Integral Cayley graphs over Abelian groups

Here we give a character-theoretic proof of a theorem of Bridges and Mena which characterizes which Cayley graphs over abelian groups are integral (i.e. have all eigenvalues integers). Throughout we shall assume that $G$ is a multiplicative abelian group. The collection of subsets of $G$ naturally forms a boolean algebra (using $\cap$, $\cup$, and complement) and we let $\mathcal{B}(G)$ denote the boolean subalgebra generated by the subgroups of $G$.

**Theorem 1** (Bridges, Mena). $\text{Cayley}(G, S)$ is integral if and only if $S \in \mathcal{B}(G)$.

“only if”

Let $G^*$ denote the dual group of $G$, consisting of all complex characters (i.e. homomorphisms from $G$ to (the multiplicative group of) $\mathbb{C}$). It is well known that $G^*$ is a group under pointwise multiplication, and that $G^* \cong G$. We define $F$ to be the matrix indexed by $G^* \times G$ and given by the rule that for $\alpha \in G^*$ and $x \in G$ we have $F_{\alpha,x} = \alpha(x)$. Note that each row of $F$ is a character. Furthermore, it follows from the fact that the characters form an orthonormal basis that $FF^\top = I$, so $F^\top = F^{-1}$. Finally, observe that if $n$ is the exponent of $G$, then every element of $F$ is an $n^{th}$ root of unity.

We define a relation $\sim$ on $G$ by the rule that if $x, y \in G$, then $x \sim y$ if $x$ and $y$ generate the same subgroup of $G$. It follows immediately that $\sim$ is an equivalence relation. In the remainder, for any vector $v \in \mathbb{C}^I$ and any $n \in \mathbb{R}$, we let $v^n$ denote the vector in $\mathbb{C}^I$ given by $(v^n)_i = (v_i)^n$.

**Observation 2.** Let $x, y \in G$ and let $F_x, F_y$ denote the column vectors of $F$ indexed by $x$ and $y$ respectively. If $x \sim y$ then there exist integers $j, k \in \mathbb{Z}$ so that $(F_x)^j = F_y$ and $(F_y)^k = F_x$.

**Proof.** Since $x \sim y$, we may choose $j, k \in \mathbb{Z}$ so that $x^j = y$ and $y^k = x$. Now, for any character $\alpha \in G^*$ we have $\alpha(y) = \alpha(x^j) = (\alpha(x))^j$ and it follows that $F_y = (F_x)^j$. A similar argument shows that $F_x = (F_y)^k$. \qed

**Lemma 3.** Let $v \in \mathbb{Q}^G$ and $u \in \mathbb{Q}^{G^*}$ and assume that $u = Fv$. If $x, y \in G$ satisfy $x \sim y$ then $v_x = v_y$.


Proof. Let \( F_x \) and \( F_y \) denote the column vectors of \( F \) indexed by \( x \) and \( y \) and let \( \ell \) (\( m \)) be the smallest integer so that every term of \( F_x \) (\( F_y \)) is a \( \ell^{th} \) (\( m^{th} \)) root of unity. It follows from the previous observation that \( \ell = m \). Now, fix a primitive \( \ell^{th} \) root of unity \( \omega \) and express each entry of \( F_x \) and \( F_y \) in the form \( \omega^k \) for some \( k \in \{0,1,\ldots,\ell-1\} \). Using this interpretation, and observing that \( u \) is rational, we obtain an expression for the dot product of \( F_x \) and \( u \) as

\[
F_x \cdot u = \sum_{i=0}^{\ell-1} a_i \omega^i
\]

where each \( a_i \in \mathbb{Q} \). Now, let \( P(z) \in \mathbb{C}[z] \) denote the polynomial \( P(z) = \sum_{i=0}^{\ell-1} a_i z^i - v_x \). Next, choose \( j \in \{0,1,\ldots,\ell-1\} \) so that \( F_y = (F_x)^j \) and note that by our assumptions, \( j \) and \( \ell \) are relatively prime. The polynomial \( P \) has rational coefficients and has \( \omega \) as a root. It follows from this and the fact that the polynomial

\[
\Phi_{\ell}(z) = \prod_{i \in \{1,\ldots,\ell\} : \gcd(i,\ell) = 1} (z - \omega^i)
\]

is irreducible over \( \mathbb{Q} \), that \( \omega^j \) is also a root of \( P \). But then we have

\[
0 = P(\omega^j) = \sum_{i=0}^{\ell-1} a_i \omega^{ij} - v_x = F_y \cdot u - v_x
\]

which implies that \( v_y = F_y \cdot u = v_x \) as desired. \( \square \)

It is well known that for every \( S \subseteq G \) the Cayley graph \( \text{Cayley}(G, S) \) has each character \( \alpha \in G^* \) as an eigenvector with eigenvalue \( \alpha(S) = \sum_{g \in S} \alpha(g) \). Alternately, if we view \( \alpha \) as a vector and let \( 1_S \in \mathbb{C}^G \) denote the characteristic vector of \( S \), this eigenvalue may be written as \( \alpha \cdot 1_S \). Before proving the “only if” direction, we need one easy observation concerning \( \mathcal{B}(G) \) which we leave without proof.

**Observation 4.**

- The atoms of \( \mathcal{B}(G) \) are precisely the equivalence classes of \( \sim \).
- \( S \in \mathcal{B}(G) \) if and only if \( S \) is a union of equivalence classes of \( \sim \).

**Proof of Theorem 1 “only if”.** Since \( \text{Cayley}(G, S) \) is integral we must have that \( \alpha \cdot 1_S \in \mathbb{Q} \) for every \( \alpha \in G^* \). Equivalently, \( F1_S \) is rational valued. But then, it follows from the previous lemma that whenever \( x, y \in G \) satisfy \( x \sim y \) we have \( (1_S)_x = (1_S)_y \). This implies that \( S \in \mathcal{B}(G) \), as desired. \( \square \)
“if”

If $X$ is a graph on the vertex set $V$ and $B$ is a basis of $\mathbb{C}^V$ then we say that $X$ is $B$-integral if $B$ is a set of eigenvectors for $X$ and all eigenvalues of $X$ are integral. For any family of graphs $\mathcal{G}$ on a common vertex set, we let $U(\mathcal{G})$ be the closure of $\mathcal{G}$ under the operation $\cup$.

We begin with an easy lemma.

**Lemma 5.**

- If $G$ is $B$-integral and $1 \in B$, then $\overline{G}$ is $B$-integral.
- If $G$ and $G \cap H$ are $B$-integral, then $G \cap \overline{H}$ is $B$-integral.
- If $\mathcal{G}$ is an intersection-closed family of $B$-integral graphs, then $U(\mathcal{G})$ is $B$-integral.

For any set of graphs $\mathcal{G}$ on a common vertex set $V$, we let $\mathcal{B}(\mathcal{G})$ denote the set of all graphs on $V$ which may be expressed using members of $\mathcal{G}$ and the operations $\cap$, $\cup$, and complement.

**Lemma 6.** Let $\mathcal{G}$ be an intersection closed family of $B$-integral graphs and assume that $1 \in B$. Then $\mathcal{B}(\mathcal{G})$ is $B$-integral.

*Proof.* Set $\mathcal{G}_0 = \mathcal{G}$ and for every $k \in \mathbb{N}$ we recursively define

$$\mathcal{G}_{k+1} = \{X_1 \cap X_2 \cap \ldots \cap X_n : \text{either } X_i \in \mathcal{G}_k \text{ or } \overline{X_i} \in \mathcal{G}_k \text{ for every } 1 \leq i \leq n\}$$

It is immediate that each $\mathcal{G}_k$ is intersection closed and it follows from De Morgan’s law that $\mathcal{B}(\mathcal{G}) = \bigcup_{k=0}^{\infty} \mathcal{G}_k$. To complete the proof, we shall show that every graph in $\mathcal{G}_k$ is $B$-integral by induction on $k$. As a base, we observe that this holds for $k = 0$ by assumption. For the inductive step, let $X$ be a graph in $\mathcal{G}_{k+1}$ and suppose that $X = X_1 \cap X_2 \ldots \cap X_{\ell} \cap \overline{Y_1} \cap \overline{Y_2} \ldots \cap \overline{Y_m}$ where $X_1 \ldots X_{\ell}, Y_1 \ldots Y_m \in \mathcal{G}_k$. Then we have

$$X = (\cap_{i=1}^{\ell} X_i) \cap (\cup_{j=1}^{m} \overline{Y_j})$$

and it now follows from the lemma that $X$ is $B$-integral, as desired. \[\square\]

*Proof of Theorem 1 “if”.* Let $\mathcal{G} = \{\text{Cayley}(G, H) : H \leq G\}$. For every $X \in \mathcal{G}$ we have that $X$ has $G^*$ as a basis of eigenvectors, and $X$ is a disjoint union of cliques, so $X$ is $G^*$-integral.

It now follows from the theorem that $\mathcal{B}(\mathcal{G}) = \{\text{Cayley}(G, S) : S \in \mathcal{B}(G)\}$ is $G^*$-integral, and this completes the proof. \[\square\]