ON THE CLASSIFICATION OF SYMMETRIC GRAPHS
WITH A PRIME NUMBER OF VERTICES

BY

CHONG-YUN CHAO

Abstract. We determine all the symmetric graphs with a prime number of vertices. We also determine the structure of their groups.

1. Introduction. A symmetric graph is an undirected graph whose group of automorphisms is transitive on its vertices as well as on its edges. Here, we determine all the symmetric graphs with a prime number \( p \) of vertices, i.e., we show that besides the null and complete graphs, for each integer \( n \) such that \( 0 < n < p - 1 \), there exists a symmetric graph with \( p \) vertices and degree \( n \) if and only if \( n \) is even and \( n \) divides \( p - 1 \). Also, if the symmetric graphs with \( p \) vertices and degree \( n \) exist, they all are isomorphic. For each given \( p \), we can construct all the symmetric graphs with \( p \) vertices. The method of construction which we use here is similar to the one in [2], i.e., we use the properties of a Cayley graph of a cyclic group of order \( p \). Our classification depends heavily on a result in [1, Theorem 5, p. 494], i.e., the group of automorphisms of a symmetric graph (nonnull and noncomplete) with \( p \) vertices is a Frobenius group. In fact, here we can determine the generators and the defining relations of this Frobenius group. Our classification also confirms a conjecture in [4, p. 144].

2. Definitions and notations. The definitions concerning groups used here are the same as in [3]. Since the definitions concerning graphs are less standard, we state them as follows: The graphs which we consider here are finite, simple, loopless and undirected, i.e., by a graph \( X \) we mean a finite set \( V(X) \), called the vertices of \( X \), together with a set \( E(X) \), called the edges of \( X \), consisting of unordered pairs \([a, b]\) of distinct elements \( a, b \in V(X) \). We also assume that there is at most one edge between two vertices. Two graphs \( X \) and \( Y \) are said to be isomorphic, denoted by \( X \cong Y \), if there is a one-to-one map \( \sigma \) of \( V(X) \) onto \( V(Y) \) such that \([a_0, b_0] \in E(Y) \) if and only if \([a, b] \in E(X) \). An isomorphism of \( X \) onto itself is said to be an automorphism of \( X \). For each given graph \( X \) there is a group of all automorphisms, denoted by \( G(X) \), where the multiplication is the multiplication of permutations. \( X \) is said to be vertex-transitive if \( G(X) \) is transitive on \( V(X) \). \( X \) is said to be edge-transitive if \( G(X) \) is transitive on \( E(X) \). \( X \) is said to be symmetric...
if it is both vertex-transitive and edge-transitive. The complete graph (consisting of all possible edges) and the null graph (having \( E(X) \) empty) of \( n \) vertices have \( S_n \), the symmetric group of \( n \) letters, as their group of automorphisms. Since \( S_n, n > 1 \), is doubly transitive, the null graph and the complete graph are symmetric. A symmetric graph is said to be nontrivial if it is neither null nor complete. (When we are only interested in vertex-transitive graphs, it makes no difference whether the graphs are loopless or not.) Let \( H \) be an additive abstract finite group and \( K \) be a subset of \( H \) such that \( K \) does not contain the identity of \( H \). The Cayley graph of \( H \) with respect to \( K \) is \( X_{H,K} \) with \( V(X_{H,K}) = H \) and \( E(X_{H,K}) = \{ [h, h+k]; h \in H, k \in K \} \). If \( K \) is the empty set, then \( E(X_{H,K}) \) is meant to be empty, i.e., \( X_{H,K} \) is a null graph. Clearly, the left regular representations of \( H \) are contained in \( G(X_{H,K}) \) for any subset \( K \) (not containing the identity of \( H \)) in \( H \). A graph \( X \) is said to be regular if the number of edges incident with each vertex is the same, or \( X \) is said to be to be of degree \( m \) if the number of edges incident with each vertex is \( m \). The Cayley graphs are regular. A cycle of length \( n \) (\( > 2 \)) is a collection of \( n \) edges \( [X_1, X_2], [X_2, X_3], \ldots, [X_n, X_1] \) where \( X_1, X_2, \ldots, X_n \) are distinct. We, sometimes, indicate a cycle of length \( n \) by \( X_1-X_2-X_3-\cdots-X_n-X_1 \). In [1, p. 493] Theorem 4 states the following:

Let \( p \) be a prime, and \( G \) be the cyclic group generated by \((12\ldots p)\). Then Schur’s algorithm on \( G \) gives all the graphs of \( p \) vertices each whose group of automorphisms is transitive.

This theorem implies that if \( X \) is a vertex-transitive graph with \( p \) vertices, then \( X \) is a regular graph with cycles of length \( p \) combined together. This is due to the fact that when each basis for the centralizer ring \( V(G) \) corresponding to \( G \) is a symmetric matrix, it is the adjacency matrix of a cycle of length \( p \). (See pp. 492–493 in [1].) Let \( D_p \) be the dihedral group of order \( 2p \) generated by

\[
R = (012\ldots(p-1)) \quad \text{and} \quad D = (0)(1-1)(2-2)\ldots((p-1)/2-0-1)/2-(p-1)/2
\]

where the negative signs are taken modulo \( p \). Then Schur’s algorithm on \( G \) generated by \( R \) and on \( D_p \) give the same graphs. Hence, we have

**Proposition 1.** Let \( p \) be a prime and \( X \) be a vertex-transitive graph with \( p \) vertices. Then

(a) \( G(X) \) contains the dihedral group \( D_p \), and

(b) the order of \( G(X) \) is even.

We shall repeatedly use Theorem 5 in [1, p. 494] which states the following:

Let \( X \) be a nontrivial vertex-transitive graph with a prime number \( p \) vertices. Then (a) \( G(X) \) is solvable; (b) \( G(X) \) is a Frobenius group; (c) \( G(X) \) is \( 3/2 \)-fold transitive.

We shall show that if \( X \) is a nontrivial symmetric graph with \( p \) vertices then this Frobenius group \( G(X) \) is metacyclic.
3. The construction. Our construction here is similar to the one used in [2].

**Lemma 1.** Let \( p \) be a prime and \( n \) be a positive integer such that \( n \) is even and \( n \) divides \( p-1 \). Then there exists a symmetric graph with \( p \) vertices and degree \( n \).

**Proof.** Let \( H = \{0, 1, 2, \ldots, p-1\} \) be the group of integers modulo \( p \), and \( A(H) \) be the group of automorphisms of \( H \). Then we know that \( A(H) \) is a cyclic group of order \( p-1 \). Say, \( A(H) \) is generated by \( \sigma \), i.e., \( A(H) = \{\sigma, \sigma^2, \ldots, \sigma^{p-2}, \sigma^{p-1} = e\} \).

Since \( n \) divides \( p-1 \), we have \( p-1 = nr \) for some positive integer \( r \). Let \( \tau = \sigma^r \) and

\[
K = \{1\tau, 1\tau^2, \ldots, 1\tau^{n-1}, 1\tau^n = 1\}.
\]

We claim that if one of the elements in \( K \) has its inverse in \( K \) (the operation is taken modulo \( p \)), then every element in \( K \) has its inverse in \( K \). Say, \( -(1\tau^i) \in K \) for some \( i, 1 \leq i \leq n \). Then, for any \( t, 1 \leq t \leq n \), \( -(1\tau^i)\tau^{-t} = -(1\tau^i) \in K \) since \( K\tau = K \). We claim that \( -1 \in K \). Since \( n \) is even, \( (1\tau^n)^2 = 1 \). If \( 1\tau^n = j \), then \( 1 = (j)^2 = j^2 \).

This means \( p \) divides \( j^2 - 1 \). Since \( p \) is a prime and \( r \) is of order \( n, j = -1 \). It follows that every element in \( K \) has its inverse in \( K \). We form the Cayley graph, \( X_{H,K} \), of \( H \) with respect to \( K \). Then since the cardinality of \( K \) is \( n \) and every element in \( K \) has its inverse in \( K \), \( X_{H,K} \) is a regular graph of degree \( n \).

Now we claim that \( X_{H,K} \) is a symmetric graph. Since \( H \) is abelian and the left regular representation of \( H \) is contained in \( G(X_{H,K}) \), the right regular representations (say, generated by \( R \)) belong to \( G(X_{H,K}) \). Consequently, \( X_{H,K} \) is vertex-transitive. Let \( E \) be an arbitrary edge in \( X_{H,K} \), then \( E = [i, i+1\tau^j] \) for some \( i \) and some \( 1\tau^j \in K \), and \([0, 1]\tau^jR = E \). Since \([0, 1] \in E(X) \), it follows that for any two edges in \( E(X_{H,K}) \), there exists an element in \( G(X_{H,K}) \) which takes one to the other, i.e., \( X_{H,K} \) is edge-transitive, and it is symmetric.

Let \( \langle \tau \rangle \) be the group generated by \( \tau = \sigma^r \). We know that the order of \( \langle \tau \rangle \) is \( n \). Two elements, \( i \) and \( j \) in \( H \), are said to be related with respect to \( \langle \tau \rangle \) if and only if there is a \( \tau^k \in \langle \tau \rangle \) such that \( i\tau^k = j \). Since \( \langle \tau \rangle \) is a group, this relation is an equivalence relation. Consequently, \( H \) is partitioned into disjoint subsets

\[
K = K_1 = \{1\tau, 1\tau^2, \ldots, 1\tau^{n-1}, 1\tau^n = 1\},
\]

\[
K_2 = \{(1\sigma)\tau, (1\sigma)\tau^2, \ldots, (1\sigma)\tau^n = 1\sigma\},
\]

\[
\vdots
\]

\[
K_r = \{(1\sigma^{r-1})\tau, (1\sigma^{r-1})\tau^2, \ldots, (1\sigma^{r-1})\tau^n = 1\sigma^{r-1}\}.
\]

The Cayley graphs \( X_{H,K}, X_{H,K_2}, \ldots, X_{H,K_r} \), are symmetric, and they are pairwise isomorphic since \( \sigma^{r-1} \) maps \( X_{H,K} \) onto \( X_{H,K_i} \) isomorphically for \( i = 2, 3, \ldots, r \). Hence, we have

**Lemma 2.** Let \( n, p, H, \sigma \) and \( \tau \) be the same as in Lemma 1, and \( K, K_2, \ldots, K_r \) be (1). Then \( X_{H,K}, X_{H,K_2}, \ldots, X_{H,K_r} \) are symmetric and are pairwise isomorphic.
Lemma 3. The Cayley graphs $X_{H,K_1}, X_{H,K_2}, \ldots, X_{H,K_r}$ constructed in Lemma 2 are independent of the generators of $A(H)$.

Proof. $A(H) = \{e, \sigma, \sigma^2, \ldots, \sigma^{p-1} = e\}$ is generated by $\sigma$, i.e., $1 \sigma$ is a primitive root modulo $p$. Let $\mu = \sigma^i$ be another generator of $A(H)$, then $i$ and $p-1$ are relatively prime, denoted by $(i, p-1) = 1$. Since $p-1 = nr$, we have $(i, n) = 1$. Let

$$K'_j = \{((1\sigma^i)^{\mu}, (1\sigma^i)^{\mu^2}, \ldots, (1\sigma^i)^{\mu^n} = 1\sigma^i)$$

for $j = 0, 1, \ldots, r-1$. Since $(i, n) = 1$, the elements in each of $K'_j$ are distinct. Also, since $(i, n) = 1$, $K'_j = K_j$ for $j = 1, 2, \ldots, r$.

4. The classification.

Lemma 4. Let $X$ be a symmetric graph with a prime number $p$ of vertices, and $[0, i]$ and $[0, j] \in E(X)$. Then there exists a $\theta \in (G(X))_0$ such that $i \theta = j$ where $(G(X))_0$ is the subgroup $\{\tau \in G(X) ; 0 \tau = 0\}$.

Proof. Since $X$ is edge-transitive, there exists $\sigma \in G(X)$ such that $[0, i] \sigma = [0, j]$. If $0 \sigma = 0$ and $i \sigma = j$, then there is nothing to prove. Consider the case $0 \sigma = j$ and $i \sigma = 0$. Since $X$ is vertex-transitive, $X$ is a regular graph with cycles of length $p$ combined together. Then $[0, j]$ is on the cycle of length $p$

$$0 \rightarrow j \rightarrow 2j \rightarrow \cdots \rightarrow (-1)j \rightarrow 0.$$

Let $\theta = R^{-i} D$. Then clearly, $\theta \in G(X)$,

$$0 \theta = 0(R^{-i} D) = j(R^{-i} D) = 0,$$

and

$$i \theta = i(R^{-i} D) = 0(R^{-i} D) = (-j)D = j.$$

Lemma 5. Let $X$ be a nontrivial symmetric graph with a prime number $p$ of vertices denoted by $H = \{0, 1, 2, \ldots, p-1\}$, and $H$ be regarded as the group of integers modulo $p$. If $\sigma \in G(X)$ and $0 \sigma = 0$, then $\sigma$ belongs to the group of automorphisms, $A(H)$, of the group $H$, i.e., $(G(X))_0 \subseteq A(H)$.

Proof. Since $X$ is a vertex-transitive graph with $p$ vertices, $X$ is a regular graph with cycles of length $p$ combined together. There is no loss of generality to assume that $X$ contains the cycle $C_1: 0 \rightarrow 1 \rightarrow 2 \rightarrow \cdots \rightarrow (p-1) \rightarrow 0$. That is, if $X$ does not contain the cycle $C_1$, then we may relabel the vertices so that it contains $C_1$ with $0$ remaining unchanged. In other words, if $X$ does not contain $C_1$, there is an isomorphic map which takes $X$ onto a symmetric graph with $p$ vertices containing $C_1$ and $0$ is left fixed under the map.

Let $\sigma \in G(X)$ such that $0 \sigma = 0$. We want to show $\sigma \in A(H)$. $\sigma \in G(X)$ implies that it is a one-to-one map of the set $H$ onto itself. We only need to show that it is a homomorphism of the group $H$ onto itself, i.e., to show

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & \cdots & i & \cdots & -1 \\ 0 & j & 2j & \cdots & ij & \cdots & (-1)j \end{pmatrix}.$$
Suppose not, then we may assume
\[ 0\sigma = 0, \quad i\sigma = ij, \text{ for } i = 1, 2, \ldots, k; \quad 1 \leq k \leq p-2, \]
\[ (k+1)\sigma \neq (k+1)j. \]

Say, \((k+1)\sigma = kj + m\) where \(m \neq j\). \(X\) contains \(C_i\) implying \([k, k+1] \in E(X)\).
\(\sigma \in G(X)\) implies \([k\sigma, (k+1)\sigma] = [kj, kj+m] \in E(X)\). That means \([0, m] \in E(X)\).
By Lemma 4, there exists a \(\tau \in (G(X))_0\) such that \(1\tau = m\). Then \(\tau^{-1}R^k\sigma R^{-kj} \in (G(X))_0\) and \(m(\tau^{-1}R^k\sigma R^{-kj}) = m\). If \(\tau^{-1}R^k\sigma R^{-kj}\) is not the identity \(e\), then we have a contradiction since \(G(X)\) is a Frobenius group by Theorem 5 in \([1]\). So, we assume \(\tau^{-1}R^k\sigma R^{-kj} = e\). Then
\[ (-1)\tau = (-1)R^k\sigma R^{-kj} = (k-1)\sigma R^{-kj} = -j. \]
We claim \((-1)\sigma = -m\). Consider \(D\tau D\) where
\[
D = \begin{pmatrix}
0 & 1 & 2 & \cdots & i & \cdots & -i & \cdots & -1 \\
0 & -1 & -2 & \cdots & -i & \cdots & i & \cdots & 1
\end{pmatrix}.
\]
Then we have \(0(D\tau D) = 0\) and
\[ 1(D\tau D) = (-1)(\tau D) = (-j)D = j. \]
Then either \((D\tau D)\sigma^{-1}\) is \(e\), or it contradicts \(G(X)\) being a Frobenius group. Hence, we assume \(D\tau D = \sigma\). Then
\[ (-1)\sigma = (-1)(D\tau D) = 1(\tau D) = mD = -m. \]
Now we have
\[
\sigma = \begin{pmatrix}
0 & 1 & \cdots & -1 \\
0 & j & \cdots & -m
\end{pmatrix}, \quad \text{and} \quad \tau = \begin{pmatrix}
0 & 1 & \cdots & -1 \\
0 & m & \cdots & -j
\end{pmatrix}.
\]
Then
\[ m(\tau^{-1}\sigma R^{m-j}) = 1(\sigma R^{m-j}) = jR^{m-j} = m, \]
\[ (-j)(\tau^{-1}\sigma R^{m-j}) = (-1)(\sigma R^{m-j}) = (-m)R^{m-j} = -j, \]
and
\[ 0(\tau^{-1}\sigma R^{m-j}) = 0R^{m-j} = m-j. \]
Since \(m \neq j\), \(0(\tau^{-1}\sigma R^{m-j}) \neq 0\). Hence, \(\tau^{-1}\sigma R^{m-j}\) is not the identity and it leaves \(m\) and \(-j\) pointwise fixed. That contradicts \(G(X)\) being a Frobenius group, and \(\sigma \in A(H)\).

**Theorem 1.** Let \(p\) be a prime and \(n\) be an integer such that \(0 < n < p-1\). Then there exists a nontrivial symmetric graph with \(p\) vertices and degree \(n\) if and only if \(n\) is even and \(n\) divides \(p-1\).

**Proof.** If \(n\) is even and \(n\) divides \(p-1\), then, by Lemma 1, there exists such a graph. Conversely, if a symmetric graph \(X\) with \(p\) vertices and degree \(n\) exists, then \(n\) cannot be an odd integer since a vertex-transitive graph is regular and a regular graph with an odd number of vertices cannot have an odd number degree. If
$p = 2$ and $n = 1$, then the graph is complete and it is a trivially symmetric graph. We claim that $n$ divides $p - 1$. Let $[0, i]$ and $[0, j]$ be any two edges in $E(X)$, then, by Lemma 4, $i$ and $j$ belong to the same orbit (set of transitivity), denoted by $U$, of $(G(X))_0$. If $[0, k]$ is a non-edge in $X$, then $k \notin U$ since each element in $G(X)$ takes an edge to an edge and a non-edge to a non-edge. Hence, the length of $U$ is $n$. Since by Theorem 5 in [1], $G(X)$ is $3/2$-fold transitive, the orbits of $(G(X))_0$ have the same length. It follows that $n$ divides $p - 1$.

**Theorem 2.** Let $p$ be a prime and $n$ be an even integer such that $0 < n < p - 1$ and $n$ divides $p - 1$. Then any two symmetric graphs with $p$ vertices and degree $n$ are isomorphic.

**Proof.** Let $X$ be a symmetric graph with $p$ vertices and degree $n$. Then $X$ is a regular graph with cycles of length $p$ combined together. We label the vertices of $X$ by $0, 1, \ldots, p - 1$, and we regard $\{0, 1, \ldots, p - 1\} = H$ as the group of integers modulo $p$. By Lemma 5, $(G(X))_0$ is contained in the group of automorphisms, $A(H)$, of $H$. Since $A(H)$ is cyclic, $(G(X))_0$ is cyclic. Let $\tau$ be a generator of $(G(X))_0$. By Lemma 4, any two edges $[0, i]$ and $[0, j]$ incident with $0$, there exists a $\tau^k \in (G(X))_0$ such that $i\tau^k = j$. This means that the length of the orbit of $(G(X))_0$ to which $i$ belongs must be $n$. In fact, the length of every orbit of $(G(X))_0$ is $n$ since $G(X)$ is $3/2$-fold transitive on $V(X) = H$. Consequently, the order of $(G(X))_0 = \langle \tau \rangle$ must also be $n$. $[0, i] \in E(X)$ implies $[0, i\tau^k] \in E(X)$ for $k = 0, 1, \ldots, n - 1$. Since $X$ is a regular graph with cycles of length $p$ combined together, $X$ is a Cayley graph $X_{H, k}$, where $K = \{i, i\tau, \ldots, i\tau^{n - 1}\}$. Let $\sigma$ be a generator of $H$, then $i = 1\sigma^t$ for some $t$, and $K$ can be written as $\{1\sigma^t, (1\sigma^t)r, \ldots, (1\sigma^t)r^{n - 1}\}$.

Let $Y$ be another symmetric graph with $p$ vertices and degree $n$. We also label the vertices of $Y$ by $0, 1, \ldots, p - 1$, i.e., $V(Y) = H$. Then, by the similar reasons, $(G(Y))_0 = \langle \theta \rangle$ is a cyclic subgroup of order $n$ in $H$, and $Y$ is a Cayley graph $Y_{H, K'}$, where $K' = \{m, m\theta, \ldots, m\theta^{n - 1}\}$ and $[0, m] \in E(Y)$. Since $\langle \theta \rangle = H$, $m = 1\sigma^s$ for some $s$, and $K' = \{1\sigma^s, (1\sigma^s)r, \ldots, (1\sigma^s)r^{n - 1}\}$. Since $A(H)$ is cyclic, the subgroup of order $n$ in $A(H)$ is unique. Hence, $\langle \tau \rangle = \langle \theta \rangle$, and $K' = \{1\sigma^s, (1\sigma^s)r, \ldots, (1\sigma^s)r^{n - 1}\}$. By Lemma 2, $X \cong Y$. By Lemma 3, $X$ and $Y$ are so constructed that they do not depend on the choice of the generators $\sigma$ of $H$.

In the proof of Theorem 2, we have shown the following:

**Corollary 1.** Let $X$ be a symmetric graph with a prime number $p$ of vertices and degree $n$ where $n$ is even, $0 < n < p - 1$ and $n$ divides $p - 1$. Then $(G(X))_0 = \langle \tau \rangle$ is a cyclic group of order $n$ generated by $\tau$ which can be regarded as an automorphism of the group of integers modulo $p$.

5. The group.

**Theorem 3.** Let $X$ be the symmetric graph with a prime number $p$ of vertices and degree $n$ where $0 < n < p - 1$, $n$ is even and $n$ divides $p - 1$. Then

1. $G(X)$ is a Frobenius group. Hence $G(X)$ is $3/2$-fold transitive. $G(X)$ contains the dihedral group of order $2p$. 

(2) $|G(X)| = np$.

(3) $\langle R \rangle$ is the Frobenius kernel of $G(X)$. Hence, $\langle R \rangle$ is normal in $G(X)$ where $R = (012\ldots(p-1))$.

(4) $G(X)$ is metacyclic.

(5) $G(X)$ is a semidirect product of the cyclic subgroups $\langle R \rangle$ and $(G(X))_0$. $G(X)$ is generated by $R$ and $\sigma$ with defining relations

$$R^n = e, \quad \sigma^n = e, \quad \sigma R \sigma^{-1} = R^r$$

where $r^n \equiv 1 \mod p$.

(6) All Sylow subgroups of $G(X)$ are cyclic.

**Proof.** (1) was proved in [1, Theorem 5]. Our Proposition 1 shows the dihedral group of order $2p$ belonging to $G(X)$.

(2) Since $G(X)$ is vertex-transitive $|G(X)|$ is equal to the product of $|(G(X))_0|$ and $p$ by Corollary 5.2.1 on p. 56 in [3].

(3) Let $N$ be the subset of $G(X)$ consisting of the identity together with those elements which fix no vertices. Then we know that, by Frobenius' theorem (see p. 292 in [3]), $N$ is a normal subgroup of $G(X)$ ($N$ is called the Frobenius kernel of $G(X)$), and the order of $N$ is equal to the index of $(G(X))_0$ in $G(X)$, i.e., $|N| = p$ by (2). Since $N$ clearly contains $\langle R \rangle$ and $|\langle R \rangle| = p$, $N = \langle R \rangle$.

(4) Since $G(X)/\langle R \rangle \simeq (G(X))_0$, $G(X)/\langle R \rangle$ is abelian. Hence $\langle R \rangle$ contains the commutator subgroup $(G(X))^2$ of $G(X)$. $G(X)$ containing the dihedral group implies $(G(X))^2 \neq \{e\}$. Since $\langle R \rangle$ is a cyclic group of order $p$, we have $\langle R \rangle = (G(X))^2$. Hence, $G(X)$ is metacyclic.

(5) Since $\langle R \rangle$ is normal in $G(X)$ and $\langle R \rangle \cap (G(X))_0 = \{e\}$, $G(X) = \langle R \rangle (G(X))_0$.

Since $(G(X))_0$ is a cyclic group of order $n$, $G(X)$ is generated by $R$ and $\sigma$ where $\sigma$ is a generator of $(G(X))_0$, and $\sigma$ by Corollary 1, belongs to the group of automorphisms of integers modulo $p$. Since $\langle R \rangle$ is normal in $G(X)$, $\sigma R \sigma^{-1} = R^r$ for some $r$. Then, using the fact that $\sigma$ belongs to the group of automorphisms of integers modulo $p$, and $\sigma$ is of order $n$, we have

$$\sigma R \sigma^{-1} = \begin{pmatrix} 0 & 1 & \cdots & k^{n-1} & \cdots \\ 0 & k & \cdots & 1 & \cdots \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ 0 & k^{n-1} & \cdots & k^{n-1} & \cdots \\ k^{n-1} & 1 & \cdots & k^{n-1}(k+1) & \cdots \end{pmatrix} \begin{pmatrix} 0 & 1 & \cdots & (k+1) & \cdots \\ 1 & 2 & \cdots & (k+1) & \cdots \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ 0 & k^{n-1} & \cdots & k^{n-1}(k+1) & \cdots \\ k^{n-1} & k^{n-1}(k+1) & \cdots & \cdots \end{pmatrix}$$

where we use the fact $k^n = 1$, and all the operations are taken modulo $p$. That means $r = k^{n-1}$, and $r^n = (k^{n-1})^n = (k^n)^{n-1} = 1$, i.e., $r^n \equiv 1 \mod p$, and we have obtained the defining relations.

(6) It follows from Theorem 9.4.3 on p. 146 in [3].

**6. Summary and examples.** For any given odd prime $p$, $p-1$ is even and is a product of primes $p-1 = 2^{t_1} q_2^{t_2} \cdots q_t^{t_t}$. From this decomposition we can find all even integers $n_i$ such that $2 \leq n_i < p-1$ and $n_i$ divides $p-1$. Say, there are $k$ of them; and for each $i = 1, 2, \ldots, k$, we have $p-1 = n_i r_i$ for some integer $r_i$. Let $\sigma$ be a generator of $A(H)$ which is the group of automorphisms of the group $H$ of integers
modulo $p$, then $\sigma$ is of order $p-1$. Let $\tau_i = \sigma^i$, then the order of $\tau_i$ is $n_i$. Let $K_i = \{1, \tau_i, \tau_i^2, \ldots, \tau_i^{n_i} = 1\}$, and we form the Cayley graph $X_{H, K_i}$ which, by Theorems 1 and 2, is the unique (up to isomorphism) symmetric graph with $p$ vertices and degree $n_i$. With the null graph and the complete graph, we have obtained all symmetric graphs with $p$ vertices. With the help of Theorem 3, we know the structure of each of their groups of automorphisms.

The case of $p = 11$. Since $(p-1)/2$ is a prime, the only symmetric graphs of 11 vertices are null graph, complete graph and cycles of length 11. Their groups of automorphisms are $S_{11}, S_{11}$ and $D_{11}$ respectively.

The case of $p = 13$. Besides the null graph and the complete graph of 13 vertices (their group of automorphisms is $S_{13}$), the symmetric graphs with 13 vertices are with degree 2, 4 and 6. Let $H = \{0, 1, 2, \ldots, 12\}$ be the group of integers modulo 13. The group of automorphisms $A(H)$ of $H$ is of order 12 generated by $\sigma$ where $1 \sigma = 2$ (2 is a primitive root modulo 13). Hence, we have $\sigma = (1 2 4 8 3 6 12 11 9 5 10 7)$ and $A(H) = \{\sigma, \sigma^2, \ldots, \sigma^{12} = e\}$.

Degree 2. Each $X_{H, \{1, \sigma^i\}}, i = 1, 2, \ldots, 6$, is a cycle of length 13. Clearly, they are pairwise isomorphic. $G(X_{H, \{1, \sigma^i\}}) = D_{13}$, $i = 1, 2, \ldots, 6$.

Degree 4. Let $K_1 = \{1, \sigma^8 = 8, 1 \sigma^6 = 12, 1 \sigma^5 = 5, 1 \sigma^{12} = 1\}$. $X_{H, K_1}$ is shown in Figure 1.
$K_2 = \{1^{\sigma_3} = 3, 1^{\sigma_7} = 11, 1^{\sigma_{10}} = 10, 1^{\sigma_2} = 2\}$ and $X_{H,K_2} \simeq X_{H,K_1}$ where the isomorphic map is $\sigma$. Similarly, $K_3 = \{1^{\sigma_6} = 6, 1^{\sigma_9} = 9, 1^{\sigma_{11}} = 7$ and $1^{\sigma_4} = 4\}$ and $X_{H,K_1} \simeq X_{H,K_3}$ where the isomorphic map is $\sigma^2$.

$G(X_{H,K_i}), i = 1, 2, 3$, is generated by $R$ and $\tau = \sigma^3$ where

$$R = (012\ldots12), \quad \text{and} \quad \tau = (18125)(231110)(4697)$$

with $R^{13} = e$, $\tau^4 = e$ and $\tau R \tau^{-1} = R^5$. The order of $G(X_{H,K_i})$ is 52, $i = 1, 2, 3$.

Degree 6. Let $K_4 = \{1^{\sigma_2} = 4, 1^{\sigma_4} = 3, 1^{\sigma_8} = 12, 1^{\sigma_9} = 9, 1^{\sigma_{10}} = 10, 1^{\sigma_{12}} = 1\}$. $X_{H,K_4}$ is shown in Figure 2.

Figure 2

$K_5 = \{1^{\sigma_3} = 8, 1^{\sigma_5} = 6, 1^{\sigma_7} = 11, 1^{\sigma_8} = 5, 1^{\sigma_{11}} = 7, 1^{\sigma_2} = 2\}$ and $X_{H,K_5} \simeq X_{H,K_0}$ where the isomorphic map is $\sigma$.

$G(X_{H,K_5}), j = 4, 5$, is generated by $R$ and $\theta = \sigma^2$ where

$$R = (012\ldots12), \quad \text{and} \quad \theta = (14312910)(2861157)$$

with $R^{13} = e$, $\theta^6 = e$ and $\theta R \theta^{-1} = R^{10}$. The order of $G(X_{H,K_5})$ is 78.
REFERENCES


UNIVERSITY OF PITTSBURGH,
PITTSBURGH, PENNSYLVANIA 15213