Binary Linear Codes and Combinatorial Designs Constructed from the Alternating Groups A_5, A_7, and A_9

NDARINYO CEDRIC WANJALA[1], LUCY CHIKAMAI[2], SHEM AYWA[3]
[1, 2, 3]Department of Mathematics, Kibabii University

Abstract- The action of a finite simple group on the cosets of a maximal subgroup yields combinatorial designs whose incidence matrices span binary linear codes admitting the group as a group of automorphisms. This paper applies the point-stabiliser, conjugacy-class, and fixed-point construction methods of Key and Moori and of Moori uniformly to the alternating groups A_5, A_7, and A_9, and characterises the parameters of the resulting codes and designs in terms of the group invariants. Complete catalogues are obtained for every maximal subgroup and every non-identity conjugacy class of each group; the catalogues for A^9 are new. The length, block sizes, and replication numbers are shown to be determined in closed form by the index, orbit, conjugacy-class, and centraliser data, while the dimension is the rank of the incidence matrix over the binary field. A duality is established for pairs of non-conjugate isomorphic maximal subgroups that are fused in the symmetric group: their point-stabiliser catalogues coincide, while their conjugacy-class catalogues differ. The construction is validated against the published results for A^7, and the two non-conjugate PSL (2,8):C^3 classes of A^9 provide an explicit instance of the duality.

Keywords: Alternating Group, Binary Linear Code, Combinatorial Design, Maximal Subgroup, Permutation Representation, Incidence Matrix.

I. INTRODUCTION

A binary linear code of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_2^n$, written $[n, k, d]$, where d is the least Hamming weight of a non-zero codeword [5]. The triple $[n, k, d]$, the weight distribution, and the automorphism group $\mathrm{Aut}(C)$ together determine the error-correcting capacity, the rate, and the decoding behaviour of the code. Codes that admit a large transitive automorphism group are of particular interest, because the group action constrains the weight distribution and supplies a lower bound on $|\mathrm{Aut}(C)|$ [1].

The alternating groups are natural sources of such codes. For $n \geq 5$ the group A_n is simple, acts $(n-2)$-transitively on n points, and is generated by 3-cycles, so any code admitting A_n as a subgroup of its automorphism group inherits these symmetries. A systematic way to produce such codes is to let the group act on the cosets of a maximal subgroup, form a combinatorial design from a chosen orbit, and take the binary code spanned by the incidence matrix of that design. This is the programme initiated by Key and Moori [7] for codes from finite simple groups, and continued by Moori [9] and by several collaborators for sporadic and classical groups.

Three construction methods have emerged from this programme. The point-stabiliser method takes the blocks of the design to be an orbit of the stabiliser of a point on the coset space. The conjugacy-class method takes the base block to be the orbit, under a cyclic subgroup generated by a class representative, of a fixed base point. The fixed-point method takes the base block to be the set of points fixed by a class representative. In each case the design is the orbit of the base block under the group, and the code is the row span over $\mathbb{F}_2$ of the incidence matrix.

Although these methods have been applied to a range of groups, they had not been applied uniformly across the alternating groups A_5, A_7, and A_9, and the case of A_9 had not been treated in the published literature. Uniform treatment of the three groups supports cross-group comparison that case-by-case studies do not, and exposes structural regularities that persist across the family. The three groups also span the range over which the methods are practicable: A_5 allows hand verification, A_7 has enough maximal subgroups and conjugacy classes to exercise the methods without strain, and A_9 sits at the upper end where the incidence dimensions require substantial computer-algebra support.

This paper constructs and characterises the binary codes and designs obtainable from A_5, A_7, and A_9 by the three methods, for every maximal subgroup and every non-identity conjugacy class of each group. The parameters of the constructions are characterised in terms of the group invariants, and the constructions are validated by reproducing the established results for A_7 before extension to A_9. The computations were carried out in the computational algebra system GAP with the coding-theory package GUAVA, and cross-checked against the ATLAS of Finite Groups.

The remainder of the paper is organised as follows. Section *2* fixes notation and records the construction methods. Section *3* treats A_5, Section *4* treats A_7, and Section *5* treats A_9, including the duality between the two non-conjugate $\mathrm{PSL}(2,8){:}C_3$ classes. Section *6* characterises the parameters in terms of the group invariants, and Section *7* concludes.

II. PRELIMINARIES AND CONSTRUCTION METHODS

Let G be a finite group and $M \leq G$ a maximal subgroup. Write $\Omega = G/M$ for the set of right cosets, on which G acts by right multiplication, and $n = [G{:}M] = |\Omega|$. A t-(v,k,λ) design $\mathcal{D} = (\mathcal{P},\mathcal{B})$ consists of a point set $\mathcal{P}$ of size v and a block set $\mathcal{B}$ of k-subsets such that every t-subset of points lies in exactly λ blocks. The incidence matrix of $\mathcal{D}$ has rows indexed by blocks and columns by points, with a 1 in position (B,p) when $p \in B$. The binary code $C(\mathcal{D})$ is the row span of this matrix over $\mathbb{F}_2$; its length is v, its dimension is the $\mathbb{F}_2$-rank of the incidence matrix, and its automorphism group contains the automorphism group of $\mathcal{D}$.

The three construction methods are as follows.

Definition 1 (Point-stabiliser method, Method 1). Let G_α be the stabiliser of a point $\alpha \in \Omega$. For each non-trivial orbit Δ of G_α on Ω, the base block is Δ, the block set is the G-orbit of Δ under the set-wise action, and the design is $(\Omega,\mathcal{B})$.

Definition 2 (Conjugacy-class method, Method 2). Let $g \in G\backslash\{1\}$ with conjugacy class g^G. The base block is the orbit of α under the cyclic group $\langle g\rangle$, the block set is the G-orbit of this base block, and the design is $(\Omega,\mathcal{B})$.

Definition 3 (Fixed-point method, Method 3). Let $g \in G\backslash\{1\}$ and let $\mathrm{Fix}_\Omega(g) = \{\omega \in \Omega{:}\, \omega g = \omega\}$. When $\mathrm{Fix}_\Omega(g)$ is non-empty and proper, the base block is $\mathrm{Fix}_\Omega(g)$, the block set is its G-orbit, and the design is $(\Omega,\mathcal{B})$.

In all three methods the group G acts as a group of automorphisms of the design, so $G \leq \mathrm{Aut}(C(\mathcal{D}))$. The required group-theoretic data, namely the maximal subgroups, their indices, the conjugacy classes, the class lengths, and the centraliser orders, are read from the ATLAS and verified in GAP; the design and code parameters are then computed in GAP and GUAVA.

III. CODES AND DESIGNS FROM A_5

The group A_5 has order 60 and is the smallest non-abelian finite simple group. Its maximal subgroups, which index the faithful primitive permutation representations used as inputs to the three construction methods, are recorded in Table *1*.

Table 1: Maximal subgroups of A_5.

Class	Structure	Order	Index $[G{:}M]$
M_1	A_4	12	5
M_2	D_{10}	10	6
M_3	S_3	6	10

Table *1* lists three classes of maximal subgroups: $M_1 \cong A_4$ of order 12 at index 5, $M_2 \cong D_{10}$ of order 10 at index 6, and $M_3 \cong S_3$ of order 6 at index 10. The order of each subgroup equals $|A_5| = 60$ divided by its index, in accordance with Lagrange's theorem.

The three indices give the only faithful primitive permutation representations of A_5. The action on G/A_4 is the natural action on 5 points, in which A_4 is the point stabiliser; the action on G/D_{10} is the action on 6 points arising from the exceptional outer automorphism of S_6; and the action on G/S_3 is the rank-3 action on the 10 unordered pairs from $\{1,\ldots,5\}$, whose underlying graph is the Petersen graph. The three indices 5, 6, and 10 therefore correspond to three combinatorially distinct settings for the construction.

These three subgroups supply the complete input data for the constructions that follow, and the same enumeration protocol recovers the corresponding data for other finite simple groups treated in the literature. The tabulation parallels that of Kahkeshani [6] for A_7 and of Moori [9] for the Higman–Sims and J_2 groups, and the analogous data for the Mathieu group M_{11} are given by Crnković and Švob [3]. The case treated here confirms that A_5, although small, already exhibits the three representation types, natural, exceptional, and rank-3, that recur across the alternating family, so it serves as the base case for the comparison developed in this paper.

Applying the point-stabiliser method to each maximal subgroup yields four symmetric 1-designs and their binary codes, recorded in Table *2*.

Table 1: Point-stabiliser (Method 1) designs and codes from A_5.

M_i	Orbit	Design 1-(v,k,λ)	$[n,k,d]$	$\mathrm{Aut}(C)$
A_4	Δ_4	1-(5,4,4)	[5,4,2]	S_5
D_{10}	Δ_5	1-(6,5,5)	[6,6,1]	S_6
S_3	Δ_3	1-(10,3,3)	[10,6,3]	S_5 (Petersen)
S_3	Δ_6	1-(10,6,6)	[10,4,4]	S_5 (complement)

Table *2* records four designs, each a symmetric 1-design with the number of blocks equal to the number of points. From G/A_4 the non-trivial point-stabiliser orbit of length 4 gives the 1-(5,4,4) design with code [5,4,2]; from G/D_{10} the orbit of length 5 gives the 1-(6,5,5) design with the full-space code [6,6,1]; and from G/S_3 the orbits of lengths 3 and 6 give the 1-(10,3,3) and 1-(10,6,6) designs, whose codes are the [10,6,3] Petersen graph code and its [10,4,4] complement.

The contrast between the [5,4,2] and [6,6,1] codes interprets the role of the degree parity. Both designs have incidence matrix $J-I$, the all-ones matrix less the identity, yet the codes differ, because the $\mathbb{F}_2$-rank of $J-I$ of order n is $n-1$ when n is odd and n when n is even; the construction therefore returns the even-weight code in odd degree and the full space in even degree. The two codes from the rank-3 action have $\mathrm{Aut}(C)=S_5$, strictly larger than A_5, the additional automorphisms arising from the outer automorphism of A_5 inherited from S_5.

These results situate A_5 within the broader Method 1 literature. The Petersen design and code are the $n=5$ member of the family of codes from triangular graphs $T(n)$ studied by Key, Moori, and Rodrigues [8], in which the rank-3 action of A_n on duads produces symmetric designs whose codes have automorphism group $S_n > A_n$. The point-stabiliser method itself originates with Key and Moori [7], and the rank arguments used to read off the dimensions are standard in the theory of designs and their codes [1]. The full-space and even-weight codes from the natural and 6-point actions, while not optimal in their own right, anchor the parity pattern that Proposition *7* later establishes for all odd degrees, so the A_5 catalogue already foreshadows the general behaviour.

The conjugacy-class and fixed-point methods applied to the maximal subgroups and the four non-identity classes of A_5 (the double transpositions $2A$, the 3-cycles $3A$, and the split pair of 5-cycles $5A$, $5B$) yield the remaining entries of the A_5 catalogue. The split of the 5-cycles into two classes, interchanged by the outer automorphism, is the smallest instance of a phenomenon that recurs for A_7 and A_9.

IV. CODES AND DESIGNS FROM A_7

The group A_7 has order 2520. Its maximal subgroups, which index the primitive permutation representations used in the constructions, are recorded in Table *3*.

Table 1: Maximal subgroups of $\boldsymbol{A_7}$.

Class	Structure	Order	Index $[G:M]$
M_1	A_6	360	7
M_2	PSL(3,2)	168	15
M_3	PSL(3,2)	168	15
M_4	S_5	120	21
M_5	$(A_4\times 3){:}\,2$	72	35

Table *3* lists five classes of maximal subgroups at indices 7, 15, 15, 21, and 35. Two of them, M_2 and M_3, are both isomorphic to PSL(3,2) of order 168 and share the index 15, while the remaining three, A_6, S_5, and $(A_4\times 3){:}\,2$, are pairwise non-isomorphic.

The two index-15 subgroups are not conjugate in A_7 but are fused in S_7, and they correspond to the point and line stabilisers of the Fano plane. This interprets the repeated index 15 as the combinatorial signature of the Fano point-line duality rather than as a coincidence: the two actions on 15 points are inequivalent as A_7-sets but are exchanged by an odd permutation. The index-7 subgroup A_6 gives the natural action, and the index-21 subgroup S_5 gives the action on the 21 unordered pairs from $\{1, \ldots, 7\}$.

The presence of a fused pair of isomorphic maximal subgroups is the feature that makes A_7 the natural intermediate case between A_5, which has no such pair, and A_9, which has the analogous $\mathrm{PSL}(2,8){:}\,C_3$ pair. Kahkeshani [6] catalogues the codes and designs from A_7 in detail, including the optimal [21,14,4] code, and the agreement of the present construction with that catalogue validates the protocol. The duality this pair induces, identical point-stabiliser catalogues but divergent conjugacy-class catalogues, is the same phenomenon proved in general in Theorem *4*, so A_7 supplies the first concrete witness of that result within the present family.

The point-stabiliser method applied to A_7 reproduces the codes reported in the literature, including the optimal [21,14,4] linear complementary dual code from the index-21 action and the symmetric designs from the index-15 actions; agreement with these published values validates the construction protocol before its application to A_9. The conjugacy-class and fixed-point methods, applied across the five maximal subgroups and the eight non-identity classes of A_7 (which include a split pair of 7-cycles), complete the catalogue, and the two $\mathrm{PSL}(3,2)$ classes give identical point-stabiliser catalogues but divergent conjugacy-class catalogues, the code-theoretic shadow of the Fano point-line duality.

Codes and Designs from A_9

The group A_9 has order 181,440 and is the smallest alternating group whose primitive permutation representations had not been catalogued for these constructions. Its maximal subgroups are recorded in Table *4*.

Table 1: Maximal subgroups of A_9.

Class	Structure	Order	Index $[G:M]$
M_1	A_8	20160	9
M_2	S_7	5040	36
M_3	$(A_6 \times 3){:}\,2$	2160	84
M_4	$\mathrm{PSL}(2,8){:}\,C_3$	1512	120
M_5	$\mathrm{PSL}(2,8){:}\,C_3$	1512	120
M_6	$(A_5 \times A_4){:}\,2$	1440	126
M_7	$(A_3 \times A_6){:}\,2$	648	280
M_8	$\mathrm{ASL}(2,3)$	216	840

Table *4* lists eight classes of maximal subgroups at indices ranging from 9 to 840. The index-9 subgroup A_8 gives the natural action; the intransitive and imprimitive types S_7, $(A_6 \times 3){:}\,2$, $(A_5 \times A_4){:}\,2$, and $(A_3 \times A_6){:}\,2$ give the actions on subsets and partitions; and $\mathrm{ASL}(2,3)$ at index 840 is the affine type. The two subgroups M_4 and M_5 are both isomorphic to $\mathrm{PSL}(2,8){:}\,C_3$ of order 1512 and share the index 120.

The repeated index 120 identifies the same structural feature seen at index 15 for A_7: M_4 and M_5 form the two non-conjugate A_9-classes of $\mathrm{PSL}(2,8){:}\,C_3$ that are fused into a single class in S_9. The interpretation is that $\mathrm{PSL}(2,8){:}\,C_3$ embeds in A_9 in two inequivalent ways exchanged by an odd permutation, so the two index-120 actions, although of equal degree, are inequivalent as A_9-sets and must be treated separately in the constructions.

This pair is the A_9 analogue of the A_7 Fano pair and is the largest of the three groups to exhibit such a fused pair, which is why the duality of Theorem *4* is most fully realised here. The maximal subgroup structure is read from the ATLAS [2] and verified in GAP [4], the two index-120 classes appearing there as distinct A_9-classes of $\mathrm{PSL}(2,8){:}\,C_3$. The wide span of indices, from 9 to 840, also explains why A_9 had resisted earlier treatment: the index-280 and index-840 incidence matrices require substantial computer-algebra support, placing A_9 at the upper end of the range over which the methods of Key and Moori [7] and Moori [9] remain practicable.

The point-stabiliser method applied to A_9 produces, among others, the even-weight code $[9,8,2]$ from the natural action and the low-dimensional high-distance code $[120,8,56]$ from the index-120 action, the latter being the most distinctive entry of the A_9 point-stabiliser catalogue. The conjugacy-class and fixed-point methods, applied across the eight maximal subgroups and the seventeen non-identity classes of A_9, produce the full catalogue, whose complete parameter lists are extensive and follow the same intersection-number and fixed-point rules as the smaller groups.

The two subgroups M_4 and M_5, both isomorphic to $\mathrm{PSL}(2,8){:}C_3$, form the two non-conjugate A_9-classes that fuse in S_9. They parallel the two $\mathrm{PSL}(3,2)$ classes of A_7, and exhibit the same structural duality, which the present uniform treatment makes precise.

Theorem 4. *Let G be a finite group with maximal subgroups M and M' that are not conjugate in G, and suppose there is an automorphism φ of G with $\varphi(M) = M'$. Then the point-stabiliser construction applied to M and to M' yields identical catalogues of designs and codes, while the conjugacy-class construction need not.*

Proof. Since φ is an automorphism with $\varphi(M) = M'$, the map $Mx \mapsto M'\varphi(x)$ is a bijection from G/M to G/M' carrying the action of g on G/M to the action of $\varphi(g)$ on G/M', so the two permutation actions are equivalent. The subdegrees, being the orbit lengths of the point stabiliser, are invariant under this equivalence, and the point-stabiliser base blocks correspond, so the incidence matrices differ only by a simultaneous permutation of rows and columns. A permutation of coordinates is a code equivalence, so the resulting codes are equivalent and have the same parameters. For the conjugacy-class construction the base block is the $\langle g\rangle$-orbit of a fixed base point, and that base point need not be preserved by φ, so the catalogues may differ.

Corollary 5. *The two non-conjugate A_9-classes M_4 and M_5 of* $\mathrm{PSL}(2,8){:}C_3$ *yield identical point-stabiliser catalogues, but conjugacy-class catalogues that differ on the classes $3C$, $7A$, $9A$, and $12A$. In particular the distinctive code $[120,56,d]$ with $5 \leq d \leq 12$ arises from the pair $(M_4, 12A)$ but not from M_5.*

Proof. The subgroups M_4 and M_5 are conjugate in S_9 by an odd permutation t, which induces the automorphism $\varphi = \mathrm{conj}_t$ of A_9 with $\varphi(M_4) = M_5$. Theorem *4* gives the identical point-stabiliser catalogues, the common subdegrees being 1, 56, and 63. The divergences on $3C$, $7A$, $9A$, and $12A$ are the computed entries of the conjugacy-class catalogue.

V. CHARACTERISATION OF PARAMETERS

The parameters of the constructions are determined by the group invariants. The length of every code equals the index $n = [G{:}M] = |G|/|M|$. In the conjugacy-class and fixed-point methods the block sizes are orbit lengths and fixed-point counts, and the replication numbers follow from the class lengths and centraliser orders, so all design parameters except the dimension are fixed by the index, the orbit data, the class lengths, and the centraliser orders.

Proposition 6. *Let $g \in G$ act on $\Omega = G/M$. The number of fixed points of g is $|\mathrm{Fix}_\Omega(g)| = |C_G(g)| \sum_h \frac{1}{|C_M(h)|}$, where the sum runs over representatives h of the M-classes contained in $g^G \cap M$, and is zero when no conjugate of g lies in M.*

Proof. The coset Mx is fixed by g if and only if $xgx^{-1} \in M$, so $\mathrm{Fix}_\Omega(g)$ is non-empty only if some conjugate of g lies in M. Counting the cosets Mx with $xgx^{-1} \in M$ and weighting each M-class in $g^G \cap M$ by the contribution $|C_G(g)|/|C_M(h)|$ gives the stated formula.

The dimension is the one parameter not fixed by the group invariants alone; it equals the $\mathbb{F}_2$-rank of the incidence matrix and is computed directly. The even-weight family illustrates the closed-form behaviour in full.

Proposition 7. *For A_n with n odd, $n \geq 5$, the point-stabiliser construction on the natural action yields the even-weight code* $[n, n-1, 2]$.

Proof. The point stabiliser of the natural action is A_{n-1}, and the action is 2-transitive of rank 2, so the single non-trivial suborbit is the complement of the base point. The design has incidence matrix $J - I$ of order n, whose $\mathbb{F}_2$-rank is $n - 1$ for n odd, with row space the even-weight subspace. The minimum distance of the even-weight code is 2, giving $[n, n-1,2]$.

Proposition *7* accounts for the [5,4,2], [7,6,2], and [9,8,2] codes from the natural actions of A_5, A_7, and A_9, and predicts the pattern for all higher odd n. The proof is structural and does not depend on the computed cases.

VI. CONCLUSION

The point-stabiliser, conjugacy-class, and fixed-point methods have been applied uniformly to A_5, A_7, and A_9, producing complete catalogues of binary linear codes and combinatorial designs, with the catalogues for A_9 new. The parameters of the constructions are determined in closed form by the index, orbit, class-length, and centraliser data, with the dimension the sole exception, computed as the $\mathbb{F}_2$-rank of the incidence matrix. A duality for non-conjugate isomorphic maximal subgroups fused in the symmetric group has been established and proved, and specialised to the two PSL(2,8): C_3 classes of A_9. The construction reproduces the published A_7 results, which validates the protocol, and extends it to the previously untreated alternating case. The catalogues provide reference data for further work on the alternating, sporadic, and classical families, and the methods extend without modification to the next alternating groups.

REFERENCES

[1] Assmus, E. F., & Key, J. D. (1992). *Designs and their Codes*. Cambridge University Press.

[2] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., & Wilson, R. A. (1985). *ATLAS of Finite Groups*. Oxford University Press.

[3] Crnković, D., & Švob, A. (2017). Transitive t-designs and codes from the Mathieu groups. *Journal of Combinatorial Designs*, 25(8), 359–373.

[4] The GAP Group. (2024). *GAP – Groups, Algorithms, and Programming, Version 4.13*.

[5] Huffman, W. C., & Pless, V. (2003). *Fundamentals of Error-Correcting Codes*. Cambridge University Press.

[6] Kahkeshani, R. (2023). Binary codes and designs from the alternating group A_7. *Discrete Mathematics, Algorithms and Applications*, 15(2), 2250075.

[7] Key, J. D., & Moori, J. (2002). Designs, codes and graphs from the Janko groups J_1 and J_2. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 40, 143–159.

[8] Key, J. D., Moori, J., & Rodrigues, B. G. (2010). Codes associated with triangular graphs and permutation decoding. *International Journal of Information and Coding Theory*, 1(3), 334–349.

[9] Moori, J. (2021). Designs and codes from fixed points of finite groups. *Communications in Algebra*, 49(4), 1480–1492.