Eigenspaces of Hamming graphs and unitary Cayley graphs

Torsten Sander
Institut für Mathematik, Technische Universität Clausthal
D-38678 Clausthal-Zellerfeld, Germany

Received 28 February 2009, accepted 7 December 2009, published online 19 January 2010

Abstract

In this work, the eigenspaces of unitary Cayley graphs and certain Hamming graphs are considered. It is shown that these graph classes are closely related and admit particularly simple eigenspace bases for all eigenvalues, namely bases containing vectors only with entries from the set \{0, 1, −1\}. A direct consequence is that the considered graph classes are integral.

Keywords: Eigenvalue, eigenspace, Hamming graph, Cayley graph.
Math. Subj. Class.: 05C50, 15A18

1 Introduction

Graph eigenspaces with particularly simple structure have excited some research interest lately [1], [5], [10], [12], [13], [14]. In this work we are interested in the eigenspaces of certain Cayley graphs and Hamming graphs. Cayley graphs are usually defined in terms of groups, encoding their structures, whereas Hamming graphs are related to codes. We show that, for all eigenvalues, the graphs we consider admit corresponding eigenspace bases that consist only of vectors with entries 0, 1, −1. We call such bases simply structured. Clearly, the associated eigenvalues are all integers.

Cayley graphs have been an object of study in algebraic graph theory for some time now. They are closely linked to groups, encoding their structures. To be precise, the Cayley graph \( \text{Cay}(G, C) \) for a given group \( G \) and a subset \( C \subseteq G \) has vertex set \( G \) and edges exactly between those vertices \( g, h \) for which \( g^{-1}h \in C \), cf. [3].

In this paper we are interested in the unitary Cayley graphs \( \text{Cay}(\mathbb{Z}_n, U_n) \), where \( U_n \) denotes the set of units of \( \mathbb{Z}_n \). Such a graph has vertex set \( \{1, \ldots, n\} \) and an arc between vertices \( i \) and \( j \) exactly if \( \gcd(i − j, n) = 1 \). Some results on unitary Cayley graphs in...
particular can be found in [2], [7] and [11]. Note that the unitary Cayley graphs are not to be confused with the coprime graphs of integers, which have a very similar definition. Two vertices $i, j$ are adjacent exactly if $\gcd(i, j) = 1$, cf. [9].

The notion of Hamming graphs has evolved over time so that in today’s literature the term “Hamming graph” is used for the original class but also for many of the possible generalizations.

The traditional Hamming graph is defined to model the 1-distance relation in a Hamming scheme. It means that, given an alphabet of $m$ letters, all possible words with $r$ letters from this alphabet are formed. Some definitions even restrict themselves to a binary alphabet. Each of the $m^r$ words is associated with a graph vertex. Two vertices are joined by an edge if their Hamming distance is one, i.e. if their associated words differ in exactly one letter position.

Two immediate generalizations come to mind. Firstly, one can allow each letter position to use its own private alphabet. Secondly, one can model alternative distance relations in the Hamming scheme by joining edges if the Hamming distance is one from a given list $K$. Our definition of the class of Hamming graphs includes both extensions. We write $HG(m_1, \ldots, m_r; K)$ where the respective alphabet sizes are $m_1, \ldots, m_r$ and $K$ a list of positive Hamming distances. We consider the eigenspaces of Hamming graphs $HG(p_1, \ldots, p_r; 1, \ldots, d)$ for distinct primes $p_1, \ldots, p_r$.

2 Basics and notation

We define the $r$-th distance power $G^{(r)}$ of a given graph $G$ as the graph with the same vertex set as $G$ and two vertices adjacent if and only if their distance in $G$ is at most $r$. By $\overline{G}$ we denote the complement of $G$.

2.1 Graph eigenspaces

The adjacency matrix $A = (a_{ij})$ of a graph with vertices $v_1, \ldots, v_n$ is defined by setting $a_{ij}$ to 1 when $v_i$ is adjacent to $v_j$ and to 0 otherwise. The eigenvalues of a graph are the eigenvalues of its associated adjacency matrix. For an undirected graph this matrix is symmetric so that the eigenvalues of a graph are real numbers. Further basic results of algebraic graph theory can be found in [3] and [8].

The entries of the adjacency matrix depend on the vertex order, and so do the entries of the eigenvectors of the adjacency matrix. A notion of graph eigenvectors that does not depend on vertex order can be obtained by considering every eigenvector as a map $V \to \mathbb{R}$ so that the $i$-th vertex of the graph is assigned the value of the $i$-th component of an eigenvector. Thus, the equation $Ax = \lambda x$ that must hold for an adjacency matrix $A$ and a potential eigenvector $x$ for eigenvalue $\lambda$ of $A$ can be checked directly on the graph itself. It translates to the requirement that for every vertex the sum over the values of its neighbors must equal $\lambda$ times its own value.

We require the following basic result on regular graphs [3]:

**Lemma 2.1.** Let $G$ be a $k$-regular graph on $n$ vertices with eigenvalues $\lambda_1, \ldots, \lambda_k$.

Then the eigenvalues of $\overline{G}$ are $n - k - 1$ and all numbers $-\lambda_i - 1$ where $\lambda_i \neq k$. The eigenspace for eigenvalue $n - k - 1$ is spanned by the all ones vector. The eigenspace for eigenvalue $-\lambda_i - 1$ of $\overline{G}$ is the same as the eigenspace for eigenvalue $\lambda_i \neq k$ of $G$.  


2.2 Graph products

We need to define two graph constructions on the Cartesian product of graph vertex sets. For \( i = 1, 2 \), let \( V(G_i) \) denote the vertex set of graph \( G_i \). The sum \( G_1 + G_2 \) (terminology follows [4]) of two graphs \( G_1 \) and \( G_2 \) is defined as the graph with vertex set \( V(G_1) \times V(G_2) \) in which the vertices \((x_1, x_2)\) and \((y_1, y_2)\) are adjacent if and only if either \( x_1 = y_1 \) and \( x_2 \) is adjacent to \( y_2 \) in \( G_2 \) or if \( x_2 = y_2 \) and \( x_1 \) is adjacent to \( y_1 \) in \( G_1 \). Similarly, we define the left strong product \( G_1 \triangleright G_2 \) as the graph on vertex set \( V(G_1) \times V(G_2) \) in which the vertices \((x_1, x_2)\) and \((y_1, y_2)\) are adjacent if and only if either \( x_1 \) is adjacent to \( y_1 \) in \( G_1 \) and \( x_2 \) is adjacent to \( y_2 \) in \( G_2 \), or if \( x_2 = y_2 \) and \( x_1 \) is adjacent to \( y_1 \) in \( G_1 \). Both definitions can be readily extended to an arbitrary finite number of terms. We write \( rG \) for the \( r \) term sum \( G + \ldots + G \). Note that the sum commutes \((G + H \simeq H + G)\) whereas the left strong product need not. Finally, observe that for regular graphs \( G_1, G_2 \) the graphs \( G_1 + G_2 \) and \( G_1 \triangleright G_2 \) are regular as well.

We denote the Kronecker product of vectors \( x, y \) by \( x \otimes y \). It is formed by replacing each entry \( x_i \) of \( x \) with the block \( x_i y \).

The eigenvalues and eigenvectors for the sum and the left strong product of graphs follow readily by well known results on the so-called \( p \)-sums of graphs (see [4], Theorem 2.3.4):

**Theorem 2.2.** Given two graphs \( G_1, G_2 \) on \( s \) and \( t \) vertices, respectively, let \( \lambda_1, \ldots, \lambda_s \) and \( \mu_1, \ldots, \mu_t \) be their respective eigenvalues.

1. The eigenvalues of \( G_1 + G_2 \) are \( \lambda_i + \mu_j \) for \( i = 1, \ldots, s \) and \( j = 1, \ldots, t \). Given such an eigenvalue \( \lambda + \mu \) of \( G_1 + G_2 \), let \( x_1, \ldots, x_\alpha \) be an eigenspace basis for eigenvalue \( \lambda \) of \( G_1 \) and let \( y_1, \ldots, y_\beta \) be an eigenspace basis for eigenvalue \( \mu \) of \( G_2 \). Then the vectors \( x_i \otimes y_j, i = 1, \ldots, \alpha, j = 1, \ldots, \beta \), form a set of \( st \) linearly independent eigenvectors of \( G_1 + G_2 \).

2. The eigenvalues of \( G_1 \triangleright G_2 \) are \( \lambda_i (\mu_j + 1) \) for \( i = 1, \ldots, s \) and \( j = 1, \ldots, t \). Given such an eigenvalue \( \lambda (\mu + 1) \) of \( G_1 \triangleright G_2 \), let \( x_1, \ldots, x_\alpha \) be an eigenspace basis for eigenvalue \( \lambda \) of \( G_1 \) and let \( y_1, \ldots, y_\beta \) be an eigenspace basis for eigenvalue \( \mu \) of \( G_2 \). Then the vectors \( x_i \otimes y_j, i = 1, \ldots, \alpha, j = 1, \ldots, \beta \), form a set of \( st \) linearly independent eigenvectors of \( G_1 \triangleright G_2 \).

**Corollary 2.3.** If the eigenvalues of \( G_1 \) and \( G_2 \) are integer, then also the eigenvalues of \( G_1 + G_2 \) and \( G_1 \triangleright G_2 \) are integer. If for every eigenvalue of \( G_1 \) and \( G_2 \) there exists a simply structured eigenspace basis, then this property also holds for \( G_1 + G_2 \) and \( G_1 \triangleright G_2 \).

3 Isomorphisms of Hamming and Cayley graphs

In the 1-distance relation Hamming graph the notions of graph theoretical distance and Hamming distance coincide. Therefore, its \( r \)-th distance power is isomorphic to an \( 1, \ldots, r \)-distance relation Hamming graph.

It is not difficult to see that this graph is isomorphic to the sum \( rK_m \), where \( K_m \) is the complete graph on \( m \) vertices. The following results are derived just as easily:
Lemma 3.1. Let $1 \leq d \leq r$. Then,
\[
\begin{align*}
HG(m_1, \ldots, m_r; 1) &\simeq K_{m_1} + \ldots + K_{m_r}, \\
HG(m_1, \ldots, m_r; 1, \ldots, d) &\simeq (K_{m_1} + \ldots + K_{m_r})^{(d)}, \\
HG(m_1, \ldots, m_r; r) &\simeq HG(m_1, \ldots, m_r; 1, \ldots, r-1).
\end{align*}
\]

Theorem 3.2. Let $n$ be the product of distinct primes $p_1, \ldots, p_r$. Then,
\[
Cay(Z_n, U_n) \simeq HG(p_1, \ldots, p_r; r).
\]

Proof. Let $n = p_1 \ldots p_r$ be a square-free product of primes. We first establish a bijection between the vertex sets of $Cay(Z_n, U_n)$ and $HG(p_1, \ldots, p_r; r)$. Associate with every $x \in Z_n = \{0, 1, \ldots, n-1\}$ the vector $(x_1, \ldots, x_r)$ such that each entry $x_i$ is the residue of $x$ modulo $p_i$. This mapping is injective because otherwise the Chinese Remainder Theorem would be contradicted.

Two vertices $(x_1, \ldots, x_r)$ and $(y_1, \ldots, y_r)$ in $HG(p_1, \ldots, p_r; r)$ are adjacent if and only if $x_i - y_i \neq 0$ for all $i = 1, \ldots, r$. Viewing the entries as residues we see that this means exactly that $p_i \not| x_i - y_i$ for all $i = 1, \ldots, r$. According to the Chinese Remainder Theorem, this is equivalent to $p_i \not| x - y$. Consequently, we arrive at $\gcd(x - y, n) = 1$, which is the condition for adjacency in $Cay(Z_n, U_n)$.

Theorem 3.3. Let $m = p_1^{a_1} \ldots p_r^{a_r}$ such that the $p_i$ are the distinct prime divisors of $m$. Let $n = p_1 \ldots p_r$ and $s = \frac{m}{n}$. Then,
\[
Cay(Z_m, U_m) \simeq Cay(Z_n, U_n) \triangleright K_s.
\]

Proof. Let us revisit the proof of Theorem 3.2. We can choose $x$ e.g. from $n, \ldots, 2n - 1$ without any impact since the equations are read modulo $p_i$. Consequently, $x$ and $y$ are adjacent in $Cay(Z_m, U_m)$ if and only if for every choice of $j, k \in \{0, \ldots, s - 1\}$ the vertices $x + jn$ and $y + kn$ are adjacent. So we can extend $Cay(Z_n, U_n)$ to $Cay(Z_m, U_m)$ by forming the product $Cay(Z_n, U_n) \triangleright K_s$ and identifying each vertex $(u, v)$ of the product with the vertex $u + vn$ of $Cay(Z_m, U_m)$. Note here that the left strong product with a complete graph $K_s$ in effect means splitting each vertex of the left hand operand graph $s - 1$ times (including neighborhood).

Corollary 3.4. Use the same definitions for $m, p_i, s$ as in Theorem 3.3. Then,
\[
Cay(Z_m, U_m) \simeq (K_{p_1} + \ldots + K_{p_r})^{(r-1)} \triangleright K_s.
\]

Proof. This follows from Theorem 3.3 together with Theorem 3.2 and Lemma 3.1.

4 Eigenspace structure

We are now concerned with obtaining real basis vectors for eigenspaces, in particular with entries from the set $\{0, 1, -1\}$ only. Such a basis we call simply structured. We will show the existence of such bases for all eigenspaces of $Cay(Z_n, U_n)$.

Theorem 4.1. Let $G$ be a graph on $n$ vertices and assume that for some positive integer $d$ the adjacency matrices of the distance powers $G^{(1)}, G^{(2)}, \ldots, G^{(d)}$ are simultaneously diagonalizable by the eigenvectors $v^[1], \ldots, v^[n]$. 


Then for every positive integer \( m \) and every linearly independent set of \( m \) eigenvectors \( w^{[j]} \) of \( K_m \) the adjacency matrices of the distance powers \( H^{(1)}, H^{(2)}, \ldots, H^{(d)} \) with \( H = G + K_m \) are simultaneously diagonalizable by the eigenvectors \( v^{[i]} \otimes w^{[j]} \) for \( i = 1, \ldots, n \) and \( j = 1, \ldots, m \).

**Proof.** According to Theorem 2.2 we only need to assert that every vector \( u = v^{[i]} \otimes w^{[j]} \) is also an eigenvector of \( H^{(q)} \) for every \( 1 \leq q \leq d \). In order to test this we can conduct the multiplication of the adjacency matrix of \( H^{(q)} \) with a vector \( u \) on the graph itself. We assign the \( k \)-th component of \( u \) as a weight to the \( k \)-th vertex of \( H^{(q)} \). Then we require that some \( \lambda \) exists such that for every vertex the sum over the weight of its neighbors is equal to \( \lambda \) times its own weight.

Up to isomorphism, the graph \( H \) is formed by taking \( s \) copies of \( G \) and joining all vertices that represent the same vertex in \( G \).

Now fix a pair of vectors \( v = v^{[i]}, w = w^{[j]} \). When applying the vector \( v \otimes w \) to the vertices of \( H \) the vertices of the \( k \)-th copy of \( G \) are assigned the respective values of \( v \) multiplied with the \( k \)-th component of \( w \).

Let \( 1 \leq q \leq d \) and pick a vertex \( x \) of \( H^{(q)} \). Let \( y \) be a neighbor of \( x \) and consider a shortest path \( P \) from \( x \) to \( y \) in \( H \). Since the corresponding vertices of the copies of \( G \) are mutually connected we may assume that \( P \) starts with a number of edges joining the copies of \( G \) and then a number of edges within a single copy, altogether forming a path of length \( d \). This yields two segments \( P_1 \) and \( P_2 \) of \( P \). Clearly, the length of \( P_1 \) must be 0 or 1 because it cannot exceed the diameter of \( K_m \).

So the set of neighbors of \( x \) in \( H^{(q)} \) consists of the neighbors of \( x \) in \( G^{(q)} \) (referring to the copy of \( G \) that \( x \) belongs to), the siblings of \( x \) in the other copies of \( G \), and the neighbors of the vertices corresponding to \( x \) in \( G^{(q-1)} \) (referring to all the other copies of \( G \) in \( H \)). By assumption \( v \) is an eigenvector for the distance powers \( G^{(q)} \) and \( G^{(q-1)} \). Let the respective eigenvalues be \( \mu \) and \( \nu \).

We may assume that \( x \) lies in the first copy of \( G \) in \( H \). Further, let \( m \geq 2 \) because the case \( m = 1 \) is trivial.

Let the weight of \( x \) be non-zero. Without loss of generality we may assume that it equals one. Subsequently, the choice of \( w \) can be limited to the vectors \((1, \ldots, 1) \) and \((1, -1, 0, \ldots, 0) \) because these vectors can be extended to a set of linearly independent eigenvectors of \( K_m \) such that the added vectors all vanish on \( x \). Let \( \Sigma \) denote the respective sum over the weights of the neighbors of \( x \). Then we have \( \Sigma = \mu + (m - 1)(\nu + 1) \) if \( w = (1, \ldots, 1) \) and \( \Sigma = \mu - \nu - 1 \) if \( w = (1, -1, 0, \ldots, 0) \).

If the weight of \( x \) is zero, then without loss we may assume \( w = (0, 1, -1, 0, \ldots, 0) \). It is easily seen that the sum over the weights of the neighbors of \( x \) equals zero.

As we see, the result is independent of the particular choice of \( x \).

\[ \square \]

Let us merge the previous results into our main theorem:

**Theorem 4.2.** Both Hamming graphs \( HG(p_1, \ldots, p_r; 1, \ldots, d) \) and the unitary Cayley graphs \( Cay(\mathbb{Z}_n, U_n) \) admit simply structured bases for all eigenvalues.

**Proof.** From Corollary 3.4 and Lemma 3.1 it follows that \( Cay(\mathbb{Z}_n, U_n) \) and \( HG(p_1, \ldots, p_r; 1, \ldots, d) \) can be constructed from complete graphs by a number of certain graph operations. We only need to assert that \( K_m \) has a simply structured eigenspace basis for every eigenvalue and that this property is preserved by each applied graph operation of only the original graphs have this property.
Consider the graph $K_m$. Its eigenvalues are $-1$ and $m$. The eigenspace for eigenvalue $-1$ is spanned by the vectors
\[(1, -1, 0, \ldots, 0), (1, 0, -1, 0, \ldots, 0), \ldots, (1, 0, \ldots, 0, -1)\]
whereas the other eigenspace is spanned by the all ones vector.

Because of Corollary 2.3 the simple basis structure property is preserved for the sum and the left strong product. Lemma 2.1 asserts this for the complement of a regular graph. Theorem 4.1 guarantees that taking the distance power of a sum of complete graphs also preserves the property. Note that regularity of $(K_{p_1} + \ldots + K_{p_r})^{(r-1)}$ follows from Lemma 3.1 and Theorem 3.2.

As a consequence of Theorem 4.2 we see that considered graphs have only integer eigenvalues. For the unitary Cayley graphs this also follows from a result of W. So since the adjacency matrix of $\text{Cay}(\mathbb{Z}_n, U_n)$ is a circulant, i.e. it can be obtained from its first column by repeated downward rotation [6]. In [16] he characterizes the integral circulant graphs as those circulants on $n$ vertices whose indices (less than $n$) of ones in the first row of the associated adjacency matrix can be partitioned into complete sets of numbers that have same greatest common divisor with $n$. This condition is trivially fulfilled for unitary Cayley graphs. It is interesting to note that integral circulants play a role in quantum physics [15].

5 Acknowledgement

The author wishes to thank Walter Klotz for the fruitful discussions on Hamming and Cayley graphs.

References


