Self-complementary circulant graphs

Brian Alspach* and Joy Morris
Department of Mathematics and Statistics
Burnaby, British Columbia
Canada V5A 1S6

V. Vilfred
Department of Mathematics
St. Jude's College
Thoothoor
India 629 176

1 Introduction

All graphs in this paper have neither loops nor multiple edges. We use $V(X)$ and $E(X)$ to denote the vertex set and edge set of X, respectively. Given a graph X, the complement of X, denoted X^c, satisfies u is adjacent to v in X if and only if u is not adjacent to v in X^c.

1.1 Definition. A graph X is said to be *self-complementary* if it is isomorphic to its complement.

The following proposition is simple to prove so we omit its proof.

1.2 Proposition. *Whenever X is a self-complementary regular graph, we have $|V(X)| \equiv 1 (\mathrm{mod}\ 4)$.*

1.3 Definition. Let $S \subseteq \{1, 2, \ldots, n-1\}$ such that $i \in S$ if and only if $n-i \in S$. The *circulant* graph $X = X(n; S)$ of order n is the graph whose vertex set is $\{u_0, u_1, \ldots, u_{n-1}\}$ with an edge joining u_i and u_j if and only if $j - i \in S$, where the latter computation is done modulo n. The set S is called the *symbol* of the circulant.

*This research was partially supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-4792

H. Sachs [2] showed how to construct self-complementary circulant graphs of order n whenever n is a product of primes all of which are congruent to 1 modulo 4. He further wrote that there are reasons to conjecture that it is necessary that all the primes in the prime factorization of n be congruent to 1 modulo 4. He supported this statement by demonstrating the non-existence of self-complementary circulant graphs of orders $n = p^{2e}$, $n = pq$ and $n = 9r$, where p and q are any primes congruent to 3 modulo 4, and $r > 5$ is a prime congruent to 1 modulo 4.

D. Fronček, A. Rosa and J. Širan [1] have proved that his conjecture is true, that is, they showed that there exists a self-complementary circulant graph of order n if and only if every prime in the prime factorization of n is congruent to 1 modulo 4. Their proof is graph theoretic. In this paper, we provide a simple algebraic proof. First, some preliminary results about permutation groups are required.

1.4 Definition. A permutation group G acting on a set Ω is said to be *transitive* if for any $\alpha, \beta \in \Omega$, there is some $g \in G$ such that $g(\alpha) = \beta$. Furthermore, if for any ordered pairs (α, β) and (δ, γ), there is some $g \in G$ such that $g(\alpha) = \delta$ and $g(\beta) = \gamma$, then G is said to be *doubly transitive.*

1.5 Definition. Let G be a permutation group acting on Ω. If $B \subseteq \Omega$ has the property that for every $g \in G$, either $g(B) = B$ or $g(B) \cap B = \emptyset$, then B is called a *block* of G.

It is easy to see that Ω, $\emptyset$, and any singleton are blocks of any permutation group. They are called trivial blocks for this reason. All other blocks are called non-trivial.

1.6 Definition. Let G be a transitive permutation group. If G has any non-trivial blocks, then G is said to be an *imprimitive* group. Otherwise, G is said to be *primitive.*

Note that if G is imprimitive, then given a non-trivial block B, there is a partition of Ω obtained by taking B and all its images under the action of G. This is called a *complete block system* and all the blocks have the same cardinality; the latter is frequently called the *length* of a block.

1.7 Definition. Let G be an abstract finite group. If every primitive group containing the regular representation of G as a transitive subgroup is doubly transitive, then G is said to be a *Burnside* group.

Burnside groups are nice groups for graph theory. Why? If we form any Cayley graph on a Burnside group G, then the regular representation of G is contained in the automorphism group of the graph as a transitive subgroup. Hence, if the Cayley graph is neither complete nor the complement of the complete graph, then the automorphism group must act imprimitively on the vertex set of the graph.

This is especially nice for circulant graphs because of the following result telling us precisely what the blocks are.

1.8 Lemma. *If n is not prime and the automorphism group $\mathrm{Aut}(X)$ of a circulant graph X of order n acts imprimitively on the vertex set of X with blocks of length d, then d is a divisor of n and the blocks are the sets $B_k = \{u_i : i \equiv k (\mathrm{mod}\ n/d)\}$, $k = 0, 1, \ldots, \frac{n}{d} - 1$.*

PROOF. Let B be a block of length d. Taking all the blocks belonging to the complete block system containing B, we see that this partitions the vertex set into parts all of which have d elements. Thus, d is a divisor of n.

We know that the permutation $\rho = (u_0\ u_1\ \cdots\ u_{n-1}) \in \mathrm{Aut}(X)$. By the definition of blocks and from the action of ρ, it is easy to see that each block must be made up of vertices equally spaced n/d apart in the order in which they occur in ρ. This completes the proof. ■

The following two known results are required later. The simple proof of the second is omitted.

1.9 Theorem ([3]). *The cyclic groups of composite order all are Burnside groups.*

1.10 Proposition. *Let G be an imprimitive group with blocks $B_1, \ldots, B_k$ and let $\overline{G}$ denote the action of G on the set of blocks. If $\overline{G}$ is itself imprimitive with blocks $C_1, C_2, \ldots, C_t$, then G is imprimitive with blocks $B'_1, B'_2, \ldots, B'_t$, where B'_i is the union of the blocks comprising C_i.*

2 Main Result

We are now ready to prove the main result whose statement follows.

2.1 Theorem. *There exists a self-complementary circulant graph with n vertices if and only if every prime p in the prime factorization of n satisfies $p \equiv 1(\mathrm{mod}\ 4)$.*

PROOF. For the sake of completeness and because of its brevity, we give a proof of the sufficiency in spite of the fact Sachs [2] also did it. When $p \equiv 1(\mathrm{mod}\ 4)$, it is easy to see that the circulant graph $X(p; S)$, where S is the set of quadratic residues modulo p, is self-complementary. If X is a self-complementary circulant graph of order m, then the wreath product $X(p; S) \wr X$ is easily seen to be self-complementary of order pm. Thus, there is a self-complementary circulant graph of order n whenever all the primes in the prime factorization of n are congruent to 1 modulo 4.

We prove necessity by induction on n. Let X be a self-complementary circulant graph of smallest order which is a counter-example. We know that $n \equiv 1(\mathrm{mod}\ 4)$ is satisfied. Hence, n is composite and has $2r$, $r > 0$, primes congruent to 3 modulo 4 in its prime factorization.

Since n is composite and X is self-complementary, $X \neq K_n$ and $X \neq K_n^c$ implying that $\mathrm{Aut}(X)$ is imprimitive by Theorem 1.9. Suppose the blocks have length d and $\rho = (u_0\ u_1\ \cdots\ u_{n-1})$. By Lemma 1.8 we know that the blocks have the form $B_i = \{u_j : j \equiv i \ (\mathrm{mod\ n/d})\}$, $i = 0, 1, \ldots, n/d - 1$. Since X^c has the same automorphism group as X, $B_0, B_1, \ldots, B_{n/d-1}$ are also the blocks of length d for the group acting on $V(X^c)$. Thus, any isomorphism of X to X^c must act as a permutation on the set of blocks. The action of ρ tells us that the subgraphs $X_0, X_1, \ldots, X_{n/d-1}$ induced by X on $B_0, B_1, \ldots, B_{n/d-1}$, respectively, are all isomorphic to each other. Further, the action of $\rho^{n/d-1}$ implies that $X_0, X_1, \ldots, X_{n/d-1}$ are all circulant graphs. We conclude that X_0 itself is a self-complementary circulant graph.

The permutation ρ cyclically permutes the blocks so that the action of $\overline{\mathrm{Aut}(X)}$ on the blocks contains the regular representation of the cyclic group of order n/d. If $\overline{\mathrm{Aut}(X)}$ is imprimitive, then we can find a block system for $\mathrm{Aut}(X)$ acting on $V(X)$ with blocks of length d', where $d' > d$, by Proposition 1.10. Without loss of generality, we may assume that $B_0, B_1, \ldots, B_{n/d-1}$ are maximal non-trivial blocks of $\mathrm{Aut}(X)$, that is, the only block properly containing B_0 is all of $V(X)$.

Since X is a minimal counter-example, the self-complementary circulant subgraph X_0 cannot be a counter-example. Thus, the prime factorization of d has no primes congruent to 3 modulo 4. However, n has at least two primes congruent to 3 modulo 4 in its prime factorization. Thus, n/d is composite and $\overline{\mathrm{Aut}(X)}$ is either doubly transitive or imprimitive. It cannot be imprimitive as this would allow us to find a non-trivial block properly containing B_0. Hence, $\overline{\mathrm{Aut}(X)}$ acts doubly transitively on the set of blocks. This implies that the number of edges between any two blocks is the same. However, there are d^2 possible edges between any two blocks which is odd because d is odd. This means that the parities of the numbers of edges between any two blocks in X and X^c are different. Thus, X cannot be self-complementary. The necessity now follows. ■

3 Concluding Remarks

There is some hint that 2 may be special with respect to the partition result proved above. Namely, if 2 divides the number of edges of K_n and the valence is even, that is, $n \equiv 1 (\mathrm{mod}\ 4)$, there is a partition of the edge set of K_n into two isomorphic circulants if and only if all primes dividing n are congruent to 1 modulo 4.

Is there some extension of the result to other $k > 2$. If $k > 2$, it is easy to construct partitions of the edge set of K_n into k isomorphic circulant graphs if every prime dividing n is congruent to 1 modulo $2k$. However, this condition is no longer necessary. For example, the edges of K_{15} can be partitioned into seven Hamilton cycles. They are certainly circulant graphs, but 15 is not a product of primes congruent to 1 modulo 14.

This suggests an obvious question. One also may want to require that the circulant subgraphs span K_n.

References

[1] D. Fronček, A. Rosa and J. Širan, The existence of selfcomplementary circulant graphs, *Europ. J. Combin.*, to appear.

[2] H. Sachs, Über selbstkomplementäre Graphen, *Publ. Math. Debrecen* **9** (1962), 270–288.

[3] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.