Walks on Unitary Cayley Graphs and Applications

Elias Cancela, Daniel A. Jaume, Adrián Pastine and Denis Videla

Universidad Nacional de San Luis

Submitted to: The Electronic Journal of Combinatorics, on May 5, 2014

Key words: Sums of units, Unitary Cayley Graphs, Walks.

AMS subject classification: 05C25, 05C50.

Abstract

In this paper, we determine an explicit formula for the number of walks in $X_n = \text{Cay}(\mathbb{Z}_n, U_n)$, the unitary Cayley Graphs of order $n$, between any pair of its vertices. With this result, we give the number of representations of a fixed residue class mod $n$ as the sum of $k$ units of $\mathbb{Z}_n$.

1 Introduction

Let $\Gamma$ be a multiplicative group with identity 1. For $S \subset \Gamma$, $1 \notin S$ and $S^{-1} = \{s^{-1} : s \in S\} = S$ the Cayley Graph $X = \text{Cay}(\Gamma, S)$ is the undirected graph having vertex set $V(X) = \Gamma$ and edge set $E(X) = \{a, b : ab^{-1} \in S\}$. By right multiplication $\Gamma$ may be considered as a group of automorphisms of $X$ acting transitively on $V(X)$. The Cayley graph $X$ is regular of degree $|S|$. Its connected components are the right cosets of the subgroup generated by $S$. So $X$ is connected, if $S$ generates $\Gamma$. More information about Cayley graph can be found in books on algebraic graph theory like those written by Biggs [1] and by Godsil and Royle [3].
For a positive integer \( n > 1 \) the unitary Cayley graph \( X_n = \text{Cay}(\mathbb{Z}_n, U_n) \) is defined by the additive group of the ring \( \mathbb{Z}_n \) of integers modulo \( n \) and the multiplicative group \( U_n \) of its units. If we represent the elements of \( \mathbb{Z}_n \) by the integers \( 0, 1, \ldots, n - 1 \) then it is well known that \( U_n = \{ r \in \mathbb{Z}_n : \gcd(r, n) = 1 \} \). So \( X_n \) has vertex set \( V(X_n) = \mathbb{Z}_n = \{ 0, 1, \ldots, n - 1 \} \) and edge set \( E(X_n) = \{ \{ a, b \} : a, b \in \mathbb{Z}_n, \gcd(a - b, n) = 1 \} \).

Klotz and Sander in [5] show that a graph \( X_n \) is regular of degree \( |U_n| = \varphi(n) \), where \( \varphi(n) \) denotes the Euler totient function. Let \( p \) be a prime number, then \( X_p = K_p \) (the complete graph on \( p \) vertices). Let \( \alpha \) be a positive integer, the \( X_p^\alpha \) is a complete \( p \)-partite graph which has the residue classes modulo \( p \) in \( \mathbb{Z}_n \) as maximal sets of independent vertices. Unitary Cayley graphs are highly symmetric. They have some remarkable properties connecting graph theory and number theory (for example it can be proved that \( \varphi(n) \) is even, for \( n > 2 \), via a graph theory argument, using unitary Cayley graphs).

2 Walks in Complete Graphs

Let \( u \) and \( v \) be (not necessarily distinct) vertices of a graph \( X \). A \( u - v \) walk of \( X \) is a finite, alternating sequence

\[
u = u_0, e_1, u_1, e_2, \ldots, u_{k-1}, e_k, u_k = v\]

of vertices and edges, beginning with vertex \( u \) and ending with vertex \( v \), such that \( e_i = u_{i-1}u_i \) for \( i = 1, 2, \ldots, k \). The number \( k \) is called the length of the walk. A trivial walk contains no edges, that is, \( k = 0 \). We note that there may be repetition of vertices and edges in a walk. We often will indicate only the edges of a walk.

A \( u - v \) walk is closed or open depending on whether \( u = v \) or \( u \neq v \).

We denote with \( w(X, k, v_i, v_j) \) the total number of walk of length \( k \) between the vertices \( v_i \) and \( v_j \) of a given graph \( X \).

In this section we are going to count the number of \( k \)-walks in \( K_n \), the complete graph of \( n \) vertices.

The adjacency matrix \( A(X) \) of a graph \( X \) is the integer matrix with rows and columns indexed by the vertices of \( X \), such that the \( uv \)-entry of \( A(X) \) is 1 if \( u \) and \( v \) are neighbors, and 0 otherwise, so \( A(X) \) is a symmetric 01-matrix. Because a graph has no loops, the diagonal entries of \( A(X) \) are zero.

We will uses the next well known result:

**Theorem 2.1** If \( A \) is the adjacency matrix of a graph \( X \) with set of vertices \( V(X) = \{ v_1, v_2, \ldots, v_n \} \), then the \( (i, j) \) entry of \( A^k \), \( k \geq 1 \), is the number of different \( v_i - v_j \) walks of length \( k \) in \( X \).
In particular, we are interested in the number of walks in complete graphs. As $A(K_n)$ is the $n \times n$-matrix
\[ A(K_n) = \text{circ}(0, 1, \ldots, 1) \]
where $\text{circ}(0, 1, \ldots, 1)$ is the circulant matrix whose first row is the $n$-vector $(0, 1, \ldots, 1)$, see Davis [2]. As the circulant matrices are closed under product, we have that
\[ A(K_n)^2 = \text{circ}(n - 1, n - 2, \ldots, n - 2) \]
And in general
\[ A(K_n)^k = \text{circ}(a_{n,k}, b_{n,k}, \ldots, b_{n,k}) \]
where $a_{n,1} = 0$ $b_{n,1} = 1$ and for $k \geq 2$
\[ a_{n,k} = (n - 1)b_{n,k-1} \]
\[ b_{n,k} = a_{n,k} + (-1)^{k-1} \]
Thus we have the following recursive relation
\[ b_{n,k} = (n - 1)b_{n,k-1} + (-1)^{k-1} \]
which has the following closed form
\[ b_{n,k} = \frac{1}{n} \left( (n - 1)^k - (-1)^k \right) \quad \text{for} \quad k \geq 0 \]

Therefore, we have the following result.

**Proposition 2.2** The number of $v_i - v_j$ walks of length $k$ in a complete graphs $K_n$ is
\[
\text{w}(K_n, k, v_i, v_j) := \begin{cases} 
\frac{1}{n} \left( (n - 1)^k - (-1)^k \right) & \text{if } v_i \neq v_j \\
\frac{n - 1}{n} \left( (n - 1)^{k-1} - (-1)^{k-1} \right) & \text{if } v_i = v_j
\end{cases}
\]

This result is known, see [13], but the proof given here is different.

### 3 Walks on $X_{\text{rad}(n)}$

Given a positive integer $n$, we are going to count the number of $k$-walks in $X_{\text{rad}(n)}$, the unitary Cayley graph of $\text{rad}(n)$ vertices, where $\text{rad}(n)$ is the product of all primes that divide $n$, i.e., $\text{rad}(n) = \prod_{p|n} p$. So, we are going to resolve the problem for square-free integers.

Let $X_1 = (V_1, E_1)$ and $X_2 = (V_2, E_2)$ be graphs. The Kronecker product of $X_1$ and $X_2$ is the graph $X = (V, E)$ denoted by $X_1 \otimes X_2$ (also known as direct product, categorical product, etc.) where $V = V_1 \times V_2$, the Cartesian product of $V_1$ and $V_2$, with $(u_1, u_2)$ and $(v_1, v_2)$ are adjacent in $X$ if and
only if \( u_1 \) and \( v_1 \) are adjacent in \( X_1 \) and \( u_2 \) and \( v_2 \) are adjacent in \( X_2 \). See [4].

A direct consequence of the definition of Kronecker product of graphs is that a \( k \)-walk of \( G \otimes H \) is the Kronecker product of a \( k \)-walk of \( G \) times a \( k \)-walk of \( H \). Conversely, the Kronecker product of a \( k \)-walk of \( G \) times a \( k \)-walk of \( H \) give us a \( k \)-walk of \( G \otimes H \). Summarizing

**Lemma 3.1** Given \( n \) graphs \( H_i \), let us consider the Kronecker product of all them

\[
G = \bigotimes_{i=1}^{n} H_i
\]

Any vertex \( x \) of \( G \) have the form \( x = (x_1, x_2, \ldots, x_n) \) where \( x_i \in V(H_i) \).
Then the number of walk of length \( k \) between any two vertices \( x \) and \( y \) of \( G \) is

\[
w(G, k, x, y) = \prod_{i=1}^{n} w(H_i, k, x_i, y_i)
\]

For our next lemma we need the following two results of Ramaswamy and Veena (2009) [7]

**Theorem 3.2 (Ramaswamy and Veena)** If \( (m, n) = 1 \), then the Kronecker product of unitary Cayley graphs \( X_m \) and \( X_n \) is isomorphic to \( X_{mn} \).

**Corollary 3.3 (Ramaswamy and Veena)** If \( n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \), then the Kronecker product of unitary Cayley graphs \( X_{p_1^{\alpha_1}} \otimes X_{p_2^{\alpha_2}} \otimes \cdots \otimes X_{p_m^{\alpha_m}} \) is isomorphic to \( X_n \)

Now we can given our next result

**Lemma 3.4** Given positive integers \( n \) and \( k \), for any \( 0 \leq i, j \leq n \) the number of \( i-j \)-walks of length \( k \) in \( X_{\text{rad}(n)} \), i.e., \( w(X_{\text{rad}(n)}, k, i, j) \) is

\[
\prod_{p \in C(n,i,j)} \frac{p-1}{p} \left( (p-1)^{k-1} - (-1)^{k-1} \right) \prod_{p \in A(n,i,j)} \frac{1}{p} \left( (p-1)^{k} - (-1)^{k} \right)
\]

where

\[
C(n,i,j) = \{ p \text{ prime : } p|n, i = j \mod p \}
\]

\[
A(n,i,j) = \{ p \text{ prime : } p|n, i \neq j \mod p \}
\]

**Proof.** Direct from the lemma 3.1 and the previous corollary.
4 Relation between $X_n$ and $X_{\text{rad}(n)}$

We use the blow-up notation. Given a graph $G$ and a positive integer $n$, The blow-up of $G$ of order $r$, denote by $B(G, r)$, is the graph with set vertex $V(B(G, r)) = V(G) \times [r]$, where as usual $[r] := \{1, 2, \ldots, r\}$, and set of edges

$$E(B(G, r)) = \{(u, a), (v, b) / \{u, v\} \in E(G), a, b \in [r]\}$$

i.e., the vertex $(u, a)$ is neighbor of the vertex $(v, b)$ in $B(G, r)$ if and only if the vertices $v$ and $u$ of $G$ are neighbors.

**Proposition 4.1** Given positive integers $r$ and $k$, and a graph $G$, the number of $k$-walks in $B(G, r)$ between its vertices $(u, a)$ and $(v, b)$ is:

$$w(B(G, r), k, (u, a), (v, b)) = r^{k-1}w(G, k, u, v)$$

**Proof.** Evident from the next observation: given a $k$-walk in $G$ between its vertices $u$ and $v$:

$$u = v_0, v_1, \ldots, v_k = v$$

We have that

$$(u, a) = (v_0, a_0), (v_1, a_1), \ldots, (v_k, a_k) = (v, b)$$

with $a_i \in [r]$, is a $k$-walk in $B(G, r)$ for any choice of the integers $a_i$. Thus if we fix the ends, i.e. if we fix $(u, a)$ and $(v, b)$, we have that the number of $k$-walks between them in $B(G, r)$ is $r^{k-1}w(G, k, u, v)$. □

Now we are going to proved that all the structural information of $X_n$ is in $X_{\text{rad}(n)}$, actually we will prove that $X_n = B(X_{\text{rad}(n)}, n/\text{rad}(n))$.

For the next proposition we recall that for each vertex $x$ of a graph $G$, the neighborhood of $x$ in $G$ is $N_G(x) = \{y \in V(G) : \{x, y\} \in E(G)\}$.

**Theorem 4.2** Given $x, y \in \mathbb{Z}_n$ if $x \equiv y \text{ mod } \text{rad}(n)$ then $x$ and $y$ are not neighbors in $X_n$ and they have the same neighborhood in $X_n$: $N(x) = N(y)$

**Proof.** The first statement is a clear consequence of the following elementary facts:

1. In an unitary Cayley graphs two vertices $x$ and $y$ are neighbors if and only if $x - y \in U_n$.
2. For any two integers $a$ and $b$, $(a, b) = 1$ if and only if $(a, \text{rad}(b)) = 1$.
3. For any two integers $a$ and $b$, if $a \equiv 0 \text{ mod } b$, then $a \equiv 0 \text{ mod } \text{rad}(b)$, i.e., $(a, \text{rad}(b)) \neq 1$. 

5
The set of neighbors of \( x \) is

\[ N(x) := \{ z \in \mathbb{Z}_n : z - x \in \mathbb{U}_n \} \]

As \( x \equiv y \mod \text{rad}(n) \), then for all \( z \in \mathbb{Z}_n \) such that \( z - x \in \mathbb{U}_n \) we have that \( z - x \equiv z - y \mod \text{rad}(n) \), then \((z - y, \text{rad}(n)) = 1\), i.e., \( z - y \in \mathbb{U}_n \), so \( N(x) = N(y) \).

**Corollary 4.3** For any positive integer \( n \) we have that the unitary Cayley graph \( X_n \) is the blow-up of order \( n/\text{rad}(n) \) of \( X_{\text{rad}(n)} \):

\[ X_n = B\left(X_{\text{rad}(n)}, \frac{n}{\text{rad}(n)}\right) \tag{4} \]

**Proof.** Obvious from the previous theorem and definition of blow-up.

Now we can set our main result:

**Theorem 4.4** Given two positive integers \( n \) and \( k \), the number of \( i-j \)-walks of length \( k \) in \( X_n \) is

\[ w(X_n, k, i, j) = \left( \frac{n}{\text{rad}(n)} \right)^{k-1} w(X_{\text{rad}(n)}, k, i \mod \text{rad}(n), j \mod \text{rad}(n)) \tag{5} \]

where \( i \mod \text{rad}(n) \) is the residue of \( i \) modulo \( \text{rad}(n) \).

**Proof.** Just use corollary 4.3 and proposition 4.1

### 5 Applications

We give two direct applications of theorem 4.4. The first one to additive number theory and the second one to linear algebra.

First application: the multiplicative groups of units in the ring \( \mathbb{Z}_n \) of residue classes mod \( n \) consists of the residues \( r \mod n \) with \( (r, n) = 1 \). We use unitary Cayley graphs to determine the number of representations of a fixed residue class mod \( n \) as the sum of \( k \) units in \( \mathbb{Z}_n \).

In this section we are going to show that there exists an obvious bijection between walks in \( X_n \) and ordered sums of units in \( \mathbb{Z}_n \).

Let \( k \) and \( n \) be positive integers, and let \( r \) be a residue class of \( \mathbb{Z}_n \). We call the set of all ordered \( k \)-sums of units of \( \mathbb{Z}_n \) that sum \( r \) module \( n \) as \( S(n, k, r) \), so

\[ S(n, k, r) := \left\{ (u_1, u_2, \ldots, u_k) \in \mathbb{U}_n^k : u_1 + u_2 + \cdots + u_k \equiv r \mod n \right\} \tag{6} \]

The cardinality of the above set will be denote with \( s(n, k, r) := |S(n, k, r)| \).

The next result says that each ordered \( k \)-sum of units of \( \mathbb{Z}_n \) that sums \( r \) give us a \( k \)-walk between 0 and \( r \) in \( X_n \), and conversely.
Theorem 5.1 For all positive integers \( n \) and \( k \), and for any residue class \( r \) of \( \mathbb{Z}_n \), we have that \( s(n, k, r) = w(X_n, k, 0, r) \).

Proof. Given \((u_1, u_2, \ldots, u_k) \in S(n, k, r)\), we can obtain a \( k \)-walk from 0 to \( r \) in \( X_n \) as follow:

\[
0, u_1, 0 + u_1, u_2, 0 + u_1 + u_2, \ldots, u_k, 0 + u_1 + u_2 + \cdots + u_k = r
\]

Conversely, if we have a \( k \)-walk from 0 to \( r \) in \( X_n \):

\[
0, u_1, x_1, u_2, x_2, \ldots, u_k, x_k = r
\]

by definition of \( X_n \) for each \( i \in 1, \ldots, k \)

\[
x_i = 0 + u_1 + u_2 + \cdots + u_i
\]

Thus \( u_1 + u_2 + \cdots + u_k = x_k = r \), and the edges of the \( k \)-walk over \( X_n \) gives an ordered \( k \)-sum of units of \( \mathbb{Z}_n \) that sums \( r \).

These results is a generalization of part of a recent work by Sander (2009) [12], who proved it in the case \( k = 2 \).

In particular we have that for any two positive integers \( n \) and \( k \), the number of ordered homogeneous \( k \)-sums in \( \mathbb{Z}_n \), is

\[
s(n, k, 0) = \left( \frac{n}{\text{rad}(n)} \right)^{k-1} \prod_{p|n} \frac{p-1}{p} \left( (p-1)^{k-1} - (-1)^{k-1} \right) \quad \text{(7)}
\]

This last result, could be prove without using unitary Cayley graphs, via a recursive argument.

Second application: Circulant matrices arise, for example, in applications involving the discrete Fourier transformation and the study of cyclic codes for error correction [2].

In Rimas [8] (2005), [9] (2005), [10] (2006), [11] (2006), and Köken and Bozkurt [6] (2011) these authors have studied positive integer powers for circulant matrices of type \( \text{circ}(0, a, 0, \ldots, b) \).

Now, using that power of circulant matrices are circulant, see [2], and theorem 4.4 we can easily derive a general expression for the arbitrary positive powers of circulant matrices that are adjacency matrices of unitary Cayley Graphs, by a very different technique for that used in the works by Rimas, or Köken and Bozkurt.

From theorems 4.4 and 2.1

Proposition 5.2 Given \( n, k \in \mathbb{Z} \), we have that

\[
A(X_n)^k = \text{circ}(w(X_n, k, 0, 0), w(X_n, k, 0, 1), \ldots, w(X_n, k, 0, n))
\]
References

[1] N. Biggs, *Algebraic graph theory*, Second Edition, Cambridge University Press, 1993.

[2] J. P. Davis, *Circulant Matrices*. Chelsea Publishing, New York. 1994.

[3] C. Godsil and R. Royle, *Algebraic graph theory*, Graduate Text in Mathematics. Springer, 2001.

[4] R. Hammack, W. Imrich and S. Klavžar, *Handbook of Product Graphs*. 2nd edition. CRC Press, 2011.

[5] W. Klotz and T. Sander, *Some properties of unitary Cayley graphs*, The Electronic Journal of Combinatorics 14 (2007), R45, pp. 1-12.

[6] F. Köken and D. Bozkurt, *Positive integer powers for one type of odd order circulant matrices*. Applied Mathematics and Computation 217 (2011) 4377-4381.

[7] H.N. Ramaswamy and C.R. Veena, *On the Energy of Unitary Cayley Graphs*. The Electronic Journal of Combinatorics 16 (2009), #N24

[8] J. Rimas, *On computing of arbitrary positive integer powers for one type of odd order symmetric circulant matrices-I*. Applied Mathematics and Computation 165 (2005) 137-141.

[9] J. Rimas, *On computing of arbitrary positive integer powers for one type of odd order symmetric circulant matrices-II*. Applied Mathematics and Computation 169 (2005) 1016-1027.

[10] J. Rimas, *On computing of arbitrary positive integer powers for one type of even order symmetric circulant matrices-I*. Applied Mathematics and Computation 172 (2006) 86-90.

[11] J. Rimas, *On computing of arbitrary positive integer powers for one type of even order symmetric circulant matrices-II*. Applied Mathematics and Computation 174 (2006) 511-552.

[12] J. W. Sander, *On the addition of units and nonunits mod m*, Journal of Number Theory 129 (2009) 2260-2266.

[13] R. P. Stanley *Topic in Algebraic Combinatorics*. Preliminary version 24th April 2010.