On automorphisms of the double cover of a circulant graph

Ademir Hujdurović
UP IAM and UP FAMNIT
University of Primorska
Koper, Slovenia
ademir.hujdurovic@upr.si

Đorđe Mitrović
UP FAMNIT
University of Primorska
Koper, Slovenia
mitrovic98djordje@gmail.com

Dave Witte Morris
Department of Mathematics and Computer Science
University of Lethbridge
Alberta, Canada
dave.morris@uleth.ca

Submitted: Aug 18, 2021; Accepted: Nov 25, 2021; Published: Dec 17, 2021

Abstract

A graph X is said to be *unstable* if the direct product $X \times K_2$ (also called the canonical double cover of X) has automorphisms that do not come from automorphisms of its factors X and K_2. It is *nontrivially unstable* if it is unstable, connected, and nonbipartite, and no two distinct vertices of X have exactly the same neighbors.

We find three new conditions that each imply a circulant graph is unstable. (These yield infinite families of nontrivially unstable circulant graphs that were not previously known.) We also find all of the nontrivially unstable circulant graphs of order $2p$, where p is any prime number.

Our results imply that there does not exist a nontrivially unstable circulant graph of order n if and only if either n is odd, or $n < 8$, or $n = 2p$, for some prime number p that is congruent to 3 modulo 4.

Mathematics Subject Classifications: 05C25, 05C76

1 Introduction

Let X be a circulant graph. (All graphs in this paper are finite, simple, and undirected.)

Definition 1.1 ([18])**.** The *canonical bipartite double cover* of X is the bipartite graph BX with $V(BX) = V(X) \times \{0, 1\}$, where

$$(v, 0) \text{ is adjacent to } (w, 1) \text{ in } BX \quad \Longleftrightarrow \quad v \text{ is adjacent to } w \text{ in } X.$$

 https://doi.org/10.37236/10655

Letting S_2 be the symmetric group on the 2-element set $\{0,1\}$, it is clear that the direct product $\operatorname{Aut} X \times S_2$ is a subgroup of $\operatorname{Aut} BX$. We are interested in cases where this subgroup is proper:

Definition 1.2 ([11, p. 160])**.** If $\operatorname{Aut} BX \neq \operatorname{Aut} X \times S_2$, then X is *unstable*.

It is easy to see (and well known) that if X is disconnected, or is bipartite, or has "twin" vertices (see Definition 2.5 below), then X is unstable (unless X is the trivial graph with only one vertex). The following definition rules out these trivial examples:

Definition 1.3 (cf. [20, p. 360])**.** If X is connected, nonbipartite, twin-free, and unstable, then X is *nontrivially unstable*.

S. Wilson found the following interesting conditions that force a circulant graph to be unstable. (See Definition 2.3 for the definition of the "Cayley graph" notation $\operatorname{Cay}(G,S)$.)

Theorem 1.4 (Wilson [20, Appendix A.1] (and [16, p. 156]))**.** *Let $X = \operatorname{Cay}(\mathbb{Z}_n, S)$ be a circulant graph, such that n is even. Let $S_e = S \cap 2\mathbb{Z}_n$ and $S_o = S \setminus S_e$. If any of the following conditions is true, then X is unstable.*

(C.1) *There is a nonzero element h of $2\mathbb{Z}_n$, such that $h + S_e = S_e$.*

(C.2′) *n is divisible by 4, and there exists $h \in 1 + 2\mathbb{Z}_n$, such that*

- *(a) $2h + S_o = S_o$, and*
- *(b) for each $s \in S$, such that $s \equiv 0$ or $-h \pmod 4$, we have $s + h \in S$.*

(C.3′) *There is a subgroup H of $\mathbb{Z}_n$, such that the set*

$$R = \{\, s \in S \mid s + H \not\subseteq S \,\},$$

is nonempty and has the property that if we let $d = \gcd\big(R \cup \{n\}\big)$, then n/d is even, r/d is odd for every $r \in R$, and either $H \not\subseteq d\mathbb{Z}_n$ or $H \subseteq 2d\mathbb{Z}_n$.

(C.4) *There exists $m \in \mathbb{Z}_n^\times$, such that $(n/2) + mS = S$.*

Remark 1.5. As will be explained in Remark 3.14, the statements (C.2′) and (C.3′) are slightly corrected versions of the original statements of Theorems C.2 and C.3 that appear in [20]. The correction (C.2′) is due to Qin-Xia-Zhou [16, p. 156].

Definition 1.6. We say that X has *Wilson type* (C.1), (C.2′), (C.3′), or (C.4), respectively, if it satisfies the corresponding condition of Theorem 1.4.

In this terminology (modulo the corrections mentioned in Remark 1.5), Wilson [20, p. 377] conjectured that every nontrivially unstable circulant graph has a Wilson type. Unfortunately, this is not true, because counterexamples of order 24 were found by Qin-Xia-Zhou [16, p. 156] (cf. Observation 6.1).

Three of our results provide new conditions that force a circulant graph to be unstable. (These conditions provide infinitely many new counterexamples.) It seems likely that other conditions (and additional counterexamples) remain to be discovered.

Our first condition includes (C.1) as the special case where $K = \mathbb{Z}_n$, includes (C.2′) as the special case where $K = 2\mathbb{Z}_n$, and includes (C.3′) as another special case (see Proposition 3.4).

Theorem 3.2 (cf. [20, Thms. 1, C.1, and C.3])**.** *Let $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph. Choose nontrivial subgroups H and K of $\mathbb{Z}_n$, such that $|K|$ is even, and let $K_o = K \setminus 2K$. If either*

(1) *$S + H \subseteq S \cup (K_o + H)$ and $H \cap K_o = \varnothing$, or*

(2) *$(S \setminus K_o) + H \subseteq S \cup K_o$ and either $|H| \neq 2$ or $|K|$ is divisible by 4,*

then X is not stable.

Our second condition is the following generalization of (C.4).

Proposition 3.7. *Assume $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph of even order. If $X \cong \mathrm{Cay}\big(\mathbb{Z}_n, (n/2) + S\big)$, then X is unstable.*

Letting S_e be the set of even elements of S, and S_o be the set of odd elements, as in Theorem 1.4, our third condition states that if $\mathrm{Cay}(\mathbb{Z}_n, S_e)$ is unstable, and S_o is invariant under sufficiently many translations, then X is unstable.

Proposition 3.12. *Assume $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph of even order. If there exist permutations α and β of $2\mathbb{Z}_n$, and a subgroup H of $2\mathbb{Z}_n$, such that:*

(1) *$\alpha \neq \beta$,*

(2) *if the vertices $u, v \in 2\mathbb{Z}_n$ are adjacent, then the vertices $\alpha(u)$ and $\beta(v)$ are also adjacent,*

(3) *$w + H \subseteq S$, for all odd $w \in S$, and*

(4) *$\alpha(v) - v \in H$ and $\beta(v) - v \in H$, for all $v \in 2\mathbb{Z}_n$,*

then X is unstable.

Wilson's conjecture is vacuously true for graphs of odd order:

Theorem 1.10 (Fernandez-Hujdurović [4] (or [12]))**.** *There are no nontrivially unstable circulant graphs of odd order.*

Therefore, only graphs of even order are of interest. Another of our main results shows that the conjecture is true in the easiest of these interesting cases:

Theorem 5.1. *If p is a prime number, then every nontrivially unstable circulant graph of order $2p$ has Wilson type* (C.4)*.*

This allows us to provide an explicit description of the nontrivially unstable circulant graphs of such orders:

Corollary 5.7. *Let $X = \mathrm{Cay}(\mathbb{Z}_{2p}, S)$ be a connected, twin-free, nonbipartite, circulant graph of order $2p$, where p is prime, and let $S_e = S \cap 2\mathbb{Z}_{2p}$. The graph X is nontrivially unstable if and only if there exists $m \in \mathbb{Z}_{2p}^{\times}$, such that $m^2 S_e = S_e$, $mS_e \neq S_e$, and $S = S_e \cup \big((n/2) + mS_e\big)$.*

It also makes it possible to strengthen Theorem 1.10 to a determination of all the possible orders of nontrivially unstable circulant graphs:

Corollary 5.8. *For $n \in \mathbb{Z}^+$, there does **not** exist a nontrivially unstable circulant graph of order n if and only if either n is odd, or $n < 8$, or $n = 2p$, for some prime number $p \equiv 3 \pmod 4$.*

Here is an outline of the paper. After this introduction comes a short section of preliminaries. Our main results, which were described above, are proved in Section 3 (Theorem 3.2 and Propositions 3.7 and 3.12) and Section 5 (Theorem 5.1 and its corollaries). In between, Section 4 discusses a lemma from [12]. Finally, Section 6 briefly presents a few minor results that were obtained by computer exploration.

2 Preliminaries

For emphasis, and ease of reference, we repeat a basic assumption from the first paragraph of the introduction (and add an exception):

Assumption 2.1. All graphs in this paper are finite, undirected, and simple (no loops or multiple edges), except that loops will be allowed in Section 4 (see Assumption 4.1).

Notation 2.2. For convenience, proofs will sometimes use the following abbreviation:

$$\text{n} = n/2.$$

Definition 2.3. Let S be a subset of an abelian group G, such that $-s \in S$ for all $s \in S$, and $0 \notin S$.

(1) The *Cayley graph* $\mathrm{Cay}(G, S)$ is the graph whose vertices are the elements of G, and with an edge from v to w if and only if $w = v + s$ for some $s \in S$ (cf. [10, §1]).

(2) For $s \in S$, we let $\tilde{s} = (s, 1)$.

(3) Note that if $X = \mathrm{Cay}(G, S)$, and we let $\widetilde{S} = \{\, \tilde{s} \mid s \in S \,\}$, then

$$BX = \mathrm{Cay}\big(G \times \mathbb{Z}_2, \widetilde{S}\,\big).$$

For $s \in S$, we say that an edge uv of BX is an *s-edge* if $v = u \pm \tilde{s}$.

Remark 2.4. The reason that the set S in $\mathrm{Cay}(G, S)$ is not allowed to contain 0 is that Assumption 2.1 forbids the graphs in this paper from having loops.

Definition 2.5 (Kotlov-Lovász [7])**.** A graph X is *twin-free* if there do not exist two distinct vertices that have exactly the same neighbors.

Remark 2.6. It is easy to see (and well known) that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is twin-free if and only if there does not exist a nonzero $h \in \mathbb{Z}_n$, such that $h + S = S$.

The notion of "block" is a fundamental concept in the theory of permutation groups, but we need only the following special case:

Definition 2.7 (cf. [3, pp. 12–13])**.** Let $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph. A nonempty subset $\mathcal{B}$ of $V(BX)$ is a *block* for the action of $\mathrm{Aut}\, BX$ if, for every $\alpha \in \mathrm{Aut}\, BX$, we have

$$\text{either} \quad \alpha(\mathcal{B}) = \mathcal{B} \quad \text{or} \quad \alpha(\mathcal{B}) \cap \mathcal{B} = \varnothing.$$

It is easy to see that this implies $\mathcal{B}$ is a coset of some subgroup H of $\mathbb{Z}_n \times \mathbb{Z}_2$, and that every coset of H is a block. Indeed, the action of $\mathrm{Aut}\, BX$ permutes these cosets, so there is a natural action of $\mathrm{Aut}\, BX$ on the set of cosets.

Definition 2.8 (cf. [10, Defn. 3.1])**.** To say that a circulant graph $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ has the *Cayley Isomorphism Property* means that if S' is a subset of $\mathbb{Z}_n$, such that $X \cong \mathrm{Cay}(\mathbb{Z}_n, S')$, then there exists $m \in \mathbb{Z}_n^\times$, such that $S' = mS$.

Theorem 2.9 (Muzychuk [13])**.** *If n is either square-free, or twice a square-free number, then every Cayley graph on $\mathbb{Z}_n$ has the Cayley Isomorphism Property.*

3 Some conditions that imply instability

The following known result is elementary, but, for the reader's convenience, we briefly recall the proof.

Lemma 3.1 ([9, Thm. 3.2], [11, Prop. 4.2])**.** *Let X be a graph. If there exist permutations α and β of $V(X)$, such that $\alpha \neq \beta$ and, for every edge uv of X, the vertex $\alpha(u)$ is adjacent to $\beta(v)$, then X is unstable.*

The converse holds if BX is connected.

Sketch of proof. ($\Rightarrow$) Define $\varphi \in \mathrm{Aut}(BX)$ by

$$\varphi(v, i) = \begin{cases} \big(\alpha(v), i\big) & \text{if } i = 0, \\ \big(\beta(v), i\big) & \text{if } i = 1. \end{cases}$$

Since $\alpha \neq \beta$, we have $\varphi \notin \mathrm{Aut}\, X \times S_2$.

($\Leftarrow$) Let $\varphi \in \mathrm{Aut}\, BX$, such that $\varphi \notin \mathrm{Aut}\, X \times S_2$. Since BX is connected, we know that its bipartition is unique, so the bipartition sets are blocks for the action of $\mathrm{Aut}\, BX$. Therefore, after composing by a translation, we may assume $\varphi\big(\mathbb{Z}_n \times \{i\}\big) = \mathbb{Z}_n \times \{i\}$ for $i = 0, 1$. So we may define permutations α and β of $V(X)$ by $\varphi(v, 0) = \big(\alpha(v), 0\big)$ and $\varphi(v, 1) = \big(\beta(v), 1\big)$. □

Theorem 3.2 (cf. [20, Thms. 1, C.1, and C.3])**.** *Let $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph. Choose nontrivial subgroups H and K of $\mathbb{Z}_n$, such that $|K|$ is even, and let $K_o = K \setminus 2K$. If either*

(1) *$S + H \subseteq S \cup (K_o + H)$ and $H \cap K_o = \varnothing$, or*

(2) *$(S \setminus K_o) + H \subseteq S \cup K_o$ and either $|H| \neq 2$ or $|K|$ is divisible by 4,*

then X is not stable.

Proof (cf. proof of [20, Thm. 1]). Let h be a generator of H. We will define permutations α and β of $\mathbb{Z}_n$, such that Lemma 3.1 applies.

(1) Define

$$\alpha(x) = \begin{cases} x + h & \text{if } x \in 2K + H; \\ x & \text{otherwise;} \end{cases} \qquad \beta(x) = \begin{cases} x + h & \text{if } x \in K_o + H; \\ x & \text{otherwise.} \end{cases}$$

Note that $0 \notin K_o + H$ (because $H \cap K_o = \varnothing$), so $\beta(0) = 0$. Since $\alpha(0) = h$, this implies $\alpha \neq \beta$.

Given an edge uv of X, we wish to show that $\alpha(u)$ is adjacent to $\beta(v)$. We may assume that either u is moved by α or v is moved by β. In fact, we may assume that exactly one of the vertices is moved, for otherwise,

$$\beta(v) - \alpha(u) = (v + h) - (u + h) = v - u \in S.$$

This means we may assume that either $u \in 2K + H$ or $v \in K_o + H$, but not both. Letting $s = v - u \in S$, this implies $s \notin K_o + H$.

Also, we have

$$\beta(v) - \alpha(u) \in (v + H) - (u + H) = (v - u) + H = s + H,$$

so we may write $\beta(v) - \alpha(u) = s + h'$, for some $h' \in H$. By the first assumption of (1), we know $s + h' \in S \cup (K_o + H)$. Since $s \notin K_o + H$, this implies $s + h' \in S$, so $\alpha(u)$ is adjacent to $\beta(v)$.

(2) If $h \in 2K$, then $K_o + H = K_o$, so

$$(S \cap K_o) + H \subseteq K_o + H = K_o.$$

Since, by the first assumption of (2), we also have $(S \setminus K_o) + H \subseteq S \cup K_o$, this implies that (1) applies. Therefore, we may assume

$$h \notin 2K.$$

Define

$$\alpha(x) = \begin{cases} x + h & \text{if } x \in 2K; \\ x - h & \text{if } x \in 2K + h; \\ x & \text{otherwise} \end{cases} \qquad \beta(x) = \begin{cases} x + h & \text{if } x \in K_o; \\ x - h & \text{if } x \in K_o + h; \\ x & \text{otherwise.} \end{cases}$$

We claim that $\alpha \neq \beta$. Note that $\alpha(0) = h$. Therefore, if $\alpha = \beta$, then we must have $\beta(0) = h$. Since $0 \notin K_o$, this implies that $0 \in K_o + h$ (which means $h \in K_o$) and $-h = h$ (which means $|h| = 2$). Since $|h| = 2$ and $h \in K_o$, we see that $|H| = 2$ and that $|K|$ is not divisible by 4. This contradicts the second half of assumption (2), so the proof of the claim is complete.

Given an edge uv of X, we wish to show that $\alpha(u)$ is adjacent to $\beta(v)$. That is, we wish to show $\beta(v) - \alpha(u) \in S$. We have $v = u + s$ for some $s \in S$. We may assume

$$\beta(v) - \alpha(u) \neq v - u.$$

In particular, we cannot have both $\alpha(u) = u$ and $\beta(v) = v$. Therefore,

$$\text{either } \ u \in 2K \cup (2K + h) \ \text{ or } \ v \in K_o \cup (K_o + h).$$

Case 1. *Assume* $u \in 2K \cup (2K + h)$ ***and*** $v \in K_o \cup (K_o + h)$. We consider two different possibilities, but both of the arguments are very similar.

Subcase 1.1. *Assume* $u \in 2K$. Then $\alpha(u) = u + h$. Since $\beta(v) - \alpha(u) \neq v - u$, this implies $\beta(v) \neq v + h$, so $v \notin K_o$. By the assumption of Case 1, this implies $v \in K_o + h$, so $\beta(v) = v - h$. Hence, $\beta(v) - \alpha(u) = s - 2h$.

We have $u \in 2K$ and $v \in K_o + h$, so $s = v - u \in K_o + h$, which means $s - h \in K_o$. Since $h \notin 2K$, this implies $s \notin K_o$ and $s - 2h \notin K_o$. Since $s \notin K_o$, the first assumption of (2) tells us $s + H \subseteq S \cup K_o$. Since $s - 2h \notin K_o$, this implies $s - 2h \in S$. So $\alpha(u)$ is adjacent to $\beta(v)$.

Subcase 1.2. *Assume* $u \in 2K + h$. We have $\alpha(u) = u - h$. Since $\beta(v) - \alpha(u) \neq v - u$, this implies $\beta(v) \neq v - h$, so $v \notin K_o + h$. By the assumption of Case 1, this implies $v \in K_o$, so $\beta(v) = v + h$. Hence, $\beta(v) - \alpha(u) = s + 2h$.

We have $u \in 2K + h$ and $v \in K_o$, so $s = v - u \in K_o - h$, which means $s + h \in K_o$. Since $h \notin 2K$, this implies $s \notin K_o$ and $s + 2h \notin K_o$. Since $s \notin K_o$, the first assumption of (2) tells us $s + H \subseteq S \cup K_o$. Since $s + 2h \notin K_o$, this implies $s + 2h \in S$. So $\alpha(u)$ is adjacent to $\beta(v)$.

Case 2. *Assume Case* 1 *does not apply.* As in Case 1, we consider two different possibilities, but both of the arguments are very similar.

Subcase 2.1. *Assume* $u \in 2K \cup (2K + h)$. Choose $\delta \in \{0, 1\}$, such that $u \in 2K + \delta h$. We have $\alpha(u) = u + \epsilon h$, where $\epsilon = 1 - 2\delta$, and we also have $v \notin K_o \cup (K_o + h)$, since Case 1 does not apply, so $\beta(v) = v$. Since $u \in 2K + \delta h$, but $u + s = v \notin K_o + \delta h$, we have $s \notin K_o$. So the first assumption of (2) tells us $s + H \subseteq S \cup K_o$, so $s - \epsilon h \in S \cup K_o$. Since $\beta(v) - \alpha(u) = s - \epsilon h$, then we may assume $s - \epsilon h \in K_o$ (otherwise, $\alpha(u)$ is adjacent to $\beta(v)$, as desired), so $s \in K_o + \epsilon h$. Then

$$v = u + s \in (2K + \delta h) + (K_o + \epsilon h) = K_o + (\delta + \epsilon)h = K_o + (1 - \delta)h.$$

Since $1 - \delta \in \{0, 1\}$, but $v \notin K_o \cup (K_o + h)$, this is a contradiction.

Subcase 2.2. *Assume* $v \in K_o \cup (K_o + h)$. Choose $\delta \in \{0, 1\}$, such that $v \in K_o + \delta h$. We have $\beta(v) = v + \epsilon h$, where $\epsilon = 1 - 2\delta$, and we also have $u \notin 2K \cup (2K + h)$, since

Case 1 does not apply, so $\alpha(u) = u$. Since $v \in K_o + \delta h$, but $v - s = u \notin 2K + \delta h$, we have $s \notin K_o$. So the first assumption of (2) tells us $s + H \subseteq S \cup K_o$, so $s + \epsilon h \in S \cup K_o$. Since $\beta(v) - \alpha(u) = s + \epsilon h$, then we may assume $s + \epsilon h \in K_o$ (otherwise, $\alpha(u)$ is adjacent to $\beta(v)$, as desired), so $s \in K_o - \epsilon h$. Then

$$u = v - s \in (K_o + \delta h) - (K_o - \epsilon h) = 2K + (\delta + \epsilon)h = 2K + (1 - \delta)h.$$

Since $1 - \delta \in \{0, 1\}$, but $u \notin 2K \cup (2K + h)$, this is a contradiction. □

Remark 3.3. In the notation of Theorem 3.2, it is clear that

$$\big(S \cap (K_o + H)\big) + H \subseteq (K_o + H) + H = K_o + H.$$

Therefore, the first condition of 3.2(1) can be restated as:

$$\big(S \setminus (K_o + H)\big) + H \subseteq S.$$

Wilson types (C.1), (C.2′), and (C.3′) are special cases of Theorem 3.2(2):

Proposition 3.4. *If* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *has Wilson type* (C.1), (C.2′), *or* (C.3′), *then there are nontrivial subgroups* H *and* K *of* $\mathbb{Z}_n$ *that satisfy the conditions given in part* (2) *of Theorem* 3.2 (*and* $|K|$ *is even*).

Proof. (C.1) Let $K = \mathbb{Z}_n$ and $H = \langle h \rangle$. Then

$$(S \setminus K_o) + H = S_e + \langle h \rangle = S_e \subseteq S,$$

so the first condition of 3.2(2) is satisfied. Also, since $h \in 2\mathbb{Z}_n = 2K$, it must be true that either $|H| \neq 2$ or $|K|$ is divisible by 4.

(C.2′) Let $H = \langle h \rangle$ and $K = 2\mathbb{Z}_n$. (Note that $|H| > 2$, since h is odd and n is divisible by 4.) Then

$$K_o = \{\, x \in \mathbb{Z}_n \mid x \equiv 2 \pmod 4 \,\}.$$

We will show that $(S \setminus K_o) + H \subseteq S \cup K_o$.

We may assume $h \equiv 1 \pmod 4$, by applying the graph automorphism $x \mapsto -x$ if necessary. Fix some $s \in S \setminus K_o$.

Suppose, first, that $s \not\equiv 0 \pmod 4$ (and recall that $s \notin K_o$, so $s \not\equiv 2 \pmod 4$), so s is odd. This means $s \in S_o$, so we see from C.2′(a) that $s + 2kh \in S$ for all $k \in \mathbb{Z}$. If $s + 2kh \equiv 3 \pmod 4$, then $s + (2k + 1)h \in S$ (by C.2′(b)). If $s + 2kh \equiv 1 \pmod 4$, then $s + (2k + 1)h \in K_o$. Thus, we have $s + H \subseteq S \cup K_o$.

Now, suppose $s \equiv 0 \pmod 4$. Then $s + h \in S$ (by C.2′(b)). Now, since $s + h \not\equiv 0 \pmod 4$, the previous case tells us that $s + h + H \subseteq S \cup K_o$. Since $h + H = H$, this means $s + H \subseteq S \cup K_o$.

(C.3′) Let $K = \langle R \rangle = \langle d \rangle$. Since n/d is even, we know that K has even order. Then, since r/d is odd for every $r \in R$, we see that $R \subseteq K_o$. By the definition of R, this means $(S \setminus K_o) + H \subseteq S$, so the first condition of 3.2(2) is satisfied.

Also, since either $H \not\subseteq d\mathbb{Z}_n$ or $H \subseteq 2d\mathbb{Z}_n$, we know that either $H \not\subseteq K$ or $H \subseteq 2K$. If $H \not\subseteq K$ and $|H| = 2$, then it is clear that $H \cap K = \{0\} \subseteq 2K$. Thus, in both cases, we have $H \cap K \subseteq 2K$, which easily implies that either $|H| \neq 2$ or $|K|$ is divisible by 4. □

There is a strong converse to Proposition 3.4 when n is not divisible by 4:

Proposition 3.5. *If $X = \mathrm{Cay}(\mathbb{Z}_n, S)$, H, and K satisfy the conditions of Theorem* 3.2(2)*, and n is not divisible by* 4*, then X has Wilson type* (C.1)*.*

Proof. Since n is not divisible by 4, it is not possible for $|K|$ to be divisible by 4, so the second half of Theorem 3.2(2) tells us that $|H| > 2$. This implies that $H_e \coloneqq H \cap 2\mathbb{Z}_n$ is nontrivial. Also, since n is not divisible by 4, we know that $K_o \cap 2\mathbb{Z}_n = \varnothing$, so

$$S_e + H_e = (S \cap 2\mathbb{Z}_n) + H_e \subseteq (S \setminus K_o) + H \subseteq S \cup K_o \subseteq S \cup (\mathbb{Z}_n \setminus 2\mathbb{Z}_n).$$

Since $H_e \subseteq 2\mathbb{Z}_n$, we also know that $S_e + H_e \subseteq 2\mathbb{Z}_n$. Therefore, we conclude that $S_e + H_e \subseteq S_e$, so X has Wilson type (C.1). □

Remark 3.6. By combining Propositions 3.4 and 3.5, we see that if X has a Wilson type, and n is not divisible by 4, then X must have Wilson type (C.1) or (C.4).

Proposition 3.7. *Assume $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph of even order. If $X \cong \mathrm{Cay}\big(\mathbb{Z}_n, S + (n/2)\big)$, then X is unstable.*

Proof. If α is an isomorphism from $\mathrm{Cay}(\mathbb{Z}_n, S)$ to $\mathrm{Cay}(\mathbb{Z}_n, S + \not{n})$, then Lemma 3.1 applies with $\beta(x) = \alpha(x) + \not{n}$. □

Remarks 3.8.

(1) Proposition 3.7 is a generalization of Wilson type (C.4). To see this, note that if $\not{n} + mS = S$, then $mS = S + \not{n}$. Also, it is well known that if $m \in \mathbb{Z}_n^\times$, then $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, mS)$ (cf. [5, Lem. 3.7.3, p. 48]). Therefore, we conclude that $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, S + \not{n})$, so Proposition 3.7 applies.

(2) M. Muzychuk [14] found an efficient method to check whether two circulant graphs (such as $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S + \not{n})$) are isomorphic.

Here is a family of examples that illustrate Proposition 3.7:

Example 3.9. Let $n = 2p^2$, where p is prime and $p \equiv 1 \pmod 4$, and choose $c \in \mathbb{Z}$, such that $c^2 \equiv -1 \pmod p$. Fix some $a \in \mathbb{Z}_n$ of order p, and let $S = S_e \cup S_o$, where

$$\begin{aligned} S_e &= \big(\pm 2 + \langle a \rangle\big) \cup \{\pm a\} \subseteq 2\mathbb{Z}_n, \\ S'_o &= \big(\pm 2 + \langle a \rangle\big) \cup \{\pm ca\} \subseteq 2\mathbb{Z}_n, \\ S_o &= \not{n} + S'_o \subseteq 1 + 2\mathbb{Z}_n. \end{aligned}$$

Then

(1) $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}\big(\mathbb{Z}_n, S + (n/2)\big)$, so Proposition 3.7 implies that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is (nontrivially) unstable, but

(2) $\mathrm{Cay}(\mathbb{Z}_n, S)$ does not have a Wilson type.

Proof. (1) Choose a set $\mathcal{R}$ of coset representatives for $\langle a\rangle$ in $\mathbb{Z}_n$, such that $\mathcal{R} + \not{n} = \mathcal{R}$, and define $\alpha\colon \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$\alpha(r + x) = r + cx \quad \text{for } r \in \mathcal{R} \text{ and } x \in \langle a\rangle.$$

It suffices to show that if $v, w \in \mathbb{Z}_n$, such that $v - w \in S$, then $\alpha(v) - \alpha(w) \in S + \not{n}$.

First, consider two vertices $v = r + x$ and $w = r + y$ that are in the same coset of $\langle a\rangle$. Then the definition of S implies that $v - w = \pm a$, so $y = x \pm a$, so

$$\alpha(v) - \alpha(w) = \big(r + cx\big) - \big(r + c(x \pm a)\big) = \pm ca \in S'_o = S_o + \not{n}.$$

Next, suppose $v \in w + \not{n} + \langle a\rangle$. Assume, without loss of generality, that $v \in 1 + 2\mathbb{Z}_n$ and $w \in 2\mathbb{Z}_n$. Write $v = r + \not{n} + x$ and $w = r + y$ with $r \in \mathcal{R}$ and $x, y \in \langle a\rangle$. The definition of S implies that $v - w = \not{n} \pm ca$, so $y = x \pm ca$, so (using the fact that $c^2 \equiv -1 \pmod p$) we have

$$\alpha(v) - \alpha(w) = \big(r + \not{n} + cx\big) - \big(r + c(x \pm ca)\big) = \not{n} \pm c^2 a = \not{n} \mp a \in \not{n} + S_e.$$

We may now assume that v and w are in two different cosets of $\langle a, \not{n}\rangle$. Then, from the definition of S, we see that every vertex in $v + \langle a\rangle$ is adjacent to every vertex in $w + \langle a\rangle$. Since $\alpha(v) \in v + \langle a\rangle$ and $\alpha(w) \in w + \langle a\rangle$, it is therefore obvious that $\alpha(v)$ is adjacent to $\alpha(w)$.

(2) The proof is by contradiction.

Suppose, first, that $\mathrm{Cay}(\mathbb{Z}_n, S)$ has Wilson type (C.1), (C.2′), or (C.3′). Then Remark 3.6 tells us that the graph actually has Wilson type (C.1), so $h + S_e = S_e$ for some non-zero $h \in 2\mathbb{Z}_n$. Since $2\mathbb{Z}_n \cong \mathbb{Z}_{p^2}$, we know that $|h|$ is divisible by p. Since S_e is a union of cosets of $\langle h\rangle$, this implies that $|S_e|$ is divisible by p, which contradicts the fact that $|S_e| = 2|a| + 2 = 2p + 2$.

We may now assume that the graph is of Wilson type (C.4). Then we can find $m \in \mathbb{Z}^\times_{2p^2}$, such that $mS + \not{n} = S$. Since $\not{n}$ is odd, this implies $mS_e + \not{n} = S_o$, so $mS_e = S'_o$. By passing to the quotient group $2\mathbb{Z}_n/\langle a\rangle$, we conclude that $m \equiv \pm 1 \pmod p$. So $ma = a \notin S'_o$. This contradicts the fact that $mS_e = S'_o$. □

It is shown in [6] that every nontrivially unstable circulant graph of valency $\leqslant 7$ has a Wilson type, so the following examples have minimal valency among those that do not have a Wilson type:

Example 3.10. Let $n \coloneqq 3 \cdot 2^\ell$, where $\ell \geqslant 4$ is even, and let

$$S \coloneqq \left\{\pm 3, \pm 6, \pm\frac{n}{12}, \frac{n}{2} \pm 3\right\}.$$

Then the circulant graph $X \coloneqq \mathrm{Cay}(\mathbb{Z}_n, S)$ has valency 8 and is nontrivially unstable, but does not have a Wilson type.

Proof. It is easy to see that X is connected, nonbipartite, and twin-free. For convenience, let $a = n/12$.

(unstable) Let $\rho_0\colon 2\mathbb{Z}_n \to \mathbb{Z}_2$ be the homomorphism with kernel $4\mathbb{Z}_n$. Then define $\rho\colon \mathbb{Z}_n \to \mathbb{Z}_2$ by

$$\rho(v) = \begin{cases} \rho_0(v) & \text{if } v \in 2\mathbb{Z}_n; \\ \rho_0(v+1) & \text{otherwise.} \end{cases}$$

Finally, we let $m \coloneqq (n/6) - 1$, and define

$$\alpha(v) = mv + \rho(v)\cancel{n}.$$

We will show that α is an isomorphism from X to $X \cong \mathrm{Cay}(\mathbb{Z}_n, S + \cancel{n})$, so Proposition 3.7 shows that X is unstable. Thus, given $v \in \mathbb{Z}_n$ and $s \in S$, we wish to show that

$$\alpha(v+s) - \alpha(v) \in S + \cancel{n}. \tag{3.11}$$

From the choice of m, we have $m \cdot 3 = \cancel{n} - 3$, and a straightforward calculation shows that $m(\cancel{n} + 3) = -3$ (in $\mathbb{Z}_n$), so

$$m\{\pm 3, \cancel{n} \pm 3\} + \langle \cancel{n} \rangle = \{\pm 3, \cancel{n} \pm 3\} \subseteq S.$$

Since it is clear from the definition of α that $\alpha(v+s) - \alpha(v) \in ms + \langle \cancel{n} \rangle$, this implies that (3.11) holds for $s \in \{\pm 3, \cancel{n} \pm 3\}$.

To deal with the remaining elements ± 6 and $\pm a$ of S, first note that $6 \notin 4\mathbb{Z}_n$ and $a = 2^{\ell-2} \in 4\mathbb{Z}_n$ (since $\ell \geqslant 4$), so $\rho_0(6) = 1$ and $\rho_0(a) = 0$. Hence, for all $v \in \mathbb{Z}_n$, we have

$$\rho(v \pm 6) = \rho(v) + 1 \text{ and } \rho(v \pm a) = \rho(v).$$

Therefore, we have

$$\begin{aligned} \alpha(v \pm 6) - \alpha(v) &= \big(m(v \pm 6) + \rho(v \pm 6)\cancel{n}\big) - \big(mv + \rho(v)\cancel{n}\big) \\ &= \pm 6m + \big(\rho(v \pm 6) - \rho(v)\big)\cancel{n} \\ &= \pm(n-6) + \cancel{n} \\ &\equiv \pm 6 + \cancel{n} && \pmod{n} \\ &\in S + \cancel{n}. \end{aligned}$$

Also note that $2^{\ell-1} \equiv 8 \pmod{12}$ (because $\ell - 1 \geqslant 3$ is odd), so we have $m = 2^{\ell-1} - 1 = 6k + 1$, where k is odd. Therefore

$$\begin{aligned} \alpha(v \pm a) - \alpha(v) &= \big(m(v \pm a) + \rho(v \pm a)\cancel{n}\big) - \big(mv + \rho(v)\cancel{n}\big) \\ &= \pm ma + \big(\rho(v \pm a) - \rho(v)\big)\cancel{n} \\ &= \pm(6k+1)a + 0\cancel{n} \\ &= \pm(k\cancel{n} + a) \\ &= \pm a + \cancel{n} \\ &\in S + \cancel{n}. \end{aligned}$$

(no Wilson type) First, suppose that the graph has Wilson type (C.1), (C.2′), or (C.3′). By Proposition 3.4, this implies there are subgroups H and K of $\mathbb{Z}_n$ that satisfy the conditions of Theorem 3.2(2). In particular, at least one coset of H is completely contained in S.

We claim that $H = \langle \not{n} \rangle$. Let $h = n/|H|$, so h is a divisor of n, and $H = \langle h \rangle$. Since S contains a coset of H, we know that at least one of any h consecutive elements $x+1, x+2, \ldots, x+h$ of $\mathbb{Z}_n$ is an element of S. Since $(\not{n} - 3) - (n/12) > n/3$, this easily implies $h = \not{n}$, which completes the proof of the claim.

Since $6 + \not{n} \notin S$ and $(n/12) + \not{n} \notin S$, we then see from the first half of 3.2(2) that $6 \in K_o$ and $n/12 \in K_o$. This is impossible, because $n/12$ is divisible by 4, but 6 is not.

Now suppose that the graph has Wilson type (C.4). This means there is some $m \in \mathbb{Z}_n^\times$, such that $mS = S + \not{n}$. Since $\not{n}$ is even, this implies $mS_o = S_o + \not{n}$, so (perhaps after replacing m with $-m$, we have $m \cdot 3 \in \{3, \not{n} + 3\}$. But then

$$m \cdot 6 + \not{n} = 2(m \cdot 3) + \not{n} \in 2\{3, \not{n} + 3\} + \not{n} = \{6 + \not{n}\}.$$

Since $6 + \not{n} \notin S$, this is a contradiction. □

Proposition 3.12. *Assume $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph of even order. If there exist permutations α and β of $2\mathbb{Z}_n$, and a subgroup H of $2\mathbb{Z}_n$, such that:*

(1) *$\alpha \neq \beta$,*

(2) *if the vertices $u, v \in 2\mathbb{Z}_n$ are adjacent, then the vertices $\alpha(u)$ and $\beta(v)$ are also adjacent,*

(3) *$s + H \subseteq S$, for all odd $s \in S$, and*

(4) *$\alpha(v) - v \in H$ and $\beta(v) - v \in H$, for all $v \in 2\mathbb{Z}_n$,*

then X is unstable.

Proof. Define permutations α' and β' of $\mathbb{Z}_n$ by stipulating that

$$\alpha'(v) = \beta'(v) = v \text{ if } v \text{ is odd,}$$

whereas

$$\alpha'(v) = \alpha(v) \text{ and } \beta'(v) = \beta(v) \text{ if } v \text{ is even.}$$

It is straightforward to verify that if uv is an edge of X, then $\alpha'(u)$ is adjacent to $\beta'(v)$, so Lemma 3.1 tells us that X is unstable. □

The following result is the special case where $\mathrm{Cay}(2\mathbb{Z}_n, S \cap 2\mathbb{Z}_n)$ has Wilson type (C.4).

Corollary 3.13. *Assume $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph with $n \equiv 0 \pmod 4$. If there exists $m \in \mathbb{Z}_n^*$, such that $mS_e + \not{n} = S_e$, and $S_o + 2(m-1)\mathbb{Z}_n = S_o + \not{n} = S_o$, then X is unstable.*

Proof. Define permutations α and β of $2\mathbb{Z}_n$ by $\alpha(x) = mx$ and $\beta(x) = mx + \not{n}$. (The assumption that $n \equiv 0 \pmod 4$ implies that $\not{n}$ is even, so the image of β is in $2\mathbb{Z}_n$.) Let $H = \langle 2(m-1)\mathbb{Z}_n, \not{n} \rangle$, so $S_o + H = S_o$, by assumption. Then Proposition 3.12 applies, since $\alpha(v) - v = (m-1)v \in 2(m-1)\mathbb{Z}_n \subseteq H$ and $\beta(v) - v = (m-1)v + \not{n} \subseteq H$. □

Remark 3.14. Parts (C.2′) and (C.3′) of the statement of Theorem 1.4 are corrected versions of the original statements of Theorems C.2 and C.3 that appear in [20].

(C.2′) Y.-L. Qin, B. Xia, and S. Zhou [16] corrected the original hypothesis (C.2) by adding condition (b). (Note that complete graphs with more than two vertices are stable [16, Eg. 2.2], but satisfy condition (a) with $h = 1$, so this condition alone does not imply instability, even when n is divisible by 4.)

(C.3′) The original statement of hypothesis (C.3) in [20, p. 376] includes the extraneous hypothesis that $d > 1$, and neglects to state the requirements that n/d is even and that either $H \not\subseteq d\mathbb{Z}_n$ or $H \subseteq 2d\mathbb{Z}_n$. (*Explanation:* [20, Thm. 1] does not require the Cayley graph generated by the red edges to be disconnected, so there is no need to assume $d > 1$. The proof of [20, Thm. C.3] uses the assumption that r/d is odd to conclude that each component of $\mathrm{Cay}(\mathbb{Z}_n, R)$ is bipartite; this requires each $r \in R$ to be an element of even order in $\mathbb{Z}_n$, which means that $n/\gcd(r, n)$ is even. Conditions (1) and (2) near the bottom of [20, p. 360] translate to the requirement that either $H \not\subseteq d\mathbb{Z}_n$ or $H \subseteq 2d\mathbb{Z}_n$.)

It was mentioned above that if $n > 2$, then the complete graph K_n is stable [16, Eg. 2.2]. However, if n is even, then K_n satisfies the conditions in the original statement of (C.3) (with $H = \langle n/2 \rangle$, $R = \{n/2\}$, $d = n/2$, and $r/d = 1$ for the unique element r of R). This shows that the additional conditions in (C.3′) cannot be deleted.

4 The main lemma of [12]

Assumption 4.1. For the proof of Corollary 4.7, it will be helpful to temporarily relax our standing assumption that all graphs are simple (see Assumption 2.1). Namely graphs are allowed to have loops (but not multiple edges) in this section.

The following elementary observation is stated only for automorphisms in [12], but the same proof applies to isomorphisms.

Lemma 4.2 (cf. [12, Lem. 2.2])**.** *Let $m \in \mathbb{Z}^+$, and let $X_1 = \mathrm{Cay}(G_1, S_1)$ and $X_2 = \mathrm{Cay}(G_2, S_2)$ be Cayley graphs, such that*

(1) *G_1 and G_2 are abelian, and*

(2) *for $j = 1, 2$, we have $ms \neq mt$ for all $s, t \in S_j$, such that $s \neq t$.*

If φ is any isomorphism from X_1 to X_2, then φ is also an isomorphism from $\mathrm{Cay}(G_1, mS_1)$ to $\mathrm{Cay}(G_2, mS_2)$, where $mS_j = \{\, ms \mid s \in S_j \,\}$.

Proof (cf. proof of [12, Lem. 2.2]). Write $m = p_1 p_2 \cdots p_r$, where each p_i is prime, and let $m_i = p_1 p_2 \cdots p_i$ for $0 \leqslant i \leqslant r$. We will prove by induction on i that φ is an isomorphism

from $\mathrm{Cay}(G_1, m_i S_1)$ to $\mathrm{Cay}(G_2, m_i S_2)$ The base case is true by assumption, since $m_0 S_j = 1S_j = S_j$.

For $v, w \in G_j$, let $\#(v, w)$ be the number of walks of length p_i from v to w in the graph $\mathrm{Cay}(G_j, m_{i-1}S_j)$. These walks are in one-to-one correspondence with the p_i-tuples $(s_1, s_2, \ldots, s_{p_i})$ of elements of $m_{i-1}S_j$, such that

$$s_1 + s_2 + \cdots + s_{p_i} = w - v.$$

Since G_j is abelian, any cyclic rotation of $(s_1, s_2, \ldots, s_{p_i})$ also corresponds to a walk from v to w. Therefore, the set of these walks can be partitioned into sets of cardinality p_i, unless $w = p_i s + v$, for some $s \in m_{i-1}S_j$, in which case there is a walk of the form $v, s+v, 2s+v, \ldots, p_i s+v = w$. (Also note that s is unique, if it exists, by assumption (2).) Hence, we see that

$$\#(v, w) \not\equiv 0 \pmod{p_i} \quad \iff \quad v \text{ is adjacent to } w \text{ in } \mathrm{Cay}(G_j, p_i m_{i-1} S_j).$$

Since $p_i m_{i-1} = m_i$, the desired conclusion that φ is an isomorphism from $\mathrm{Cay}(G_1, m_i S_1)$ to $\mathrm{Cay}(G_2, m_i S_2)$ now follows from the induction hypothesis that φ is an isomorphism from $\mathrm{Cay}(G_1, m_{i-1} S_1)$ to $\mathrm{Cay}(G_2, m_{i-1} S_2)$ (and the observation that isomorphisms preserve the value of the function $\#$). □

Corollary 4.3. *Let $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ be a circulant graph of even order, let φ be an automorphism of BX, and let*

$$S' = \{\, s' \in S \mid s' + (n/2) \notin S \,\}.$$

Then φ is an automorphism of $\mathrm{Cay}(\mathbb{Z}_n \times \mathbb{Z}_2, 2S' \times \{0\})$.

Proof. For every $s \in S$, we have

$$\{\, (t,1) \in G \times \{1\} \mid 2(t,1) = 2(s,1) \,\} = \{(s,1), (s + \pi, 1)\},$$

since π is the unique element of order 2 in $\mathbb{Z}_n$. Hence, the set

$$\{\, (t,1) \in S \times \{1\} \mid 2(t,1) = 2(s,1) \,\}$$

has cardinality 1 (which is odd) if $s + \pi \notin S$, and has cardinality 2 (which is even) otherwise. Therefore, the desired conclusion is obtained by applying the proof of Lemma 4.2 with $G_1 = G_2 = \mathbb{Z}_n \times \mathbb{Z}_2$ and $m = 2$, since $2(S' \times \{1\}) = 2S' \times \{0\}$. □

Corollary 4.4 ([12, Rem. 3.1], [17, Thm. 23.9(a), p. 58])**.** *Let φ be an automorphism of a Cayley graph $\mathrm{Cay}(G, S)$, and let $m \in \mathbb{Z}^+$. If G is abelian and $\gcd\big(m, |G|\big) = 1$, then φ is an automorphism of $\mathrm{Cay}(G, mS)$.*

Proof. Apply Lemma 4.2 with $G_1 = G_2 = G$ and $S_1 = S_2 = S$. To verify hypothesis (2) of the lemma, note that the map $x \mapsto mx$ is a bijection on G, since $\gcd\big(m, |G|\big) = 1$. □

Corollary 4.5. *Let α be an automorphism of BX, where $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph, let $s, t \in S$, and let $k, \ell \in \mathbb{Z}^+$. Assume*

(1) *α maps some s-edge to a t-edge,*

(2) *$ks \in S$,*

(3) *$k \equiv \ell \pmod{\gcd\big(|s|, |t|\big)}$, and*

(4) *$\gcd\big(k, |s|\big) = \gcd\big(\ell, |t|\big) = 1$.*

Then $\ell t \in S$.

Proof. By assumption (3), there exists $m \in \mathbb{Z}^+$, such that $m \equiv k \pmod{s}$ and $m \equiv \ell \pmod{|t|}$. Then assumption (4) implies that m is relatively prime to $|s|$ and $|t|$, so, by Dirichlet's Theorem on primes in arithmetic progressions, we may choose a prime $p > 2n$, such that $pm \equiv 1 \pmod{\mathrm{lcm}\big(|s|, |t|\big)}$. This implies $pks = s$ and $p\ell t = t$.

Since p is relatively prime to $|\mathbb{Z}_n \times \mathbb{Z}_2|$, we know from Corollary 4.4 that every automorphism of BX is an automorphism of $\mathrm{Cay}\big(\mathbb{Z}_n \times \mathbb{Z}_2, p\big(S \times \{1\}\big)\big)$. Since $(s, 1) = p(ks, 1) \in p\big(S \times \{1\}\big)$, and α maps some s-edge to a t-edge, this implies that $t \in pS$. Since $t = p\ell t$, and multiplication by p is a bijection on $\mathbb{Z}_n \times \mathbb{Z}_2$, this implies $\ell t \in S$. □

Here are two interesting special cases:

Corollary 4.6. *Let α be an automorphism of BX, where $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a circulant graph, and let $s, t \in S$. If α maps some s-edge to a t-edge, and either $\gcd\big(|s|, |t|\big) = 1$, or S contains every element that generates $\langle s \rangle$ (e.g., if $|s| \in \{1, 2, 3, 4, 6\}$), then S contains every element that generates $\langle t \rangle$.*

Proof. Let ℓt be a generator of $\langle t \rangle$, so $\gcd\big(\ell, |t|\big) = 1$. It suffices to find $k \in \mathbb{Z}^+$, such that

$$ks \in S, \;\; k \equiv \ell \pmod{\gcd\big(|s|, |t|\big)}, \;\text{ and }\; \gcd\big(k, |s|\big) = 1,$$

for then Corollary 4.5 tells us that $\ell t \in S$.

If $\gcd\big(|s|, |t|\big) = 1$, we may let $k = 1$.

Since $\gcd\big(\ell, |t|\big) = 1$, we know that ℓ is relatively prime to $\gcd\big(|s|, |t|\big)$, so there is some $k \in \mathbb{Z}^+$, such that

$$k \equiv \ell \pmod{\gcd\big(|s|, |t|\big)} \;\text{ and }\; \gcd\big(k, |s|\big) = 1.$$

(For example, we could take k to be a large prime.) If S contains every element that generates $\langle s \rangle$, then $ks \in S$. □

Recall that the following cor's assumption that X is loopless will automatically be satisfied in all of the following sections of the paper (see Assumption 2.1).

Corollary 4.7. *Let α be an automorphism of BX, where $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ is a connected, nonbipartite, loopless, circulant graph, and let $t \in \mathbb{Z}_n$. If $\alpha(0, 1) = (t, 1)$, then S does not contain any generator of the subgroup $\langle t \rangle$.*

Proof. Let $S^c = G \setminus S$ be the complement of S, and let $X^c = \mathrm{Cay}(\mathbb{Z}_n, S^c)$. Since BX is connected, it is easy to see that every automorphism of BX is also an automorphism of BX^c.

Note that $0 \in S^c$, since X is assumed to be loopless. Therefore, we may let $s = 0$ (so $|s| = 1$) to conclude from Corollary 4.6 that S^c contains every generator of $\langle t \rangle$. □

The following result is stated only for automorphisms in [12], but essentially the same proof applies to isomorphisms.

Corollary 4.8 (cf. [12, Thm. 1.1])**.** *Assume $X_1 = \mathrm{Cay}(\mathbb{Z}_n, S_1)$ and $X_2 = \mathrm{Cay}(\mathbb{Z}_n, S_2)$ are twin-free, connected, circulant graphs of odd order. If φ is any isomorphism from BX_1 to BX_2, such that*

$$\varphi(\mathbb{Z}_n \times \{0\}) = \mathbb{Z}_n \times \{0\},$$

then there is an isomorphism $\alpha\colon X_1 \to X_2$, such that $\varphi(x, i) = \big(\alpha(x), i\big)$ for all $(x, i) \in BX_1$.

Proof. This follows quite easily from Lemma 4.2 (with $m = n + 1$), by the argument in the proof of [12, Thm. 1.1]. □

5 Unstable circulant graphs of order $2p$

Theorem 5.1. *If p is a prime number, then every nontrivially unstable circulant graph of order $2p$ has Wilson type* (C.4)*.*

The proof of this theorem will use several lemmas that are stated in greater generality than is needed here, because they may be useful for understanding the unstable circulant graphs of other square-free orders.

Lemma 5.2. *Let $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ be a connected, nonbipartite, circulant graph, such that $n \equiv 2 \pmod 4$. Then X has Wilson type* (C.1) *if and only if BX has an automorphism α, such that*

(1) *$\alpha \notin \mathrm{Aut}\, X \times S_2$, and*

(2) *α fixes $2\mathbb{Z}_n \times \mathbb{Z}_2$ (setwise).*

Proof. ($\Rightarrow$) This is the easy half of the proof (and does not require the assumption that $n \equiv 2 \pmod 4$). If $h + S_e = S_e$, then we may define $\alpha \in \mathrm{Aut}(BX)$ by

$$\alpha(x, i) = \begin{cases} (x + h, i) & \text{if } x \equiv i \pmod 2, \\ (x, i) & \text{if } x \not\equiv i \pmod 2. \end{cases}$$

($\Leftarrow$) Since $\alpha \notin \mathrm{Aut}\, X \times S_2$, there is some $v \in \mathbb{Z}_n$, such that $\alpha(v, 1) \neq \alpha(v, 0) + (0, 1)$. After conjugating α by a translation that moves $(v, 0)$ to $(0, 0)$, we may assume $v = 0$. This means that $\alpha(0, 0) = (0, 0)$ and $\alpha(0, 1) \neq (0, 1)$.

Let $S_e = S \cap 2\mathbb{Z}_n$, and let $X_e = \mathrm{Cay}(2\mathbb{Z}_n, S_e)$, so the subgraph of X induced by $2\mathbb{Z}_n \times \mathbb{Z}_2$ is BX_e. Then assumption (2) implies that α restricts to an automorphism of BX_e.

Now, let X'_e be the connected component of X_e that contains 0. Since $n \equiv 2 \pmod 4$, we know that $n/2$ is odd, so $|\langle S_e \rangle|$ is odd. This implies that BX'_e is connected, and is therefore a connected component of BX_e. Since BX'_e contains the fixed point $(0,0)$, we conclude that BX'_e is α-invariant. Therefore, α restricts to an automorphism of BX'_e. Since α fixes $(0,0)$, then it follows from Theorem 1.10 that $\alpha(0,1) = (0,1)$. This is a contradiction. □

Lemma 5.3 (Klin-Muzychuk, 1995, personal communication)**.** *Let*

- $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ *be a circulant graph of order* n*,*
- G *be an abelian group of order* n*,*
- $e \in \mathbb{Z}$*, such that* $eg = 0$ *for all* $g \in G$*, and*
- $m \in \mathbb{Z}$*, such that* $m \equiv 1 \pmod e$ *and* $\gcd(m, n) = 1$*.*

If X *is isomorphic to some Cayley graph* $\mathrm{Cay}(G, T)$ *on* G*, then* $S = mS$*.*

Proof (Klin-Muzychuk). Let ζ be a primitive nth root of unity, and, for $1 \leqslant i \leqslant n$, let $\lambda_i = \sum_{s \in S} \zeta^{is}$, so $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of X [2, Prop. 3.5, p. 16]. Since $\gcd(m, n) = 1$, there is a Galois automorphism α of the field extension $\mathbb{Q}[\zeta]/\mathbb{Q}$, such that $\alpha(\zeta) = \zeta^m$ [8, Thm. 6.3.1, p. 278]. Since $eg = 0$ for all $g \in G$ (and G is abelian), we know that each eigenvalue of $\mathrm{Cay}(G, T)$ is a sum of eth roots of unity. (The range of any homomorphism $\chi \colon G \to \mathbb{C}^\times$ consists of eth roots of unity, so this is a consequence of the well-known formula in [1, Cor. 3.2] that generalizes the above formula for the eigenvalues of a circulant graph.) Since $m \equiv 1 \pmod e$, this implies that every eigenvalue of $\mathrm{Cay}(G, T)$ is fixed by α. So $\lambda_1, \lambda_2, \ldots, \lambda_n$ are fixed by α. For $1 \leqslant i \leqslant n$, this means

$$\sum_{s \in S} \zeta^{is} = \lambda_i = \alpha(\lambda_i) = \alpha\left(\sum_{s \in S} \zeta^{is}\right) = \sum_{s \in S} \zeta^{mis} = \sum_{s \in mS} \zeta^{is}.$$

Since the Vandermonde matrix $[\zeta^{ij}]_{1 \leqslant i,j \leqslant n}$ is invertible [19] (and therefore has linearly independent rows), this implies that $S = mS$. □

Lemma 5.4. *Assume* $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ *is a nontrivially unstable, circulant graph of even order, and there exists* $\alpha \in \mathrm{Aut}\, BX$*, such that* α *fixes the two cosets of* $2\mathbb{Z}_n \times \{0\}$ *that are in* $\mathbb{Z}_n \times \{0\}$*, but interchanges the two cosets that are in* $\mathbb{Z}_n \times \{1\}$*. If* X *does not have Wilson type* (C.1)*, then:*

(1) $n \equiv 2 \pmod 4$,

(2) $\langle S \cap 2\mathbb{Z}_n \rangle = 2\mathbb{Z}_n$*, and*

(3) $X \cong \mathrm{Cay}(\mathbb{Z}_n, S + (n/2))$ (*so Proposition* 3.7 *applies*).

Proof. Let

- $S_e = S \cap 2\mathbb{Z}_n$,
- $S_o = S \setminus S_e$,
- $G_e = 2\mathbb{Z}_n \times \mathbb{Z}_2$,
- $G_o = \langle 2\mathbb{Z}_n \times \{0\}, (1,1)\rangle = \langle (1,1)\rangle = \big(2\mathbb{Z}_n \times \{0\}\big) \cup \big((2\mathbb{Z}_n + 1) \times \{1\}\big)$,
- $X_o = \mathrm{Cay}(2\mathbb{Z}_n, S_o + \not{n})$,
- $B_e = BX_e = \mathrm{Cay}\big(G_e, S_e \times \{1\}\big)$ be the subgraph of BX induced by G_e,
- $B_o = \mathrm{Cay}\big(G_o, S_o \times \{1\}\big)$ be the subgraph of BX induced by G_o, and
- $\not{n} = n/2$ (see Notation 2.2).

By assumption,

$$\text{the restriction of } \alpha \text{ to } G_e \text{ is an isomorphism from } B_e \text{ to } B_o.$$

(1) [The proof of this part of the lemma does not require the assumption that X does not have Wilson type (C.1).] Suppose $n \not\equiv 2 \pmod 4$. Then $\gcd(1+\not{n}, n) = 1$. Therefore, since G_o is cyclic, and $\not{n}g = 0$ for all $g \in G_e$, we see from Lemma 5.3 that

$$S_o = (1 + \not{n})S_o = S_o + \not{n}.$$

This means that B_o has twins. More precisely, since $|\not{n}| = 2$, each equivalence class of vertices with the same neighbors has even cardinality. So the same must be true in the isomorphic graph B_e, which means there exists an element (h_1, h_2) of order 2 in G_e, such that

$$\big(S_e \times \{1\}\big) + (h_1, h_2) = S_e \times \{1\}.$$

Since the element of order 2 in the cyclic group $2\mathbb{Z}_n$ is unique (and the equation $1+h_2 = 1$ implies that $h_2 = 0$), we conclude that S_e is invariant under translation by $\not{n}$. We already know that the same is true for S_o, so we conclude that $S + \not{n} = S$. This contradicts the assumption that X is nontrivially unstable (and therefore twin-free).

(2) Since $n \equiv 2 \pmod 4$, we know that $\not{n}$ is odd. So $\mathbb{Z}_n = 2\mathbb{Z}_n \cup (2\mathbb{Z}_n + \not{n})$. For convenience, label the 4 cosets of $2\mathbb{Z}_n \times \{0\}$ by

$$C_e^i = 2\mathbb{Z}_n \times \{i\} \quad \text{and} \quad C_o^i = (2\mathbb{Z}_n + \not{n}) \times \{i\} \qquad \text{for } i \in \mathbb{Z}_2.$$

Then $G_e = C_e^0 \cup C_e^1$ and $G_o = C_e^0 \cup C_o^1$. By assumption, α fixes C_e^0 and C_o^0, but interchanges C_e^1 and C_o^1.

The function $\varphi(x, i) = (x + i\not{n}, i)$ is an isomorphism

$$\text{from } B_o = \mathrm{Cay}\big(G_o, S_o \times \{1\}\big) \text{ to } BX_o = \mathrm{Cay}\big(2\mathbb{Z}_n \times \mathbb{Z}_2, (S_o + \not{n}) \times \{1\}\big).$$

By composing φ with the restriction of α to G_e (that is, by restricting the map $\varphi\big(\alpha(x,i)\big)$ to G_e), we obtain an isomorphism from BX_e to BX_o. Since X does not have Wilson type (C.1), we know that X_e is twin-free (see Remark 2.6), so we see from Theorem 1.10 that each connected component of X_e is isomorphic to a connected component of X_o. Hence, these two connected components must have the same order, which means that the two subgroups $\langle S_e\rangle$ and $\langle S_o + \not{n}\rangle$ of $\mathbb{Z}_n$ have the same order, and are therefore equal. So

$$\langle S_e, \not{n}\rangle \supseteq \langle S_e \cup S_o\rangle = \langle S\rangle = \mathbb{Z}_n.$$

Hence, $\langle S_e\rangle$ is a subgroup of index $\leqslant 2$ in $\mathbb{Z}_n$, and must therefore be all of $2\mathbb{Z}_n$. This establishes (2).

(3) Let us begin by making a part of the above proof of (2) more concrete. It was established there that composing φ with the restriction of α to G_e is an isomorphism from BX_e to BX_o. Since X_e is twin-free, we therefore see from Corollary 4.8 that there is an isomorphism $\alpha_0\colon X_e \to X_o$, such that

$$\alpha(x,1) = \big(\alpha_0(x) + \not{n}, 1\big) \text{ for } x \in 2\mathbb{Z}_n.$$

Similarly, if we let $\varphi'(x,i) = \big(x + (1-i)\not{n}, i\big)$, then restricting the map $\alpha\big(\varphi'(x,i)\big) - (\not{n}, 0)$ to G_e yields an isomorphism from BX_o to BX_e. So there is an isomorphism $\alpha_1\colon X_o \to X_e$, such that

$$\alpha(x,1) = \big(\alpha_1(x) + \not{n}, 1\big) \text{ for } x \in 2\mathbb{Z}_n.$$

By comparing the two formulas for $\alpha(x,1)$, we see that $\alpha_0 = \alpha_1$.

Now, define $\alpha'\colon \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$\alpha'(x) = \begin{cases} \alpha_0(x) & \text{if } x \in 2\mathbb{Z}_n, \\ \alpha_0(x + \not{n}) + \not{n} & \text{if } x \notin 2\mathbb{Z}_n. \end{cases}$$

Since $S = S_e \cup S_o$ (and therefore $S + \not{n} = (S_o + \not{n}) \cup (S_e + \not{n})$), it will suffice to show that

$$\alpha' \text{ is an isomorphism from } \mathrm{Cay}(\mathbb{Z}_n, S_e) \text{ to } \mathrm{Cay}(\mathbb{Z}_n, S_o + \not{n})$$

and

$$\alpha' \text{ is an isomorphism from } \mathrm{Cay}(\mathbb{Z}_n, S_o) \text{ to } \mathrm{Cay}(\mathbb{Z}_n, S_e + \not{n}).$$

The first is easy to see from the definition of α', because

$$\alpha_0 \text{ is an isomorphism from } X_e = \mathrm{Cay}(2\mathbb{Z}_n, S_e) \text{ to } X_o = \mathrm{Cay}(2\mathbb{Z}_n, S_o + \not{n}).$$

To establish the second, let $s \in S_o$. If $x \in 2\mathbb{Z}_n$, then

$$\begin{aligned} \alpha'(x+s) &= \alpha_0\big((x+s) + \not{n}\big) + \not{n} && \text{(definition of } \alpha', \text{ since } x+s \notin 2\mathbb{Z}_n) \\ &\in \alpha_0(x) + S_e + \not{n} && \begin{pmatrix}\alpha_0 = \alpha_1 \text{ is an isomorphism} \\ \text{from } X_o \text{ to } X_e\end{pmatrix} \\ &= \alpha'(x) + (S_e + \not{n}). && \text{(definition of } \alpha', \text{ since } x \in 2\mathbb{Z}_n) \end{aligned}$$

Similarly, if $x \notin 2\mathbb{Z}_n$, then

$$\begin{aligned}
\alpha'(x+s) &= \alpha_0(x+s) && \begin{pmatrix}\text{definition of } \alpha',\\ \text{since } x+s \in 2\mathbb{Z}_n\end{pmatrix}\\
&= \alpha_0\big((x+\not{n})+(s+\not{n})\big) && (\not{n}+\not{n}=0)\\
&\in \alpha_0(x+\not{n})+S_e && \begin{pmatrix}\alpha_0=\alpha_1 \text{ is an isomorphism}\\ \text{from } X_o \text{ to } X_e\end{pmatrix}\\
&= \big(\alpha_0(x+\not{n})+\not{n}\big)+\big(S_e+\not{n}\big) && (\not{n}+\not{n}=0)\\
&= \alpha'(x)+\big(S_e+\not{n}\big). && \begin{pmatrix}\text{definition of } \alpha',\\ \text{since } x \notin 2\mathbb{Z}_n\end{pmatrix}
\end{aligned}$$

Since $\alpha'(x+s) \in \alpha'(x)+(S_e+\not{n})$ in both cases, we conclude that α' is an isomorphism from $\mathrm{Cay}(\mathbb{Z}_n, S_o)$ to $\mathrm{Cay}(\mathbb{Z}_n, S_e+\not{n})$, as desired. This completes the proof of (3). □

The following result gathers the most important conclusions of Lemmas 5.2 and 5.4.

Corollary 5.5. *Let $X = \mathrm{Cay}(\mathbb{Z}_n, S)$ be a nontrivially unstable, circulant graph, such that $n \equiv 2 \pmod 4$, and such that $2\mathbb{Z}_n \times \{0\}$ is a block for the action of $\mathrm{Aut}\, BX$. Then either X has Wilson type* (C.1)*, or X is isomorphic to $\mathrm{Cay}\big(\mathbb{Z}_n, S+(n/2)\big)$ (so Proposition* 3.7 *applies).*

Proof. Since X is unstable, there exists $\alpha \in \mathrm{Aut}\, BX$, such that $\alpha \notin \mathrm{Aut}\, X \times S_2$. By composing with a translation, we may assume that α fixes $(0,0)$. Since $2\mathbb{Z}_n \times \{0\}$ is a block for the action of $\mathrm{Aut}\, BX$, this implies that α fixes $2\mathbb{Z}_n \times \{0\}$. It must also fix the bipartition set $\mathbb{Z}_n \times \{0\}$, so it fixes the difference

$$\big(\mathbb{Z}_n \times \{0\}\big) \setminus \big(2\mathbb{Z}_n \times \{0\}\big) = (2\mathbb{Z}_n + 1) \times \{0\}.$$

And then α either fixes the two remaining cosets, or interchanges them. In the first case, Lemma 5.2 tells us that X has Wilson type (C.1). In the second case, Lemma 5.4(3) provides the desired conclusion. □

The following result presents some useful special cases. Recall that the "Cayley Isomorphism Property" was defined in Definition 2.8.

Corollary 5.6. *Assume X is as in Corollary* 5.5*. Also assume that either*

(1) *X has the Cayley Isomorphism Property, or*

(2) *X_e has the Cayley Isomorphism Property, or*

(3) *n is square-free, or*

(4) *the valency of X_e is $\leqslant 5$.*

Then X has Wilson type (C.1) *or* (C.4)*.*

Proof. Assume X does not have Wilson type (C.1). Then Corollary 5.5 tells us that $X \cong \mathrm{Cay}(\mathbb{Z}_n, S + \not{n})$.

(1) If X has the Cayley Isomorphism Property, this implies there is some $m \in \mathbb{Z}_n^\times$, such that $S + \not{n} = mS$, so X has Wilson type (C.4).

(2) Assume that X_e has the Cayley Isomorphism Property. Let α_0 and α_1 be the isomorphisms in the proof of Lemma 5.4(3). Since X_e has the Cayley Isomorphism Property, we have $\alpha_0(x) = m\,\varphi(x)$, for some $m \in \mathbb{Z}_n^\times$, and some $\varphi \in \mathrm{Aut}\, X_e$. Then

$$\begin{aligned} mS_e &= m\big(\varphi(S_e) - \varphi(0)\big) && (\varphi \in \mathrm{Aut}\, X_e) \\ &= \alpha_0(S_e) - \alpha_0(0) && (\alpha_0(x) = m\,\varphi(x)) \\ &= S_o + \not{n} && (\alpha_0 \colon X_e \xrightarrow{\cong} X_o). \end{aligned}$$

Now, since $\varphi \in \mathrm{Aut}\, X_e = \mathrm{Aut}\,\mathrm{Cay}(2\mathbb{Z}_n, S_e)$ and $m \in \mathbb{Z}_n^\times$, Corollary 4.4 implies

$$\varphi \in \mathrm{Aut}\,\mathrm{Cay}(2\mathbb{Z}_n, mS_e) = \mathrm{Aut}\,\mathrm{Cay}(2\mathbb{Z}_n, S_o + \not{n}) = \mathrm{Aut}\, X_o.$$

Therefore

$$\begin{aligned} m(S_o + \not{n}) &= m\big(\varphi(S_o + \not{n}) - \varphi(0)\big) && (\varphi \in \mathrm{Aut}\, X_o) \\ &= \alpha_0(S_o + \not{n}) - \alpha_0(0) && (\alpha_0(x) = m\,\varphi(x)) \\ &= S_e, && \begin{pmatrix} \alpha_0 = \alpha_1 \text{ is an isomorphism} \\ \text{from } X_o \text{ to } X_e \end{pmatrix} \end{aligned}$$

so $mS_o = S_e + \not{n}$. Therefore

$$mS = m(S_e \cup S_o) = mS_e \cup mS_o = (S_o + \not{n}) \cup (S_e + \not{n}) = S + \not{n}.$$

So X has Wilson type (C.4).

(3) The order of X is square-free, so Theorem 2.9 tells us that X has the Cayley Isomorphism Property. Therefore (1) applies.

(4) It is known [10, §7.2] that every connected, circulant graph of valency $\leqslant 5$ has the Cayley Isomorphism Property. (A proof for valency 4 can also be found in [15, Thm. 5.4].) Therefore (2) applies. □

Proof of Theorem 5.1. Let $X = \mathrm{Cay}(\mathbb{Z}_{2p}, S)$ be a nontrivially unstable, circulant graph of order $n = 2p$. It is easy to see, by inspection, that there are no nontrivially unstable, circulant graphs of order 4, so p is odd. Therefore $n = 2p$ is square-free.

Let

$$S' = S \setminus (S + p).$$

Since X is twin-free, we know that $S + p \neq S$ (see Remark 2.6), which means that $2S'$ is nonempty.

Case 1. *Assume* $2S' \neq \{0\}$. Since $2\mathbb{Z}_{2p}$ has order p, which is prime, every nonzero element is a generator. So $2S'$ generates $2\mathbb{Z}_{2p}$. We also know from Corollary 4.3 that every automorphism of BX is an automorphism of

$$\mathrm{Cay}\big(\mathbb{Z}_{2p} \times \mathbb{Z}_2, 2S' \times \{0\}\big).$$

By combining these two facts, we conclude that $2\mathbb{Z}_{2p} \times \{0\}$ is a block for the action of $\operatorname{Aut} BX$.

Therefore, Corollary 5.6(3) applies, so X has Wilson type (C.1) or (C.4). However, $2\mathbb{Z}_{2p} \cong \mathbb{Z}_p$ has no nontrivial, proper subgroups, so it is obvious that X does not have Wilson type (C.1). Therefore, it must have Wilson type (C.4), which is exactly what we needed to prove.

Case 2. *Assume* $2S' = \{0\}$. This means that $S' = \{p\}$, so $p \in S$.

Since X is unstable, we may let α be an automorphism of BX, such that $\alpha(0,1) = (t,1)$ with $t \neq 0$. For all $x \in \mathbb{Z}_n$, we see from Corollary 4.7 that if $|x| = |t|$, then $x \notin S$. Since $p \in S$, this tell us that $|t| \neq 2$. So $|t|$ is either p or $2p$. Therefore, either S does not contain any element of order p, or S does not contain any element of order $2p$. However, since $2S' = \{0\}$, we also know that $s + p \in S$ for all $s \in S \setminus \{p\}$. Also note that

$$|s| = p \iff |s + p| = 2p.$$

Putting this together, we conclude that $S = \{p\}$. This contradicts the fact that the nontrivially unstable graph X must be connected. □

Corollary 5.7. *Let* $X = \operatorname{Cay}(\mathbb{Z}_{2p}, S)$ *be a circulant graph of order* $2p$*, where* p *is an odd prime, and let* $S_e = S \cap 2\mathbb{Z}_{2p}$*. The graph* X *is unstable if and only if either it is trivially unstable, or there exists* $m \in \mathbb{Z}_{2p}^{\times}$*, such that* $m^2 S_e = S_e$*,* $mS_e \neq S_e$*, and* $S = S_e \cup \big((n/2) + mS_e\big)$*.*

Proof. ($\Leftarrow$) If X is not trivially unstable, then the conditions imply that X has Wilson type (C.4).

($\Rightarrow$) Assume X is nontrivially unstable. We conclude from Theorem 5.1 that X has Wilson type (C.4), so there is some $m \in \mathbb{Z}_{2p}$, such that $S = mS + p$. Since p is odd, this implies that $S_o = mS_e + p$ (where $S_o = S \setminus S_e$) and

$$S_e = mS_o + p = m(mS_e + p) = m^2 S_e.$$

If $mS_e = S_e$, then $S_o = S_e + p$, so $S = S + p$, which contradicts the fact that nontrivially unstable graphs are twin-free. □

Corollary 5.8. *For* $n \in \mathbb{Z}^+$*, there does* ***not*** *exist a nontrivially unstable circulant graph of order* n *if and only if either* n *is odd, or* $n < 8$*, or* $n = 2p$*, for some prime number* $p \equiv 3 \pmod 4$*.*

Proof. ($\Rightarrow$) If $\not{n}$ is not prime, then $2\mathbb{Z}_n \cong \mathbb{Z}_{n/2}$ has a nontrivial, proper subgroup A. Choose some $b \in 2\mathbb{Z}_n \setminus A$, and let $S = \{\pm 1\} \cup (\pm b + A)$, so $S_e := S \cap 2\mathbb{Z}_n = \pm b + A$. Then $X = \operatorname{Cay}(\mathbb{Z}_n, S)$ has Wilson type (C.1), so it is unstable.

If $\not{n}$ is prime, and $\not{n} \not\equiv 3 \pmod 4$ (and $n \geqslant 8$), then $\not{n} \equiv 1 \pmod 4$, so there exists $m \in \mathbb{Z}_n^{\times}$, such that $m^2 = -1$. Let $S = \{\pm 1, \not{n} \pm m\}$, so $S_e := S \cap 2\mathbb{Z}_n = \{\pm m + \not{n}\}$ and $S = mS + \not{n}$. Then $X = \operatorname{Cay}(\mathbb{Z}_n, S)$ has Wilson type (C.4), so it is unstable.

In either case, X is also connected (because $1 \in S$) and nonbipartite (because $S_e \neq \varnothing$). Hence, if X is not nontrivially unstable, then it must not be twin-free, so there is a nonzero

$h \in \mathbb{Z}_n$, such that $h + S = S$. Note that in both cases, $S_o = \{\pm 1\}$ and since $n > 4$ and h is nonzero, it cannot happen that $\{\pm 1\} + h = \{\pm 1\}$. It follows that $S_o + h = S_e$ and $S_e + h = S_o$ (and h is odd).

Since $S_o + 2h = S_o$ (and $S_0 = \{\pm 1\}$), we must have $2h = 0$, which means $h = \not{n}$, so $S_e = S_o + \not{n} = \{\not{n} \pm 1\}$.

If $\not{n}$ is not prime, then, since $\{\not{n} \pm 1\} = S_e = \pm b + A$, we must have $\langle 2 \rangle \subseteq A$. Since $n > 4$, this implies $|b + A| = |A| \geqslant n/2 > 2$, which is a contradiction.

If $\not{n}$ is prime, we must have $m = \pm 1$ (since $S_e = \{\not{n} \pm m\}$, which contradicts the fact that $m^2 = -1$.

($\Leftarrow$) We prove the contrapositive: supposing there does exist a nontrivially unstable circulant graph of order n, we will show that n is odd, that $n \geqslant 8$, and that $n/2$ is *not* a prime number that is congruent to 3 (mod 4).

The fact that n is odd is immediate from Theorem 1.10. Also, it is easy to see, by inspection, that there are no nontrivially unstable circulant graphs of order 2 or 4; so $n \geqslant 6$.

Now suppose $X = \mathrm{Cay}(\mathbb{Z}_{2p}, S)$ is a nontrivially unstable circulant graph of order $2p$, where p is prime, and $p \equiv 3 \pmod 4$. (This includes the case where $n = 6$.) We will show that this leads to a contradiction. By Theorem 5.1, we know that X has Wilson type (C.4), so there is some $m \in \mathbb{Z}_{2p}^\times$, such that $S = mS + \not{n}$. Write $m = m_o m_2$, where m_o has odd order (as an element of the group $\mathbb{Z}_{2p}^\times$), and the order of m_2 is a power of 2. Since $\mathbb{Z}_{2p}^\times$ is cyclic of order $p - 1 \equiv 2 \pmod 4$, there are no elements of order 4 in $\mathbb{Z}_{2p}^\times$, so $m_2 \in \{\pm 1\}$. Since $S = -S$, this implies $S = m_2 S$, so we conclude that $S = m_o S + \not{n}$. After repeatedly multiplying both sides of this equation by m_o, we see that $S = m_o^k S + \not{n}$ for any odd number k, including $k = |m_o|$. Hence, we have $S = S + \not{n}$. This contradicts the fact that X is twin-free. □

6 Computational results

S. Wilson [20, p. 377] mentioned: "There are 3274 circulant graphs which are non-trivially unstable and have no more than 38 vertices." However, we performed computations that produce a different number: there seem to be 3576 such graphs (up to isomorphism). The interested reader can reproduce our results in only a few minutes by running the Sagemath[1] code or Magma code or Maple code that is available online at https://arxiv.org/src/2108.05893/anc/.

Analysis of these graphs establishes:

Observation 6.1. Every nontrivially unstable circulant graph of order less than 40 has a Wilson type, *except* the following six graphs (up to isomorphism), all of order 24:

(1) $\mathrm{Cay}(\mathbb{Z}_{24}, \{\pm 2, \pm 3, \pm 8, \pm 9, \pm 10\})$,

(2) $\mathrm{Cay}(\mathbb{Z}_{24}, \{\pm 2, \pm 3, \pm 8, \pm 9, \pm 10, 12\})$,

[1]Sagemath code can be run online at https://cocalc.com/

(3) $\mathrm{Cay}(\mathbb{Z}_{24}, \{\pm1, \pm2, \pm5, \pm7, \pm8, \pm10, \pm11\})$,

(4) $\mathrm{Cay}(\mathbb{Z}_{24}, \{\pm1, \pm2, \pm5, \pm7, \pm8, \pm10, \pm11, 12\})$,

(5) $\mathrm{Cay}(\mathbb{Z}_{24}, \{\pm1, \pm2, \pm3, \pm5, \pm7, \pm8, \pm9, \pm10, \pm11\})$,

(6) $\mathrm{Cay}(\mathbb{Z}_{24}, \{\pm1, \pm2, \pm3, \pm5, \pm7, \pm8, \pm9, \pm10, \pm11, 12\})$.

The first of these graphs appears explicitly in [16, p. 156], and it seems that some (or all) of the others were also known to the authors of that paper.

Remark 6.2. Several additional days of computer time extended the exhaustive calculations to order 50. (However, these calculations are certainly not definitive, because they were performed only once, so their correctness has not been verified.) Lists of the additional 67725 nontrivially unstable graphs have been archived at https://arxiv.org/src/2108.05893/anc/.

We note that the instability of every example that was found is explained by the instability conditions in Section 3. On the other hand, the calculations uncovered 316 additional examples of nontrivially unstable circulant graphs with no Wilson type: 52 of order 40, 262 of order 48, and 2 of order 50.

Acknowledgements

The work of Ademir Hujdurović is supported in part by the Slovenian Research Agency (research program P1-0404 and research projects N1-0102, N1-0140, N1-0159, N1-0208, J1-1691, J1-1694, J1-1695, J1-2451 and J1-9110).

References

[1] L. Babai. Spectra of Cayley graphs. *J. Combin. Theory, Ser. B,* 27 (1979), no. 2, 180–189. MR 0546860, https://doi.org/10.1016/0095-8956(79)90079-0

[2] N. Biggs. *Algebraic Graph Theory*. Cambridge University Press, London, 1974. MR 0347649, https://doi.org/10.1017/CBO9780511608704

[3] J. D. Dixon and B. Mortimer. *Permutation Groups*. Springer, New York, 1996. MR 1409812, https://doi.org/doi:10.1007/978-1-4612-0731-3

[4] B. Fernandez and A. Hujdurović. Canonical double covers of circulants (preprint, 2020). arXiv:2006.12826

[5] C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer, New York, 2001. MR 1829620, https://doi.org/10.1007/978-1-4613-0163-9

[6] A. Hujdurović, Đ. Mitrović, and D. W. Morris. Automorphisms of the double cover of a circulant graph of valency at most 7 (preprint, 2021). arXiv:2108.05164

[7] A. Kotlov and L. Lovász. The rank and size of graphs. *J. Graph Theory* 23 (1996), no. 2, 185–189. MR 1408346, https://doi.org/10.1002/(SICI)1097-0118(199610)23:2<185::AID-JGT9>3.0.CO;2-P

[8] S. Lang. *Algebra.* Springer-Verlag, New York, 2002. MR 1878556, https://doi.org/10.1007/978-1-4613-0041-0

[9] J. Lauri, R. Mizzi, R. Scapellato. Unstable graphs: a fresh outlook via TF-automorphisms. *Ars Math. Contemp.* 8 (2015), no. 1, 115–131. MR 3281124, https://doi.org/10.26493/1855-3974.534.934

[10] C. H. Li. On isomorphisms of finite Cayley graphs—a survey. *Discrete Math.* 256 (2002), no. 1-2, 301–334. MR 1927074, https://doi.org/10.1016/S0012-365X(01)00438-1

[11] D. Marušič, R. Scapellato, and N. Zagaglia Salvi. A characterization of particular symmetric (0,1) matrices. *Linear Algebra Appl.* 119 (1989), 153–162. MR 1005241, https://doi.org/10.1016/0024-3795(89)90075-X

[12] D. W. Morris. On automorphisms of direct products of Cayley graphs on abelian groups. *Electronic J. Combin.* 28(3) (2021), #P3.5. https://doi.org/10.37236/9940

[13] M. Muzychuk. On Ádám's conjecture for circulant graphs (corrigendum). *Discrete Math.* 176 (1997), no. 1-3, 285–298. MR 1477298, https://doi.org/10.1016/S0012-365X(97)81804-3

[14] M. Muzychuk. A solution of the isomorphism problem for circulant graphs. *Proc. London Math. Soc.* (3) 88 (2004), no. 1, 1–41. MR 2018956, https://doi.org/10.1112/S0024611503014412

[15] M. Muzychuk, M. Klin, and R. Pöschel. The isomorphism problem for circulant graphs via Schur ring theory, in: A. Barg and S. Litsyn, eds., *Codes and Association Schemes (Piscataway, NJ, 1999)*, pp. 241–264. Amer. Math. Soc., Providence, RI, 2001. MR 1816402, https://doi.org/10.1090/dimacs/056

[16] Y.-L. Qin, B. Xia, and S. Zhou. Stability of circulant graphs, *J. Combin. Theory, Ser. B,* 136 (2019) 154–169. MR 3926283, https://doi.org/10.1016/j.jctb.2018.10.004

[17] H. Wielandt. *Finite Permutation Groups.* Academic Press, New York, 1964. MR 0183775, https://doi.org/10.1016/C2013-0-11702-3

[18] Wikipedia. Bipartite double cover. https://en.wikipedia.org/wiki/Bipartite_double_cover

[19] Wikipedia. Vandermonde matrix. https://en.wikipedia.org/wiki/Vandermonde_matrix

[20] S. Wilson. Unexpected symmetries in unstable graphs. *J. Combin. Theory, Ser. B,* 98 (2008), no. 2, 359–383. MR 2389604, https://doi.org/10.1016/j.jctb.2007.08.001