called *semiregular* if for any selected point, the only permutation fixing it is the identity [13]. Thus the definitions of semiregular group and group of derangements are essentially the same. The following proposition can be found in [13].

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 $i_1 \neq i_2, i_1 \neq i_3, i_2 \neq i_3$ $\Phi_{i_1 i_2} \neq \Phi_{i_1 i_3}$.*

Proof. Assume $\Phi_{i_1 i_2} = \Phi_{i_1 i_3}$. Recall that $\Phi_{i_2 i_1} = \Phi^{-1}_{i_1 i_2}$. As both Φ_{1i} and Φ_{i1} are the identity permutation for all $2 \leq i \leq k$, $\Phi_{1i_2}\Phi_{i_2 i_1}\Phi_{i_1 i_3}\Phi_{i_3 1} = \Phi_{1i_2}\Phi_{i_2 i_1}\Phi_{i_1 i_2}\Phi_{i_3 1} = \Phi_{1i_2}\Phi^{-1}_{i_1 i_2}\Phi_{i_1 i_2}\Phi_{i_3 1} = \Phi_{1i_2}\Phi_{i_3 1} = \Phi_{1i_2}\Phi_{1i_3}$ is the identity permutation. For any choice of fixed point p' of this identity permutation, vertices $(1, p'), (i_2, p'), (i_1, p''), (i_3, p'), (1, p')$ would form a cycle of length 4, which is a contradiction. □

It follows from Propositions 1 and 2 that the group of derangements used would have to have order $k - 1 = 56$. This should make the group of derangements case somewhat easier than the remaining general case, where a massive number of derangements is possible.

Definition 2. *A* transversal *in a group table is a set of entries, one selected from each row and each column such that no two entries contain the same symbol.*

In the proof of Theorem 1, a partial transversal of the additive group of $\mathbf{Z}_{k-1}$ is essentially used, omitting rows, columns, and entries for 0 and 1. The non-existence result for this partial transversal is stronger than that for the full transversal. It is well known that no transversal exists in the addition table of $\mathbf{Z}_{k-1}$ for $k - 1$ even, but transversals do exist for $k - 1$ odd. When other groups of derangements are considered, most groups do have many transversals [14]. It seems unlikely that general non-existence results could be proved for partial transversals. Thus any proof for a general group of derangements would probably need to consider a larger configuration of permutations Φ_{ij} than is used in the proof of Theorem 1.

Now consider elements Φ_{ij} of the permutation group for which $\Phi_{ij} = \Phi^{-1}_{ij} = \Phi_{ji}$ (involutions). Treating the set $\{i \mid 2 \leq i \leq k\}$ as the set of vertices of a complete graph K_{k-1}, it can be seen from Proposition 2 that the set of all edges $(i'j')$ with $\Phi_{i'j'} = \Phi_{ij}$ form an isolated set of edges (with no pair of edges sharing an end vertex). On the other hand, if Φ_{ij} is not an involution, Proposition 2, together with the fact that the group has $k - 2$ non-identity elements, implies that $\Phi_{ij} = \Phi_{j\ell}$ with $\ell \neq i$. In a similar way, if Φ_{ij} is not an involution, $\Phi_{ij} = \Phi_{\ell j}$ with $\ell \neq i$. It then follows that the set of all edges $(i'j')$ with $\Phi_{i'j'} = \Phi_{ij}$ is a union of disjoint cycles (or possibly a single cycle). However, in both cases additional conditions are necessary to ensure girth 5.

The remaining case, when the permutations are not all elements of a group of derangements, might usefully be split into three sub-cases:

1. The permutations are all involutions.
2. None of the permutations are involutions.
3. The permutations are a mixture of involutions and involutions.

It can be observed that the construction of the (unique) Hoffman–Singleton graph presented in [3] uses only involutions (not forming a group). The involutions used are (in the notation used here) shown in Figure 5.

$\Phi_{23} = (01)(23)(45)$
$\Phi_{24} = (02)(14)(35)$
$\Phi_{25} = (03)(15)(24)$
$\Phi_{26} = (04)(13)(25)$
$\Phi_{27} = (05)(12)(34)$
$\Phi_{34} = (05)(13)(24)$
$\Phi_{35} = (04)(12)(35)$
$\Phi_{36} = (02)(15)(34)$
$\Phi_{37} = (03)(14)(25)$
$\Phi_{45} = (01)(25)(34)$
$\Phi_{46} = (03)(12)(45)$
$\Phi_{47} = (04)(15)(23)$
$\Phi_{56} = (05)(14)(23)$
$\Phi_{57} = (02)(13)(45)$
$\Phi_{67} = (01)(24)(35)$

Figure 5. The involutions used in the construction of the Hoffman–Singleton graph.

It can be observed that in the case of $k = 7$, there are 15 derangements necessary and with $k - 1 = 6$ there are 15 derangement involutions available. This makes the selection of derangements to use fortuitously easy. In general, the number of derangements that are involutions is $(k-2) \times (k-4) \times \ldots \times 1$, which is massively greater than the number $(k-1) \times (k-2)/2$ of derangements required for $k = 57$.

Irrespective of whether only involutions are used or not, one approach for $k = 57$ might be to replace the derangements Φ_{ij} labelling oriented edges of K_{k-1} by sets of derangements

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

There are $k - 2$ such sets and a result similar to Proposition 2 can be proved.

8. Conclusions

The problem of resolving the existence or non-existence of a Moore graph of diameter 2 and degree 57 can be split into three cases. In the first case, the derangements described in Section 4 are cyclic permutations, dealt with as described in Section 5. Although this has proved useful in constructing t-subgraphs, Theorem 1 presented in Section 6 excludes this possibility of using a cyclic group of derangements for the Moore graph itself. For the second case it would be interesting to consider using other groups of derangements. It appears that any proof would probably need to consider a larger configuration of derangements Φ_{ij} than is used in the proof presented here. Some basic ideas for dealing with this case were presented in Section 7. The final case, when the derangements are not selected from a group of derangements may be much harder to resolve, with no special structure to exploit.

The question of the existence of the Moore graph of diameter 2 and degree 57 has proved frustrating for many decades. The results presented in [5] and here add to the belief of many that the graph does not exist. However, a complete proof of this remains elusive. Most counting arguments seem to fail as they must allow $k = 7$ but exclude $k = 57$.

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.

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

References

1. Miller, M.; Širáň, J. Moore graphs and beyond: A survey of the degree/diameter problem. *Electron. J. Comb.* **2013**, *20*, 1–92.
2. Dalfó, C. A survey on the missing Moore graph. *Linear Algebra Appl.* **2019**, *569*, 1–14.
3. Hoffman, A.J.; Singleton, R.R. On Moore graphs with diameters 2 and 3. *IBM J. Res. Dev.* **1960**, *4*, 497–504.
4. Biggs, N. *Algebraic Graph Theory*; Cambridge Tracts in Mathematics, No. 67; Cambridge University Press: Cambridge, UK, 1974.
5. Smith, D.H.; Montemanni, R. The missing Moore graph as an optimization problem. *EURO J. Comput. Optim.* **2023**, *11*, 100060.
6. Mačaj, M.; Širáň, J. Search for properties of the missing Moore graph. *Linear Algebra Appl.* **2010**, *432*, 2381–2398.
7. Aschbacher, M. The nonexistence of rank three permutation groups of degree 3250 and subdegree 57. *J. Algebra* **1971**, *19*, 538–540.
8. 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.
9. Makhnev, A.A.; Paduchikh, D.V. Automorphisms of Aschbacher graphs. *Algebra Log.* **2001**, *40*, 69–74.
10. Smith, D.H. (Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd, Wales, UK). Personal communication, 2026.
11. Smith, D.H.; Montemanni, R. Potential subgraphs of the missing Moore graph. *Symmetry* **2024**, *16*, 1563.
12. Google OR-Tools. Available online: https://developers.google.com/optimization/ (accessed on 20 March 2026).
13. Wielandt, H. *Finite Permutation Groups*; Academic Press: New York, NY, USA, 1964.
14. McKay, B.D.; McLeod, J.C.; Wanless, I.M. The number of transversals in a Latin square. *Des. Codes Cryptogr.* **2006**, *40*, 269–284.