A FINITE SIMPLE GROUP IS CCA IF AND ONLY IF IT HAS NO ELEMENT OF ORDER FOUR

LUKE MORGAN, JOY MORRIS, AND GABRIEL VERRET

Abstract. A Cayley graph for a group G is *CCA* if every automorphism of the graph that preserves the edge-orbits under the regular representation of G is an element of the normaliser of G. A group G is then said to be *CCA* if every connected Cayley graph on G is CCA. We show that a finite simple group is CCA if and only if it has no element of order 4. We also show that "many" 2-groups are non-CCA.

1. Introduction

All groups and all graphs in this paper are finite. Let G be a group and let S be an inverse-closed subset of G. The *Cayley graph* $\mathrm{Cay}(G,S)$ of G with respect to S is the graph with vertex-set G and, for every $g \in G$ and $s \in S$, an edge $\{g, sg\}$. This graph admits a natural edge-colouring in which an edge $\{g, sg\}$ is coloured $\{s, s^{-1}\}$. The colour-preserving automorphism group is denoted $\mathrm{Aut}_c(\mathrm{Cay}(G,S))$ and we define $\mathrm{Aut}_{\pm 1}(G,S) = \{\alpha \in \mathrm{Aut}(G) \mid s^\alpha \in \{s, s^{-1}\} \text{ for all } s \in S\}$. It is easy to see that $G_R \rtimes \mathrm{Aut}_{\pm 1}(G,S) \leqslant \mathrm{Aut}_c(\mathrm{Cay}(G,S))$, where G_R is the right-regular representation of G and, in fact, the former group is precisely the normaliser of G_R in $\mathrm{Aut}_c(\mathrm{Cay}(G,S))$.

Definition 1.1 ([15])**.** The Cayley graph $\mathrm{Cay}(G,S)$ is *CCA* (Cayley colour automorphism) if $\mathrm{Aut}_c(\mathrm{Cay}(G,S)) = G_R \rtimes \mathrm{Aut}_{\pm 1}(G,S)$. The group G is *CCA* if every connected Cayley graph on G is CCA.

Thus, $\mathrm{Cay}(G,S)$ is CCA if and only if G_R is normal in $\mathrm{Aut}_c(\mathrm{Cay}(G,S))$, c.f. [15, Remark 6.2]. Note that $\mathrm{Cay}(G,S)$ is connected if and only if S generates G.

Previous results on the CCA problem have focused on groups of odd order and, more generally, on solvable groups (see [9] and [15] for example). In this paper, we will focus on two ends of the spectrum of groups: non-abelian simple groups and 2-groups.

In Section 2, we introduce some basic terminology and previous results on the CCA problem. In particular, Proposition 2.2 is a condition from [15] that is sufficient to guarantee that a group is non-CCA. This condition requires the group to contain elements of order four. We also include various results that will allow us to apply this condition to many of the groups we study in this paper.

2010 *Mathematics Subject Classification.* Primary 05C25.

Key words and phrases. CCA problem, Cayley graphs, edge-colouring, 2-groups, finite simple groups.

This research was supported by the Australian Research Council grants DE130101001 and DE160100081, by the Natural Science and Engineering Research Council of Canada, and by the Cheryl E. Praeger Visiting Research Fellowship from The University of Western Australia.

In Section 3 we focus on 2-groups. We show that a lower bound on the number of groups of order 2^n that are non-CCA has the same leading term as the total number of groups of order 2^n. In Sections 4 and 5 we prove the following.

Theorem 1.2. *A finite simple group is CCA if and only if it has no element of order four.*

This theorem also holds for almost simple groups whose socle is either an alternating group or a Suzuki group; the proof of this is also in Section 5.

The proof of Theorem 1.2 involves some case-by-case analysis of finite simple groups, and relies on their classification.

2. Preliminaries

We begin by describing a sufficient criterion for a group to be non-CCA that appeared in [15]. This criterion is surprisingly powerful, as will be made abundantly clear in Sections 3 and 5. We first need the following definition.

Definition 2.1. Let G be a group. A *non-CCA triple* of G is a triple (S, T, τ) where S and T are subsets of G and τ is an involution in G such that the following hold:

(Ai) $G = \langle S \cup T \rangle$;
(Aii) τ inverts or centralises every element of S;
(Aiii) $t^2 = \tau$ for every $t \in T$;
(Aiv) $\langle S \cup \{\tau\} \rangle \neq G$;
(Av) either τ is non-central in G or $|G : \langle S \cup \{\tau\} \rangle| > 2$.

We may sometimes abuse notation and write (S, t, τ) for the non-CCA triple (S, T, τ) when $T = \{t\}$.

Proposition 2.2 ([15, Proposition 2.5])**.** *If (S, T, τ) is a non-CCA triple of G, then $\mathrm{Cay}(G, S \cup T)$ is connected and non-CCA and thus G is non-CCA.*

For G a group and τ an involution of G, we set

$$S_G(\tau) = (C_G(\tau) \cup \{y\tau \mid y \in G \text{ and } y^2 = 1\}) - \{1\}.$$

Remark 2.3. The subgroup $\langle S_G(\tau) \rangle$ contains every involution of G, and thus contains the normal subgroup of G generated by the set of involutions of G.

The following lemmas prove useful in allowing us to apply Proposition 2.2.

Lemma 2.4. *If G is a group with an involution τ, then*

$$S_G(\tau) = \{x \in G \mid x^\tau \in \{x, x^{-1}\}\}.$$

Proof. By definition, $x^\tau = x$ if and only if $x \in C_G(\tau)$. If $u = y\tau$ with $y^2 = 1$, then $u^\tau = \tau y \tau\tau = \tau y = \tau^{-1} y^{-1} = (y\tau)^{-1} = u^{-1}$. In the other direction, if $x^\tau = x^{-1}$, then $(x\tau)^2 = 1$ hence $x = (x\tau)\tau \in S_G(\tau)$, as required. □

Remark 2.5. Lemma 2.4 shows that (Aii) of Definition 2.1 holds whenever we use some $S_G(\tau)$ as the first entry of a putative non-CCA triple, with τ as the final entry. This fact will be used repeatedly throughout Section 5, usually without explicit reference.

We now state two results on colour-preserving automorphisms of Cayley graphs.

Lemma 2.6 ([15, Lemma 6.3])**.** *The vertex-stabiliser in the colour-preserving group of automorphisms of a connected Cayley graph is a 2-group.*

Lemma 2.7 ([17, Lemma 2.4])**.** *Let $\Gamma = \mathrm{Cay}(G, S)$, let A be a colour-preserving group of automorphisms of Γ, let N be a normal 2-subgroup of A and let K be the kernel of the action of A on the N-orbits. If $K_v \neq 1$ for some $v \in \Gamma$, then S contains an element of order four.*

3. Many 2-groups are not CCA

Abelian CCA groups were determined in [15, Proposition 4.1]. From this classification, it follows that, while the number of abelian CCA groups of order 2^n increases with n, almost all abelian 2-groups are non-CCA. We are not able to prove a result quite this strong for all 2-groups but, using a slightly modified version of an argument of Higman, we get the following.

Theorem 3.1. *There are at least $2^{\frac{2}{27}n^3+O(n^2)}$ pairwise non-isomorphic groups of order 2^n that are non-CCA.*

Proof. We assume that $n \geqslant 3$, and follow the account by Sims [20, pg.151–152] of a result of Higman [14, Theorem 2.1]. Let r and s be positive integers such that $r + s = n$. For $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant s$, let $b(i, j) \in \{0, 1\}$. For $1 \leqslant i < j \leqslant r$ and $1 \leqslant k \leqslant s$, let $c(i, j, k) \in \{0, 1\}$. The relations

$$\begin{array}{rcll} h_i^2 & = & 1, & 1 \leqslant i \leqslant s, \\ [h_i, h_j] & = & 1, & 1 \leqslant i \leqslant j \leqslant s, \\ [g_i, h_j] & = & 1, & 1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s, \\ g_i^2 & = & h_1^{b(i,1)} \cdots h_s^{b(i,s)}, & 1 \leqslant i \leqslant r, \\ [g_i, g_j] & = & h_1^{c(i,j,1)} \cdots h_s^{c(i,j,s)}, & 1 \leqslant i < j \leqslant r, \end{array}$$

on $\{g_1, \ldots, g_r, h_1, \ldots, h_s\}$ define a group of order 2^n. The number of ways of choosing the $b(i, j)$s and the $c(i, j, k)$s is $2^{\binom{r}{2}s+rs}$ which, if we take $r = \lfloor 2n/3 \rfloor$, is $2^{2n^3/27+O(n^2)}$. Moreover, Higman showed that the number of choices of the $b(i, j)$s and the $c(i, j, k)$s which determine isomorphic groups is $2^{O(n^2)}$.

We now add the extra requirement that $g_r^2 = g_{r-1}^2 = h_1$. This completely determines $b(r, j)$ and $b(r - 1, j)$ for every $j \in \{1, \ldots, s\}$. The number of ways of choosing the parameters is now $2^{\binom{r}{2}s+(r-2)s}$ which is again $2^{2n^3/27+O(n^2)}$ for $r = \lfloor 2n/3 \rfloor$ and, by Higman's result, we still get $2^{2n^3/27+O(n^2)}$ pairwise non-isomorphic groups.

Let $G = \langle g_1, \ldots, g_r, h_1, \ldots, h_s \rangle$ be such a group. Let $S = \{g_1, \ldots, g_{r-2}, h_1, \ldots, h_s\}$, let $\tau = h_1$ and let $T = \{g_{r-1}, g_r\}$. We show that (S, T, τ) is a non-CCA triple and thus G is not CCA by Proposition 2.2. Clearly, $G = \langle S \cup T \rangle$. Moreover, τ is central in G and $g_{r-1}^2 = g_r^2 = \tau$. Finally, let $X = \langle S \cup \{\tau\} \rangle$ and let $H = \langle h_1, \ldots, h_s \rangle$. Note that $H \leqslant X$

and that G/H is an elementary abelian 2-group of order 2^r with $\{Hg_1, \ldots, Hg_r\}$ forming a basis. This implies that $|G : X| = 4$ and thus (S, T, τ) is a non-CCA triple. □

Remark 3.2. Note that, by [20], the number of groups of order 2^n is $2^{\frac{2}{27}n^3+O(n^{8/3})}$. Still, Theorem 3.1 falls short of proving that almost all 2-groups are non-CCA, although this seems likely to be the case.

4. Simple groups with no element of order four

In this section, we show that simple groups with no element of order four are CCA. It is easy to see that cyclic groups of prime order are CCA. (See [15, Proposition 4.1] or [18]. This can also be seen as a consequence of Burnside's Theorem [8, Theorem 3.5A].) We therefore restrict our attention to non-abelian simple groups with no element of order four. Such groups were classified by Walter.

Theorem 4.1 ([22])**.** *A non-abelian simple group has no element of order four if and only if it is isomorphic to one of the following:*

- $\mathrm{PSL}(2, 2^e)$, $e \geqslant 2$,
- $\mathrm{PSL}(2, q)$, $q \equiv \pm 3 \pmod 8$, $q \geqslant 5$,
- *a Ree group* ${}^2\mathrm{G}_2(3^{2n+1})$, $n \geqslant 1$,
- *the Janko group* J_1.

We will need the following result concerning the dimensions of irreducible $\mathbb{F}_2$-modules for $\mathrm{PSL}(2, 2^e)$.

Lemma 4.2. *Let $G = \mathrm{PSL}(2, 2^e)$ and let W be a non-trivial irreducible $\mathbb{F}_2G$-module. Then $\dim_{\mathbb{F}_2}(W) \geqslant 2e$.*

Proof. Let $K = \mathbb{F}_2$ and set $L = \mathbb{F}_{2^f}$ where f is minimal such that $W^L := L \otimes_K W$ is a sum of absolutely irreducible LG-modules. Note that f divides e since $\mathbb{F}_{2^e}$ is a splitting field for G. Using [1, (26.2)] and the notation from loc. cit. we have

$$W^L = \bigoplus_{i=1}^{a} V_i$$

where each V_i is a Galois twist of $V := V_1$ and $a = |\Gamma : \mathrm{N}_\Gamma(V)|$ with $\Gamma = \mathrm{Gal}(L, K)$. Since V cannot be written over a subfield of L, [1, (26.5)] implies that $\mathrm{N}_\Gamma(V) = 1$ and so $a = f$.

We now use the Brauer-Nesbitt Theorem as formulated in [4, Section 5.3] and borrow the notation established there. Since V is irreducible, [4, Theorem 5.3.2] states that $V = M(n)$ for some integer n with $0 \leqslant n \leqslant 2^e - 1$. Further, since V is written over L, there are $0 \leqslant a_0, \ldots, a_{e-1} \leqslant 1$ such that $n = \sum_{i=0}^{e-1} a_i 2^i$ and we have $V = M(a_0) \otimes M(a_1)^\phi \otimes \cdots \otimes M(a_{e-1})^{\phi^{e-1}}$ and $\dim_L(V) = (a_0 + 1)(a_1 + 1) \cdots (a_{e-1} + 1)$. Since V is non-trivial we have $n \geqslant 1$, so there is some i such that $a_i = 1$. Now since V is written over L, [4, Corollary 5.3.3] gives that $a_i = a_j$ if $i \equiv j \mod f$. Hence $\dim_L(V) \geqslant 2^{\frac{e}{f}}$ and we obtain

$$\dim_K(W) = \dim_L(W^L) = \dim_L(V) f \geqslant 2^{\frac{e}{f}} f \geqslant 2\frac{e}{f} f = 2e. \qquad \square$$

For a group A, the largest normal 2-subgroup of A is denoted $\mathrm{O}_2(A)$.

Proposition 4.3. *Let A be a group containing a non-abelian simple subgroup G. If $|A : G|$ is a power of 2, then either*

(1) $A/\mathrm{O}_2(A)$ is almost simple with socle isomorphic to G, or
(2) $G \cong \mathrm{Alt}(2^n - 1)$ and $A/\mathrm{O}_2(A)$ is isomorphic to $\mathrm{Alt}(2^n)$ or $\mathrm{Sym}(2^n)$, where $n \geqslant 3$.

Proof. Note that $A/\mathrm{O}_2(A)$ also satisfies the hypothesis hence we may assume that $\mathrm{O}_2(A) = 1$. Let N be a minimal normal subgroup of A and let p be an odd prime that divides $|N|$. Since $|A : G|$ is a power of 2, $G \cap N \neq 1$ and, since G is simple, $G \leqslant N$. Since distinct minimal normal subgroups intersect trivially, this shows that N is the unique minimal normal subgroup of A. It also follows that N is non-abelian hence $N = T_1 \times \cdots \times T_k$ where $T_i \cong T$ for some non-abelian simple group T. Since T_1 is a minimal normal subgroup of N, and has order divisible by p, the same argument as above gives $G \leqslant T_1$. Since $|A : G|$ is a power of 2, it follows that $|N : T_1| = |T|^{k-1}$ is a power of 2 hence $k = 1$, N is simple and A is almost simple. If $N = G$, then (1) holds. Otherwise, $G < N$ and [13, Theorem 1] implies that $N \cong \mathrm{Alt}(2^n)$ and $G \cong \mathrm{Alt}(2^n - 1)$ with $n \geqslant 3$. □

Theorem 4.4. *Non-abelian simple groups with no element of order four are CCA.*

Proof. Let G be a non-abelian simple group without elements of order four, let Γ be a connected Cayley graph on G and let A be the colour-preserving group of automorphisms of Γ. Let $N = \mathrm{O}_2(A)$ and let K be the kernel of the action of A on the set of N-orbits. Since G has no element of order four, Lemma 2.7 implies that for all $v \in \Gamma$ we have $K_v = 1$ and hence $K = N$. By Lemma 2.6, $|A : G|$ is a power of 2. Since G has no element of order four, Proposition 4.3 implies that NG is normal in A. We claim that G centralises N.

Suppose otherwise, and note therefore that G acts faithfully on N, and therefore on $N/\Phi(N)$ (where $\Phi(N)$ denotes the Frattini subgroup of N), and we may identify G with a subgroup of $\mathrm{Aut}(N/\Phi(N)) \cong \mathrm{GL}(d, 2)$ for some $d \in \mathbb{N}$. Let P be a Sylow 2-subgroup of G. Since $K_v = 1$ for all $v \in \Gamma$, $|N|$ is the size of an N-orbit hence $|N|$ divides $|\Gamma| = |G|$ and thus $|N|$ divides $|P|$. Note that P must be elementary abelian since G has no element of order four, and G must appear in Theorem 4.1. Suppose that G is not isomorphic to $\mathrm{PSL}(2, 2^n)$. Then $|N| \leqslant |P| \leqslant 8$ and so $d \leqslant 3$. However G is not a subgroup of $\mathrm{GL}(3, 2)$, a contradiction. We may thus assume that $G \cong \mathrm{PSL}(2, 2^n)$ and $|N| \leqslant |P| = 2^n$ so $d \leqslant n$. By Lemma 4.2, the smallest faithful representation for $\mathrm{PSL}(2, 2^n)$ over $\mathbb{F}_2$ is of dimension $2n$, so $d \geqslant 2n$, a contradiction.

We have shown that G centralises N, hence $NG = N \times G$ and G is characteristic in NG which is normal in A. It follows that G is normal in A and hence Γ is CCA. This concludes the proof. □

5. Simple groups with elements of order four

In this section we complete the proof of Theorem 1.2 by showing that simple groups with elements of order four are non-CCA. We use the Classification of Finite Simple Groups and simply consider each family of groups in turn (ignoring those that appear in Theorem 4.1).

5.1. **Alternating groups.** The idea of the proof for the alternating groups is used for each simple group considered in the rest of this section. Let $G = \mathrm{Alt}(n)$. Since $\mathrm{Alt}(5)$ does not have an element of order four, we may assume that $n \geqslant 6$. Let $t = (1\ 2)(3\ 4\ 5\ 6)$, $\tau = t^2$ and $H = G_1 \cong \mathrm{Alt}(n-1)$. We claim that $(S_H(\tau), t, \tau)$ is a non-CCA triple of G. Since H is maximal in G and $t \notin H$, we have $G = \langle S_H(\tau), t\rangle$, so (Ai) holds. By Lemma 2.4, (Aii) holds. By definition of τ, (Aiii) holds (where we take $T = \{t\}$). By definition, $S_H(\tau) \subseteq H$ and $\tau \in S_H(\tau)$, so $\langle S_H(\tau)\rangle \leqslant H$ and (Aiv) holds (in fact, Remark 2.3 shows that $\langle S_H(\tau)\rangle = H$). Finally, (Av) is clear as G has trivial centre. Hence, Proposition 2.2 shows that G is non-CCA.

Remark 5.1. One can also prove that $\mathrm{Sym}(n)$ is non-CCA for $n \geqslant 5$. In fact, the same proof as above works for $n \geqslant 6$. For $n = 5$ we take $t = (1\ 4\ 2\ 5)$, and $\tau = t^2$ and $H = \mathrm{Sym}(5)_{\{4,5\}} \cong \mathrm{Sym}(3)$. Then $(S_H(\tau), t, \tau)$ is a non-CCA triple of G.

By Theorem 4.4, $\mathrm{Alt}(5)$ is CCA. Moreover, $\mathrm{Alt}(n)$ is CCA for $n \leqslant 4$, whereas $\mathrm{Sym}(4)$ is not CCA, but $\mathrm{Sym}(3)$ and $\mathrm{Sym}(2)$ are CCA (see for example [15]). One can also check that almost simple groups with socle $\mathrm{Alt}(6)$ are not CCA (using Magma [3], for example).

These results include every almost simple group whose socle is alternating. In each case, a group is CCA if and only if it does not contain an element of order four.

5.2. **Chevalley groups.** We now turn to the Chevalley groups (also called untwisted groups of Lie type). Most of the families can be dealt with in a uniform manner, but to do this we require some setup. Our approach is to use the Chevalley presentation. We refer (and recommend) the reader to [5] or [12] for a more detailed exposition. In particular, all details in the following paragraphs are found in [12, Section 2.4]. First, we recall the notation. Let $G = X_n(q)$ be a *Chevalley group* where $q = p^f$ for a prime p, $X \in \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}, \mathrm{G}\}$ and n is a positive integer, with $n \geqslant 1$ if $X = \mathrm{A}$, $n \geqslant 2$ if $X = \mathrm{B}$, $n \geqslant 3$ if $X = \mathrm{C}$, $n \geqslant 4$ if $X = \mathrm{D}$, $n \in \{6, 7, 8\}$ if $X = \mathrm{E}$, $n = 4$ if $X = \mathrm{F}$ and $n = 2$ if $X = \mathrm{G}$. Associated to G is a root system Φ (a set of vectors in a vector space associated to G) with fundamental system Π so that $\Phi = \Phi^+ \cup \Phi^-$ with respect to Π (that is, each vector in Φ can be written as either a positive or a negative linear combination of elements of Π). For explicit models of the root systems see [12, Remark 1.8.8]. For each $\alpha \in \Phi$ we have homomorphisms $x_\alpha : (\mathbb{F}_q, +) \to G$ and $h_\alpha : (\mathbb{F}_q - \{0\}, \times) \to G$. The *root subgroups* of G are $X_\alpha = \langle x_\alpha(\eta) \mid \eta \in \mathbb{F}_q\rangle$. Finally, there are elements $n_\alpha \in G$ for each $\alpha \in \Phi^+$.

With this notation in hand, we set

$$\begin{aligned} U &= \langle x_\alpha(\eta) \mid \alpha \in \Phi^+, \eta \in \mathbb{F}_q\rangle, \\ H &= \langle h_\alpha(\lambda) \mid \alpha \in \Phi^+, \lambda \in \mathbb{F}_q - \{0\}\rangle = \langle h_\alpha(\lambda) \mid \alpha \in \Pi, \lambda \in \mathbb{F}_q - \{0\}\rangle \\ N &= \langle H, n_\alpha \mid \alpha \in \Phi^+\rangle. \end{aligned}$$

Then U is a Sylow p-subgroup of G, H normalises U and $B = UH$ is the normaliser in G of U. Further, $H = B \cap N$ is abelian and H is normal in N. The Weyl group of G is $W := N/H$, with generators $s_\alpha := Hn_\alpha$ such that $\alpha \in \Pi$. The Weyl group of G acts faithfully on the root system Φ, and we write $s_\alpha(\beta)$ for the image of $\beta \in \Phi$ under the Weyl group element s_α. The Chevalley Relations [12, Theorem 2.4.8] give a presentation for the group $X_n(q)$ in terms of the elements of U, H and N as follows. For $\alpha, \beta \in \Phi$ with

$\beta \neq \pm\alpha$, if $\alpha+\beta \notin \Phi$, then $[X_\alpha, X_\beta] = 1$ and if $\alpha+\beta \in \Phi$, then the Chevalley Commutator Formula [12, Theorem 2.4.5] allows us to calculate $[X_\alpha, X_\beta]$. The action of N on the root subgroups is given by

$$x_\beta(\eta)^{n_\alpha} = x_{s_\alpha(\beta)}(\pm\eta) \quad \text{and} \quad x_\beta(\eta)^{h_\alpha(\lambda)} = x_\beta(\eta\lambda^{A_{\beta\alpha}})$$

where the constants $A_{\beta\alpha}$ are found in the Cartan matrix of Φ, which we again do not dwell upon. Finally, the action of N on H is given by $h_\beta(\lambda)^{n_\alpha} = h_{s_\alpha(\beta)}(\lambda)$ and we mention that $(n_\alpha)^2 = h_\alpha(-1)$ for all $\alpha \in \Phi^+$.

5.2.1. $\boldsymbol{X_n \notin \{A_1, G_2\}}$. We are now ready to deal with most Chevalley groups, except for two families of low rank.

Since the rank of G ($= |\Pi|$) is at least two and since G is not of type G_2, we may pick simple roots $\alpha, \beta \in \Pi$ such that with $\gamma := s_\alpha(\beta)$ we have $\beta + \gamma \notin \Phi$. More precisely, if G is not of type B_2, the simple roots corresponding to nodes 1 and 2 of the Dynkin diagram of G (as labelled in [12, pg.12]) have this property. If G is of type B_2 we set α to be the short root, so that $s_\alpha(\beta) = 2\alpha + \beta$. Set $J = \Pi - \{\alpha\}$ and let $P_J = \langle B, n_\gamma \mid \gamma \in J\rangle$ be the maximal parabolic subgroup corresponding to J (P_J is a maximal subgroup of G by [1, (43.7)]).

Suppose first that q is even. In this case, we have that $\{n_\gamma \mid \gamma \in \Pi\}$ is a set of involutions in G and we let $t = x_\beta(1)n_\alpha$. Then

$$\tau := t^2 = x_\beta(1)x_\beta(1)^{n_\alpha} = x_\beta(1)x_{s_\alpha(\beta)}(1) = x_\beta(1)x_\gamma(1).$$

Since $\beta + \gamma \notin \Phi$, $x_\beta(1)$ and $x_\gamma(1)$ commute, and since q is even, we have $\tau^2 = 1$. Note that $\tau \in P_J$ since $\tau \in U$, but $t \notin P_J$ since $n_\alpha \notin P_J$. Let $S := \langle S_{P_J}(\tau)\rangle$. We claim that P_J is the unique maximal subgroup of G containing S. Indeed, suppose that M is a maximal subgroup of G containing S. First note that since q is even the elements $x_\delta(\eta)$ for $\eta \in \mathbb{F}_q$ and $\delta \in \Phi$ are involutions, thus since S contains each involution in P_J, S contains U. Hence by [12, Theorem 2.6.7], M must be a parabolic subgroup containing B. Since S contains all of the involutions n_δ for $\delta \in J$, we have $Bn_\delta \subset M$. Hence $P_J = \langle B, n_\gamma \mid \gamma \in J\rangle \leqslant M$ which forces $P_J = M$ since P_J is maximal. This proves the claim. Now it is easy to verify that $(S_{P_J}(\tau), t, \tau)$ is a non-CCA triple of G.

Suppose now that q is odd. Set $t = n_\alpha$, so that (by [12, Remark 2.4.0(c)] and [12, Theorem 1.12.1k]) we have $\tau := t^2 = h_\alpha(-1) \neq 1$ (note that when G is of type B_2, this is due to our choice of α). Let $S = \langle S_{P_J}(\tau)\rangle$. Let $\gamma \in \Pi$ be arbitrary and let $\eta \in \mathbb{F}_q$. We have

$$(x_\gamma(\eta))^\tau = x_\gamma((-1)^{A_{\gamma\alpha}}\eta) = x_\gamma(\pm\eta) = (x_\gamma(\eta))^{\pm 1}.$$

In particular, τ inverts or centralises each generator of U and so $U \leqslant S$. If n_β is an involution in G (when G is of type B_2 for example) then $n_\beta \in S$. If n_β has order four, then

$(n_\beta)^2 = h_\beta(-1)$ and (recalling that H is abelian)

$$\begin{aligned}(\tau n_\beta)^2 &= h_\alpha(-1)n_\beta^2 h_\alpha(-1)^{n_\beta}\\ &= h_\alpha(-1)h_\beta(-1)h_{s_\beta(\alpha)}(-1)\\ &= h_\alpha(-1)h_\beta(-1)h_{\alpha+\beta}(-1)\\ &= (h_\alpha(-1)h_\beta(-1))^2\\ &= 1\end{aligned}$$

where the second to last equality holds by [12, Theorem 2.4.7]. Hence τn_β is an involution in P_J, and so $n_\beta \in S$ since $\tau \in S$. Next, if $\gamma \in \Pi$ with $\alpha \neq \gamma \neq \beta$, then n_γ commutes with $h_\alpha(-1) = \tau$, so that $n_\gamma \in S$. Hence, arguing as above, if M is a maximal subgroup of G containing S, then $M = P_J$. In particular, $(S_{P_J}(\tau), t, \tau)$ is a non-CCA triple of G, so Proposition 2.2 completes the proof in this case.

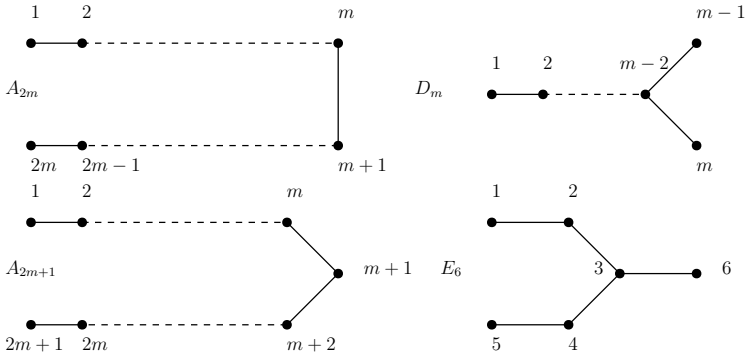
We now turn to the excluded families.

5.2.2. $\boldsymbol{X_n = A_1}$. We now assume that $G = \mathrm{A}_1(q) \cong \mathrm{PSL}(2,q)$. In view of Theorem 4.1, we can assume that $q \equiv 1, 7 \pmod 8$ and, taking into account exceptional isomorphisms, that $q \notin \{7, 9\}$. In this case, G has one conjugacy classes of involutions, so each involution in G is a square. Further, G has maximal subgroups M_1 and M_2 isomorphic to D_{q+1} and D_{q-1}. Depending on q, we may pick $i \in \{1, 2\}$ and an involution τ in M_i such that τ is a non-square in M_i and $M_i = \langle S_{M_i}(\tau)\rangle$. Since τ is a square in G, but not in M_i, there is $t \in G$ such that $t^2 = \tau$ and $t \notin M_i$. Hence $(S_{M_i}(\tau), t, \tau)$ is a non-CCA triple of G, and Proposition 2.2 completes the proof in this case.

5.2.3. $\boldsymbol{X_n = G_2}$. Finally, we assume that $G = \mathrm{G}_2(q)$. We may assume that $q \geqslant 3$. If q is odd, then G has a unique conjugacy class of involutions [6, Theorem (4.4)], so each involution in G is a square. If q is even, then G has two conjugacy classes of involutions [10, Proposition 2.6] and one of the classes consists of squares – using notation of loc. cit. the involution x_3 is the square of x_5, for example. We consult [23, Table 4.1] for the maximal subgroups of G. If q is odd, let M be a maximal subgroup with $M \cong \mathrm{SL}(3,q) : 2$ and let τ be an involution in M that does not lie in the $\mathrm{SL}(3,q)$ subgroup. If q is even, let M be a maximal subgroup with $M \cong \mathrm{PSL}(2,q) \times \mathrm{PSL}(2,q)$ and let τ be an involution in M which is a conjugate of x_3 (the first paragraph of [23, Section 4.3.6] shows that M contains such an involution). If q is even, the structure of M shows that τ is not a square in M and, if q is even, then the Sylow 2-subgroups of M are elementary abelian, so τ is not a square in M. Thus, in either case, there is $t \in G$ such that $t^2 = \tau$. Now $t \notin M$ so $\langle M, t\rangle = G$. In both cases, we have $\langle S_M(\tau)\rangle = M$. Thus $(S_M(\tau), t, \tau)$ is a non-CCA triple of G, so Proposition 2.2 completes the proof in this case.

5.3. **Twisted groups of Lie type.** Next, we deal with the so-called twisted (or "Steinberg") groups. These groups arise as fixed points of the so-called *graph-field automorphisms* of the Chevalley groups, which exist whenever the associated Dynkin diagrams admit a graph automorphism (of order d if the group is ${}^dX_n(q)$).

We start with the case $d = 2$ that is, groups of the form ${}^2\mathrm{A}_n(q) \cong \mathrm{PSU}(n+1,q)$, ${}^2\mathrm{D}_n(q) \cong \mathrm{P}\Omega^-(2n,q)$ $(n \geqslant 4)$ and ${}^2\mathrm{E}_6(q)$. Below we have shown the Dynkin diagrams in such a way that the orbits of the graph automorphism are clear.



A twisted group ${}^2X_n(q)$ admits a *twisted* root system. These root systems are in fact equivalence classes of the images of roots from the corresponding untwisted group $X_n(q)$, see [12, Definition 2.3.1]. The graph automorphism of the Dynkin diagram extends to an isometry ρ of the vector space associated to the untwisted group $X_n(q)$, and thus acts on the root system Φ. The average of the roots in the orbit of $\alpha \in \Phi$ is denoted $\tilde{\alpha}$, and the set of these averages is denoted $\tilde{\Phi}$. We say two vectors of $\tilde{\Phi}$ are equivalent if one is a positive multiple of the other. The equivalence class of $\tilde{\alpha}$ is denoted by $\hat{\alpha}$. Thus there are maps $\Phi \to \tilde{\Phi} \to \hat{\Phi}$, and the set $\tilde{\Phi}$ is the twisted root system of the twisted group ${}^2X_n(q)$ (it may not be an actual root system). In the cases under consideration, $\tilde{\Sigma} = \hat{\Sigma}$, except for ${}^2A_{2m}(q)$. The twisted group is generated by the root subgroups $\langle x_{\hat{\alpha}}(\eta) \mid \eta \in \mathbb{F}_q \rangle$ for $\hat{\alpha} \in \hat{\Phi}$. The definition of $x_{\hat{\alpha}}$ depends upon the orbit of α under ρ, and is found in [12, Table 2.4]. Three possibilities arise for us, the orbit is a single vertex, two disconnected vertices or two vertices joined by an edge. The definition of $x_{\hat{\alpha}}$ is then found in Row I, II or IV respectively of [12, Table 2.4]. (For example, in the case of ${}^2\mathrm{D}_4(q)$, we have α_3 and α_4 are in the same orbit, and $x_{\hat{\alpha_3}}(\eta) = x_{\alpha_3}(\eta)x_{\alpha_4}(\eta^q)$, see Row II of [12, Table 2.4].) There is an analogous definition of $h_{\hat{\alpha}}$ for $\hat{\alpha} \in \hat{\Phi}$, found in [12, Table 2.4.7]. For the precise definition of $n_{\hat{\alpha}}$ we actually consult the proof of [12, Theorem 2.4.8] (see also [12, Remark 2.4.9(b)]) and conclude that either α is fixed by the isometry ρ and we can take $n_{\hat{\alpha}} = n_\alpha$ or the orbit of α has length two. In even characteristic, $n_{\hat{\alpha}}$ always has order two and in odd characteristic $n_{\hat{\alpha}}$ has order four if $\hat{\alpha}$ is of type II, and has order two if $\hat{\alpha}$ is of type IV. More specifically, when $\hat{\alpha}$ is of type II, we have $n_{\hat{\alpha}} = h n_\alpha n_{\alpha^\rho}$ for some $h \in T_1$ (see loc. cit.), where $h = 1$ in even characteristic. If $\hat{\alpha}$ is of type IV, we have $n_{\hat{\alpha}} = h n_\alpha n_{\alpha^\rho} n_\alpha = h n_{\alpha^\rho} n_\alpha n_{\alpha^\rho}$ for some $h \in T_1$ (see loc. cit.), where again $h = 1$ if the characteristic is even. We calculate that, if $n_{\hat{\alpha}}$ has order four, then (in all cases) $n_{\hat{\alpha}}^2 = h_{\hat{\alpha}}(-1)$.

5.3.1. ***${}^2\mathbf{D}_n(q)$ for $n \geqslant 4$ and ${}^2\mathbf{E}_6(q)$.*** Let $G = {}^2X_n(q)$, where $X \in \{D, E\}$. The idea of the proof is analogous to the untwisted case, but the setup requires a little more care because of the twist. First, we select two simple roots $\alpha, \beta \in \Pi$ that are fixed by the isometry ρ. In detail: if $X = D$ pick $\alpha = \alpha_1$, $\beta = \alpha_2$ and if $X = E$ pick $\alpha = \alpha_4$ and

$\beta = \alpha_3$. The proof can now proceed exactly as for the untwisted groups. We provide some details to show how the various steps may be adjusted. Let $\delta \in \{\alpha, \beta\}$. Since δ is fixed by the isometry ρ, any calculations involving $n_{\hat{\delta}} = n_\delta$ and $h_{\hat{\delta}}(\eta) = h_\delta(\eta)$ are the same as for the untwisted groups. Further, the calculations regarding $s_\alpha(\beta)$ and β are the same as for the untwisted group. Finally, since all of the root subgroups are either of type I or II, the assertions concerning the structure of the Sylow p-subgroups (that it is generated by involutions when q is even and that the generators are either inverted or centralised when q is odd) are the same as for the untwisted groups.

5.3.2. ***${}^2\mathbf{A}_n(q)$ for $n \geqslant 3$***. Let $n \geqslant 3$ and let $G = {}^2\mathrm{A}_n(q) \cong \mathrm{PSU}(n+1, q)$. For the unitary groups in odd dimension, the root subgroups can be of type IV and so, in even characteristic, are not necessarily generated by involutions. For this reason, we use a different approach. We first claim that there is a maximal parabolic subgroup P stabilising a totally isotropic 1-space or 2-space and an element $t \in G - P$ of order four such that $\tau := t^2 \in P$.

Suppose first that q is odd. Since $n \geqslant 3$, the claim holds with $t = n_{\hat{\alpha}_1}$, $\tau = t^2 = h_{\hat{\alpha}_1}(-1)$ and P the stabiliser of a totally isotropic 1-space corresponding to the first node of the Dynkin diagram for $A_n(q)$.

Suppose now that q is even and assume first that $n \geqslant 4$. Set $w = n_{\hat{\alpha}_2}$, $x = x_{\hat{\alpha}_1}(1)$ and put $t = xw$. Since q is even, $n_{\hat{\alpha}_2}$ is an involution and, since $n \geqslant 3$, the twisted root $\hat{\alpha}_1$ is of type II, so that both x and w are involutions. We set $\tau := t^2 = xx^w$. To calculate τ, there are three cases depending on the type of $\hat{\alpha_2}$. Since we assume $n \geqslant 4$, $\hat{\alpha_2}$ is of type II or IV.

If $\hat{\alpha_2}$ is of type II then necessarily $n \geqslant 5$ and $w = n_{\alpha_2} n_{\alpha_{n-1}}$. Then

$$\begin{aligned} xx^w &= x_{\alpha_1}(1) x_{\alpha_n}(1) (x_{\alpha_1}(1))^{n_{\alpha_2}} (x_{\alpha_n}(1))^{n_{\alpha_{n-1}}} \\ &= x_{\alpha_1+\alpha_2}(1) x_{\alpha_2}(1) x_{\alpha_n}(1) x_{\alpha_n+\alpha_{n-1}}(1). \end{aligned}$$

Note that since $n \geqslant 5$, each of the elements in the expression for xx^w above commute, and so $\tau^2 = 1$ since q is even. Hence the claim holds with P the stabiliser of a totally isotropic 2-space.

Suppose that $\hat{\alpha_2}$ is of type IV, so that $n = 4$, $x = x_1(1)x_4(1)$ and $n_{\hat{\alpha_2}} = n_{\alpha_2} n_{\alpha_3} n_{\alpha_2} = n_{\alpha_3} n_{\alpha_2} n_{\alpha_3}$. Then

$$\begin{aligned} xx^w &= x_{\alpha_1}(1) x_{\alpha_4}(1) (x_{\alpha_1}(1))^{n_{\alpha_2} n_{\alpha_3}} (x_{\alpha_4}(1))^{n_{\alpha_2} n_{\alpha_3}} \\ &= x_{\alpha_1}(1) x_{\alpha_4}(1) x_{\alpha_1+\alpha_2+\alpha_3}(1) x_{\alpha_2+\alpha_3+\alpha_4}(1). \end{aligned}$$

Using the Chevalley Commutator Formula, we calculate that $\tau^2 = 1$. (Note that there are exactly two pairs of non-commuting elements in the expression for τ, so when calculating the square, we introduce twice the element $x_{\alpha_1+\alpha_2+\alpha_3+\alpha_4}(1)$ which is the commutator of both $x_{\alpha_1}(1)$ and $x_{\alpha_2+\alpha_3+\alpha_4}(1)$ and of $x_{\alpha_4}(1)$ and $x_{\alpha_1+\alpha_2+\alpha_3}(1)$.) Hence the claim holds with P the stabiliser of a totally isotropic 2-space in the 5-dimensional vector space on which $\mathrm{SU}(5, q)$ acts.

Now assume that $n = 3$ and set $w = n_{\hat{\alpha_1}}$, $x = x_{\hat{\alpha_2}}(1) = x_{\alpha_2}(1)$ and $t = xw$. Since q is even, w is an involution, so $\tau := t^2 = xx^w$. Since $w = n_{\alpha_1} n_{\alpha_3}$, we calculate that

$\tau = x_{\alpha_2}(1)x_{\alpha_1+\alpha_2+\alpha_3}(1)$. Hence $\tau^2 = 1$ and the claim holds with P the stabiliser of a totally isotropic 1-space in the 4-dimensional vector space on which $\mathrm{SU}(4,q)$ acts.

Set $S = \langle S_P(\tau)\rangle$ and let X be the normal subgroup of P generated by the involutions in P, so that $X \leqslant S$. We claim that P is the unique maximal subgroup of G containing P. The proof of this claim depends on the structure of P, for which we refer to [23, Theorem 3.9(ii)] (noting that $n-k$ should read $n-2k$). Let $P = QL$ be the Levi decomposition of P.

Let M be a normal quasisimple subgroup of L, so that $M/Z(M)$ is non-abelian simple. We claim that $M \leqslant S$. Since M is quasisimple, either $X \cap M \leqslant Z(M)$ or $X \cap M = M \leqslant S$. If the former holds, then $[X,M,M] = 1 = [M,X,M]$ and so the Three Subgroups Lemma gives $1 = [M,M,X] = [M,X]$, where the last equality holds since M is perfect. Since $\tau \in X$, this yields $M \leqslant C_P(\tau)$ and so $M \leqslant S$. Let E be the product of the normal quasisimple subgroups of L, so that $E \leqslant S$.

Assume that $(n,q) \notin \{(3,2),(3,3),(5,2),(6,2)\}$. Then QE contains a Sylow p-subgroup of G. Note that $Q = [Q,E] \leqslant [Q,X] \leqslant X$. Hence $QE \leqslant S$ and so S contains a Sylow p-subgroup of G. By [12, Theorem 2.6.7] the only maximal subgroup containing S must therefore be a parabolic subgroup, that is, a stabiliser of some totally isotropic subspace. Since QE fixes a unique totally isotropic subspace, the only maximal subgroup of G containing S is P, as claimed.

For $(n,q) \in \{(3,2),(3,3),(5,2),(6,2)\}$, one can verify the claim directly (say, with Magma [3]).

From the claim, it follows $(S_P(\tau), t, \tau)$ is a non-CCA triple of G, and so G is non-CCA by Proposition 2.2.

5.3.3. $\mathbf{^2A_2(q)}$. Let $G = {}^2\mathrm{A}_2(q) \cong \mathrm{PSU}(3,q)$ for q a prime power. Let $M \leqslant \mathrm{SU}(3,q)$ be the stabiliser of a non-degenerate direct sum decomposition of the natural vector space that $\mathrm{SU}(3,q)$ acts on. Then $M \cong (\mathrm{C}_{q+1})^2 \rtimes \mathrm{Sym}(3)$ and M is maximal in $\mathrm{SU}(3,q)$ by [4]. Since $\mathrm{Z}(\mathrm{SU}(3,q)) \cong \mathrm{C}_{(3,q+1)}$ is contained in M, we have $H := M/Z(\mathrm{SU}(3,q))$ is maximal in G. Pick τ to be an involution in a subgroup of H conjugate to $\mathrm{Sym}(3)$. Then τ is a non-square in H. Since G has elements of order four, and one conjugacy class of involutions (see [12, Table 4.5.1] for q odd and [2, (6.1)] for q even) there is $t \in G - H$ such that $t^2 = \tau$.

Let $X := \langle S_H(\tau)\rangle$. We claim that $H = X$. Note that X is a normal subgroup of H containing our chosen $\mathrm{Sym}(3)$ subgroup. Write $q+1 = p_1^{a_1}\dots p_r^{a_r}$. Then, for $p_i \neq 3$, we have $T_i = \mathrm{O}_{p_i}(H)$ and $\mathrm{Sym}(3)$ acts irreducibly on $T_i \cong (C_{p_i^{a_i}})^2$. This forces $T_i \leqslant X$. For $p_i = 3$, $T_i \cong \mathrm{C}_{3^{a_i}} \circ_3 \mathrm{C}_{3^{a_i}}$ (where the symbol $\circ_3$ means that a subgroup of order three has been identified). It follows that there are generators x and y for T_i such that $x^\tau = x$ and $y^\tau = y^{-1}$. Thus $y = z\tau$ for some involution z and so $T_i \leqslant X$.

The previous two paragraphs show that $(S_M(\tau), t, \tau)$ is a non-CCA triple of G hence, by Proposition 2.2, G is non-CCA.

5.3.4. $\mathbf{^3D_4(q)}$. Let $G = {}^3\mathrm{D}_4(q)$ for q a prime power. When q is odd, G has a unique conjugacy class of involutions by [16, Lemma 2.3(i)], so each involution is a square in G. When q is even, G has two conjugacy classes of involutions [21, (8.1)]. Representatives are

$x_6(1)$ and $x_4(1)$ (using the notation of [21]). Using [21, (2.1)], we calculate that $x_6(1) = (x_2(1)x_5(1))^2$. For $\alpha \in \mathbb{F}_{q^3} - \mathbb{F}_q$, we find that the square of $x_1(\alpha)x_3(1)$ is conjugate to $x_4(1)$ by [21, (3.1)]. Hence, for all q, every involution in G is a square. Now, by [23, Theorem 4.3], there is a maximal subgroup M of the form $2 \cdot (\mathrm{PSL}(2, q^3) \times \mathrm{PSL}(2, q)) : 2$ for q odd and, for q even, there is a maximal subgroup M of the form $\mathrm{PSL}_2(q^3) \times \mathrm{PSL}_2(q)$. For q odd, we let τ be an involution in M outside the derived subgroup and, for q even, we let τ be an involution in M. In both cases, we have that τ is a square in G, but not in M, so there is $t \in G$ such that $t^2 = \tau$. This case can now be finished by arguing as in the previous one.

5.4. **Suzuki-Ree groups.**

5.4.1. $\mathbf{{}^2F_4(q)}$. Let G be either a large Ree group ${}^2\mathrm{F}_4(q)$, where $q = 2^e \geqslant 4$ with e odd, or the Tits group ${}^2\mathrm{F}_4(2)'$. We note that G has two conjugacy classes of involutions by [2, (18.2)]. Consulting [19] and using notation of loc. cit., we find representatives $x_{12}(1)$ and $x_{10}(1)$. We find $x_{12}(1) = x_5(1)^2$ and $(x_4(1)x_2(1))^2 = x_7(1)x_8(1)x_{11}(1)x_{12}(1)$. The latter element is conjugate to $x_7(1)$ by [19, Section 2] and $x_7(1)$ is conjugate to $x_{10}(1)$ by [19, Lemma 10]. Thus all involutions in G are squares. By [23, Theorem 4.5] there is a maximal subgroup $M \cong \mathrm{Sp}(4, q) : 2$. Let τ be an involution in M that does not lie in the $\mathrm{Sp}(4, q)$ subgroup. Then $M = \langle S_M(\tau) \rangle$ since M is almost simple (even for $q = 2$). There is $t \in G$ such that $t^2 = \tau$ and $t \notin M$ since the structure of M shows that τ is not a square in M. Then $(S_M(\tau), t, \tau)$ is a non-CCA triple of G, and Proposition 2.2 completes the proof.

5.4.2. $\mathbf{{}^2B_2(q)}$. Let $q = 2^e \geqslant 8$ with e odd. We will prove something slightly stronger than required, namely that, if G is an almost simple group with socle ${}^2\mathrm{B}_2(q)$, then G is non-CCA. By [4, Theorem 7.3.5] and [4, Table 8.16], the normaliser in G of a maximal subgroup $M \cong \mathrm{D}_{q-1}$ of $\mathrm{soc}(G)$ is maximal in G. Now $\mathrm{N}_G(M) \cong C_{q-1} \rtimes (C_2 \times C_f)$ for some divisor f of e. Since q is even, we may pick involutions x and τ and an element $c \in G$ of order f that commutes with τ such that $\mathrm{N}_G(M) = \langle \tau x, \tau, c \rangle$. Since all involutions in G are squares (see the description of a Sylow 2-subgroup of G in [4, Table 8.16]), there is $t \in G$ such that $t^2 = \tau$. Now $(\{\tau x, \tau, c\}, \{t\}, \tau)$ is a non-CCA triple, so Proposition 2.2 completes the proof.

5.5. **Sporadic groups.** To finish the proof of Theorem 1.2, only the sporadic groups remain to be addressed. In view of Theorem 4.1, we can ignore the Janko group J_1. Let (G, H) be one of the pairs from the table below. That H is a maximal subgroup of G and other facts regarding properties of G used below can be found in [7] or [24].

G	H
M_{11}	$PSL(2,11)$
M_{22}	$PSL(2,11)$
M_{23}	M_{11}
M_{24}	$PSL(2,7)$
J_3	$PSL(2,19)$
McL	M_{11}
He	$7^{1+2} : (3 \times \mathrm{Sym}(3))$
Suz	$\mathrm{Alt}(7)$
Co_2	M_{23}

G	H
Co_1	Co_2
HN	$\mathrm{Alt}(12)$
ON	$\mathrm{Alt}(7)$
J_4	$PSU(3,3)$
Ly	$37:18$
Th	$PSL(3,3)$
Fi'_{24}	$29:14$
M	$PSL(2,59)$

G	H
M_{12}	M_{11}
J_2	$PSU(3,3)$
HS	M_{11}
Ru	$\mathrm{Alt}(8)$
Co_3	M_{23}
Fi_{22}	M_{12}
Fi_{23}	$PSL(2,23)$
B	M_{11}

For $X = H$ or $X = G$ and τ an involution of X we define

$$ {}_X\sqrt{\tau} = \{t \in X \mid t^2 = \tau\} $$

and we have that

$$ |{}_X\sqrt{\tau}| = \sum_{\chi \in \mathrm{Irr}(X)} s(\chi)\chi(\tau) $$

where $s(\chi)$ is the Frobenius-Schur indicator of χ. For both G and H, the character tables are either stored in GAP [11] or can be computed easily. We used GAP to compute the values of $|{}_X\sqrt{\tau}|$ for each conjugacy class of involutions in both G and H. For G in the left or middle table above we let τ be an involution of H. For G in the right table, let $\tau \in H$ be an involution with $|{}_H\sqrt{\tau}| \neq 0$. Our calculations then show that $|{}_G\sqrt{\tau}| \neq |{}_H\sqrt{\tau}|$ for the pair (G, H). Hence there is $t \in G - H$ such that $t^2 = \tau$. Since $\langle S_H(\tau) \rangle$ contains both $C_H(\tau)$ and the normal subgroup of H generated by the involutions of H, we have $\langle S_H(\tau) \rangle = H$. Then it is easy to check that $(S_H(\tau), \{t\}, \tau)$ is a non-CCA triple of G, and Proposition 2.2 completes the proof.

ACKNOWLEDGEMENTS. We would like to thank Michael Giudici for his helpful comments on an early version of this manuscript.

REFERENCES

[1] M. Aschbacher, *Finite group theory*, Second edition in *Cambridge Studies in Advanced Mathematics* **10** Cambridge University Press, Cambridge, 2000.

[2] M. Aschbacher and G. M. Seitz, Involutions in Chevalley Groups Over Fields of Even Order, *Nagoya Math. J.* **63** (1976), 1–91.

[3] W. Bosma, J. Cannon and C. Playoust, The `Magma` algebra system. I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[4] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Ser. **407**, Cambridge University Press, Cambridge, 2013.

[5] R. W. Carter, *Simple groups of Lie type*, Pure and Applied Mathematics, Vol. 28. John Wiley & Sons, London-New York-Sydney, 1972.

[6] B. Chang, The conjugate classes of Chevalley groups of type (G2), *J. Algebra* **9** (1968), 190–211.

[7] J. Conway, R. T. Curtis, S. Norton, R. Parker, and R. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[8] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.
[9] E. Dobson, A. Hujdurović, K. Kutnar and J. Morris, On color-preserving automorphisms of Cayley graphs of odd square-free order, *J. Algebraic. Combin.* **44** (2016), 407–422.
[10] H. Enomoto, The conjugacy classes of Chevalley groups of type (G2) over finite fields of characteristic 2 or 3, *J. Fac. Sci. Univ. Tokyo Sect. I* **16** 1969 497–512 (1970).
[11] The Gap Group, Gap–Groups, Algorithms, and Programming, 2015, http://www.gap-system.org.
[12] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple $\mathcal{K}$-groups*. Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.
[13] R. M. Guralnick, Subgroups of prime power index in a simple group, *J. Algebra* **81** (1983), 304–311.
[14] G. Higman, Enumerating p-groups. I: Inequalities, *Proc. London Math. Soc.* **10** (1960), 24–30.
[15] A. Hujdurović, K. Kutnar, D. W. Morris, J. Morris, On colour-preserving automorphisms of Cayley graphs, *Ars Math. Contemporanea* **11** (2016), 189–213.
[16] P. B. Kleidman, The maximal subgroups of the Steinberg Triality groups ${}^3D_4(q)$ and of their automorphism groups, *J. Algebra* **115** (1988), 182–199.
[17] L. Morgan, J. Morris and G. Verret, Characterising CCA Sylow cyclic groups whose order is not divisible by four, arXiv:1702.06651.
[18] J. Morris, Automorphisms of circulants that respect partitions, *Contributions to Discrete Mathematics,* **11** (2016), 1–6.
[19] D. Parrott, A Characterization of the Ree Groups ${}^2F_4(q)$, *J. Algebra* **27** (1973), 341–357.
[20] C. Sims, Enumerating p-groups, *Proc. London Math. Soc.* **15** (1965), 151–166.
[21] G. Thomas, A characterization of the Steinberg groups $D_4^2(q^3)$, $q = 2^n$, *J. Algebra* **14** (1970), 373–385.
[22] J. H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. of Math.* **89** (1969), 405–514.
[23] R. A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics volume 251, Springer-Verlag, London, 2009.
[24] R. A. Wilson, ATLAS of Finite Group Representations, http://brauer.maths.qmul.ac.uk/Atlas/v3/

Luke Morgan and Gabriel Verret*, Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics (M019), The University of Western Australia, Crawley, 6009, Australia
E-mail address: luke.morgan@uwa.edu.au

Joy Morris, Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada
E-mail address: joy.morris@uleth.ca

∗ Current address: Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland 1142, New Zealand.
E-mail address: g.verret@auckland.ac.nz