Integral Cayley graphs defined by greatest common divisors

Walter Klotz

Institut für Mathematik
Technische Universität Clausthal, Germany
klotz@math.tu-clausthal.de

Torsten Sander

Fakultät für Informatik
Ostfalia Hochschule für angewandte Wissenschaften, Germany
t.sander@ostfalia.de

Submitted: Dec 6, 2010; Accepted: Apr 12, 2011; Published: Apr 21, 2011
Mathematics Subject Classification: 05C25, 05C50

Abstract

An undirected graph is called integral, if all of its eigenvalues are integers. Let $\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}$ be an abelian group represented as the direct product of cyclic groups Z_{m_i} of order m_i such that all greatest common divisors $\gcd(m_i, m_j) \leq 2$ for $i \neq j$. We prove that a Cayley graph $Cay(\Gamma, S)$ over Γ is integral, if and only if $S \subseteq \Gamma$ belongs to the the Boolean algebra $B(\Gamma)$ generated by the subgroups of Γ. It is also shown that every $S \in B(\Gamma)$ can be characterized by greatest common divisors.

1 Introduction

The greatest common divisor of nonnegative integers a and b is denoted by $\gcd(a, b)$. Let us agree upon $\gcd(0, b) = b$. If $x = (x_1, \ldots, x_r)$ and $m = (m_1, ..., m_r)$ are tuples of nonnegative integers, then we set

$$\gcd(x, m) = (d_1, \ldots, d_r) = d, \quad d_i = \gcd(x_i, m_i) \text{ for } i = 1, \ldots, r.$$

For an integer $n \geq 1$ we denote by Z_n the additive group, respectively the ring of integers modulo n, $Z_n = \{0, 1, \ldots, n-1\}$ as a set. Let Γ be an (additive) abelian group represented as a direct product of cyclic groups.

$$\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}\ ,\ m_i \geq 1 \text{ for } i = 1, \ldots, r$$

Suppose that d_i is a divisor of m_i, $1 \le d_i \le m_i$, for $i = 1, \ldots, r$. For the divisor tuple $d = (d_1, \ldots, d_r)$ of $m = (m_1, \ldots, m_r)$ we define the *gcd-set* of Γ with respect to d,

$$S_\Gamma(d) \;=\; \{x = (x_1, \ldots, x_r) \in \Gamma : \gcd(x, m) = d\}.$$

If $D = \{d^{(1)}, \ldots, d^{(k)}\}$ is a set of divisor tuples of m, then the gcd-set of Γ with respect to D is

$$S_\Gamma(D) \;=\; \bigcup_{j=1}^{k} S_\Gamma(d^{(j)}).$$

In Section 2 we realize that the gcd-sets of Γ constitute a Boolean subalgebra $B_{gcd}(\Gamma)$ of the Boolean algebra $B(\Gamma)$ generated by the subgroups of Γ. The finite abelian group Γ is called a *gcd-group*, if $B_{gcd}(\Gamma) = B(\Gamma)$. We show that Γ is a gcd-group, if and only if it is cyclic or isomorphic to a group of the form

$$Z_2 \otimes \cdots \otimes Z_2 \otimes Z_n, \; n \ge 2.$$

Eigenvalues of an undirected graph G are the eigenvalues of an arbitrary adjacency matrix of G. Harary and Schwenk [8] defined G to be *integral*, if all of its eigenvalues are integers. For a survey of integral graphs see [3]. In [2] the number of integral graphs on n vertices is estimated. Known characterizations of integral graphs are restricted to certain graph classes, see e.g. [1]. Here we concentrate on integral Cayley graphs over gcd-groups.

Let Γ be a finite, additive group, $S \subseteq \Gamma$, $0 \notin S$, $-S = \{-s : \; s \in S\} = S$. The undirected *Cayley graph over* Γ *with shift set* S, $Cay(\Gamma, S)$, has vertex set Γ. Vertices $a, \; b \in \Gamma$ are adjacent, if and only if $a - b \in S$. For general properties of Cayley graphs we refer to Godsil and Royle [7] or Biggs [5]. We define a *gcd-graph* to be a Cayley graph $Cay(\Gamma, S)$ over an abelian group $\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}$ with a gcd-set S of Γ. All gcd-graphs are shown to be integral. They can be seen as a generalization of unitary Cayley graphs and of circulant graphs, which have some remarkable properties and applications (see [4], [9], [11], [15]).

In our paper [10] we proved for an abelian group Γ and $S \in B(\Gamma)$, $0 \notin S$, that the Cayley graph $Cay(\Gamma, S)$ is integral. We conjecture the converse to be true for finite abelian groups in general. This can be confirmed for cyclic groups by a theorem of So [16]. In Section 3 we extend the result of So to gcd-groups. A Cayley graph $Cay(\Gamma, S)$ over a gcd-group Γ is integral, if and only if $S \in B(\Gamma)$.

2 gcd-Groups

Throughout this section Γ denotes a finite abelian group given as a direct product of cyclic groups,

$$\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}\;, \; m_i \ge 1 \text{ for } i = 1, \ldots, r.$$

Theorem 1. *The family $B_{gcd}(\Gamma)$ of gcd-sets of Γ constitutes a Boolean subalgebra of the Boolean algebra $B(\Gamma)$ generated by the subgroups of Γ.*

Proof. First we confirm that $B_{gcd}(\Gamma)$ is a Boolean algebra with respect to the usual set operations. From $S_\Gamma(\emptyset) = \emptyset$ we know $\emptyset \in B_{gcd}(\Gamma)$. If D_0 denotes the set of all (positive) divisor tuples of $m = (m_1, \dots, m_r)$ then we have $S_\Gamma(D_0) = \Gamma$, which implies $\Gamma \in B_{gcd}(\Gamma)$. As $B_{gcd}(\Gamma)$ is obviously closed under the set operations union, intersection and forming the complement, it is a Boolean algebra.

In order to show $B_{gcd}(\Gamma) \subseteq B(\Gamma)$, it is sufficient to prove for an arbitrary divisor tuple $d = (d_1, \dots, d_r)$ of $m = (m_1, \dots, m_r)$ that

$$S_\Gamma(d) \;=\; \{x = (x_1, \dots, x_r) \in \Gamma : \gcd(x, m) = d\} \in B(\Gamma).$$

Observe that $d_j = m_j$ forces $x_j = 0$ for $x = (x_i) \in S_\Gamma(d)$. If $d_i = m_i$ for every $i = 1, \dots, r$ then $S_\Gamma(d) = \{(0, 0, \dots, 0)\} \in B(\Gamma)$. So we may assume $1 \le d_i < m_i$ for at least one $i \in \{1, \dots, r\}$. For $i = 1, \dots, r$ we define $\delta_i = d_i$, if $d_i < m_i$, and $\delta_i = 0$, if $d_i = m_i$, $\delta = (\delta_1, \dots, \delta_r)$. For $a_i \in Z_{m_i}$we denote by $[a_i]$ the cyclic group generated by a_i in Z_{m_i}. One can easily verify the following representation of $S_\Gamma(d)$:

$$S_\Gamma(d) \;=\; [\delta_1] \otimes \cdots \otimes [\delta_r] \setminus \bigcup_{\lambda_1, \dots, \lambda_r} ([\lambda_1 \delta_1] \otimes \cdots \otimes [\lambda_r \delta_r]). \tag{1}$$

In (1) we set $\lambda_i = 0$, if $\delta_i = 0$. For $i \in \{1, \dots, r\}$ and $\delta_i > 0$ the range of λ_i is

$$1 \le \lambda_i < \frac{m_i}{\delta_i} \text{ such that } \gcd(\lambda_i, \frac{m_i}{\delta_i}) > 1 \text{ for at least one } i \in \{1, \dots, r\}.$$

As $[\delta_1] \otimes \cdots \otimes [\delta_r]$ and $[\lambda_1 \delta_1] \otimes \cdots \otimes [\lambda_r \delta_r]$ are subgroups of Γ, (1) implies $S_\Gamma(d) \in B(\Gamma)$. □

A gcd-graph is a Cayley graph $Cay(\Gamma, S_\Gamma(D))$ over an abelian group $\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}$ with a gcd-set $S_\Gamma(D)$ as its shift set. In [10] we proved that for a finite abelian group Γ and $S \in B(\Gamma)$, $0 \notin S$, the Cayley graph $Cay(\Gamma, S)$ is integral. Therefore, Theorem 1 implies the following corollary.

Corollary 1. *Every gcd-graph $Cay(\Gamma, S_\Gamma(D))$ is integral.*

We remind that we call Γ a gcd-group, if $B_{gcd}(\Gamma) = B(\Gamma)$. For $a = (a_i) \in \Gamma$ we denote by $[a]$ the cyclic subgroup of Γ generated by a.

Lemma 1. *Let Γ be the abelian group $Z_{m_1} \otimes \cdots \otimes Z_{m_r}$, $m = (m_1, \dots, m_r)$. Then Γ is a gcd-group, if and only if for every $a \in \Gamma$, $\gcd(a, m) = d$ implies $S_\Gamma(d) \subseteq [a]$.*

Proof. Let Γ be a gcd-group, $B_{gcd}(\Gamma) = B(\Gamma)$. Then every subgroup of Γ, especially every cyclic subgroup $[a]$ is a gcd-set of Γ. This means $[a] = S_\Gamma(D)$ for a set D of divisor tuples of m. Now $\gcd(a, m) = d$ implies $d \in D$ and therefore $S_\Gamma(d) \subseteq S_\Gamma(D) = [a]$.

To prove the converse assume that the condition in Lemma 1 is satisfied. Let H be an arbitrary subgroup of Γ. We show $H \in B_{gcd}(\Gamma)$. Let $a \in H$, $\gcd(a, m) = d$. Then our assumption implies

$$a \in S_\Gamma(d) \subseteq [a] \subseteq H, \quad H = \bigcup_{d \in D} S_\Gamma(d) = S_\Gamma(D) \in B_{gcd}(\Gamma),$$

where $D = \{\gcd(a, m) : \; a \in H\}$. □

For integers x, y, n we express by $x \equiv y \mod n$ that x is congruent to y modulo n.

Lemma 2. *Every cyclic group* $\Gamma = Z_n,\ n \geq 1$, *is a gcd-group.*

Proof. As the lemma is trivially true for $n = 1$, we assume $n \geq 2$. Let $a \in \Gamma$, $0 \leq a \leq n-1$, $\gcd(a, n) = d$. According to Lemma 1 we have to show $S_\Gamma(d) \subseteq [a]$. Again, to avoid the trivial case, assume $a \geq 1$. From $\gcd(a, n) = d < n$ we deduce

$$a = \alpha d,\ 1 \leq \alpha < \frac{n}{d},\ \gcd(\alpha, \frac{n}{d}) = 1.$$

As the order of $a \in \Gamma$ is $ord(a) = n/d$, the cyclic group generated by a is

$$[a] = \{x \in \Gamma :\ x \equiv (\lambda\alpha)d \mod n,\ 0 \leq \lambda < \frac{n}{d}\}.$$

Finally, we conclude

$$\begin{aligned} [a] &\supseteq \{x \in \Gamma :\ x \equiv (\lambda\alpha)d \mod n,\ 0 \leq \lambda < \frac{n}{d},\ \gcd(\lambda, \frac{n}{d}) = 1\} \\ &= \{x \in \Gamma :\ x \equiv \mu d \mod n,\ 0 \leq \mu < \frac{n}{d},\ \gcd(\mu, \frac{n}{d}) = 1\} = S_\Gamma(d). \end{aligned}$$

□

Lemma 3. *If* $\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r},\ r \geq 2$, *is a gcd-group, then* $\gcd(m_i, m_j) \leq 2$ *for every* $i \neq j,\ i, j = 1, \ldots, r$.

Proof. Without loss of generality we concentrate on $\gcd(m_1, m_2)$. We may assume $m_1 > 2$ and $m_2 > 2$. Consider $a = (1, 1, 0, \ldots, 0) \in \Gamma$ and $b = (m_1 - 1, 1, 0, \ldots, 0) \in \Gamma$. For $m = (m_1, \ldots, m_r)$ we have

$$\gcd(a, m) = (1, 1, m_3, \ldots, m_r) = \gcd(b, m).$$

By Lemma 1 the element b must belong to the cyclic group $[a]$. This requires the existence of an integer λ, $b = \lambda a$ in Γ, or equivalently

$$\lambda \equiv -1 \mod m_1 \text{ and } \lambda \equiv 1 \mod m_2.$$

Therefore, integers k_1 and k_2 exist satisfying $\lambda = -1 + k_1 m_1$ and $\lambda = 1 + k_2 m_2$, which implies $k_1 m_1 - k_2 m_2 = 2$ and $\gcd(m_1, m_2)$ divides 2. □

The next two lemmas will enable us to prove the converse of Lemma 3.

Lemma 4. *Let* $a_1, \ldots, a_r, g_1, \ldots, g_r$ *be integers,* $r \geq 2$, $g_i \geq 2$ *for* $i = 1, \ldots, r$. *Moreover, assume* $\gcd(g_i, g_j) = 2$ *for every* $i \neq j$, $i, j = 1, \ldots, r$. *The system of congruences*

$$x \equiv a_1 \mod g_1, \ldots, x \equiv a_r \mod g_r \tag{2}$$

is solvable, if and only if

$$a_i \equiv a_j \mod 2 \text{ for every } i, j = 1, \ldots, r. \tag{3}$$

If the system is solvable, then the solution consists of a unique residue class modulo $(g_1 g_2 \cdots g_r)/2^{r-1}$.

Proof. Suppose that x is a solution of (2). As every g_i is even, the necessity of condition (3) follows by

$$a_i \equiv x \mod 2 \text{ for } i = 1, \ldots, r.$$

Assume now that condition (3) is satisfied. We set $\kappa = 0$, if every a_i is even, and $\kappa = 1$, if every a_i is odd. By $x \equiv a_i \mod 2$ we have $x = 2y + \kappa$ for an integer y. The congruences (2) can be equivalently transformed to

$$y \equiv \frac{a_1 - \kappa}{2} \mod \frac{g_1}{2}, \ldots, y \equiv \frac{a_r - \kappa}{2} \mod \frac{g_r}{2}. \tag{4}$$

As $\gcd((g_i/2), (g_j/2)) = 1$ for $i \neq j$, $i, j = 1, \ldots, r$, we know by the Chinese remainder theorem [14] that the system (4) has a unique solution $y \equiv h \mod (g_1 \cdots g_r)/2^r$. This implies for the solution x of (2):

$$x = 2y + \kappa \equiv 2h + \kappa \mod \frac{g_1 \cdots g_r}{2^{r-1}}.$$

□

Lemma 5. *Let $a_1, \ldots, a_r, m_1, \ldots, m_r$ be integers, $r \geq 2$, $m_i \geq 2$ for $i = 1, \ldots, r$. Moreover, assume* $\gcd(m_i, m_j) \leq 2$ *for every $i \neq j$, $i, j = 1, \ldots, r$. The system of congruences*

$$x \equiv a_1 \mod m_1, \ldots, x \equiv a_r \mod m_r \tag{5}$$

is solvable, if and only if

$$a_i \equiv a_j \mod 2 \text{ for every } i \neq j,\ m_i \equiv m_j \equiv 0 \mod 2,\ i, j = 1, \ldots, r. \tag{6}$$

Proof. If at most one of the integers m_i, $i = 1, \ldots r$, is even then $\gcd(m_i, m_j) = 1$ for every $i \neq j$, $i, j = 1, \ldots, r$, and system (5) is solvable. Therefore, we may assume that $m_1, \ldots, m_k$ are even, $2 \leq k \leq r$, and $m_{k+1}, \ldots, m_r$ are odd, if $k < r$. Now we split system (5) into two systems.

$$x \equiv a_1 \mod m_1, \ldots, x \equiv a_k \mod m_k \tag{7}$$

$$x \equiv a_{k+1} \mod m_{k+1}, \ldots, x \equiv a_r \mod m_r \tag{8}$$

By Lemma 4 the solvability of (7) requires (6). If this condition is satisfied, then (7) has a unique solution $x \equiv b \mod (m_1 \cdots m_k)/2^{k-1}$ by Lemma 4. System (8) has a unique solution $x \equiv c \mod (m_{k+1} \cdots m_r)$ by the Chinese remainder theorem, because $\gcd(m_i, m_j) = 1$ for $i \neq j$, $i, j = k + 1, \ldots, r$. So the original system (5) is equivalent to

$$x \equiv b \mod \frac{m_1 \cdots m_k}{2^{k-1}} \text{ and } x \equiv c \mod (m_{k+1} \cdots m_r). \tag{9}$$

As $\gcd((m_1 \cdots m_k), (m_{k+1} \cdots m_r)) = 1$, the Chinese remainder theorem can be applied once more to arrive at a unique solution $x \equiv h \mod (m_1 \cdots m_r)/2^{k-1}$ of (9) and (5). □

Theorem 2. *The abelian group $\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}$ is a gcd-group, if and only if*

$$\gcd(m_i, m_j) \leq 2 \text{ for every } i \neq j,\ i, j = 1, \ldots, r. \tag{10}$$

Proof. As every cyclic group is a gcd-group by Lemma 2, we may assume $r \geq 2$. Then (10) necessarily holds for every gcd-group Γ by Lemma 3.

Suppose now that Γ satisfies (10). Let $a = (a_1, \ldots, a_r)$ and $b = (b_1, \ldots, b_r)$ be elements of Γ, $m = (m_1, \ldots, m_r)$, and

$$\gcd(a, m) = d = (d_1, \ldots, d_r) = \gcd(b, m). \tag{11}$$

According to Lemma 1 we have to show that b belongs to the cyclic group $[a]$ generated by a. Now $b \in [a]$ is equivalent to the existence of an integer λ which solves the following system of congruences:

$$b_1 \equiv \lambda a_1 \mod m_1, \ldots, b_r \equiv \lambda a_r \mod m_r. \tag{12}$$

If $d_i = m_i$ then $a_i = b_i = 0$ and the congruence $b_i \equiv \lambda a_i \mod m_i$ becomes trivial. Therefore, we assume $1 \leq d_i < m_i$ for every $i = 1, \ldots, r$. By (11) we have $\gcd(a_i, m_i) = \gcd(b_i, m_i) = d_i$, which implies the existence of integers μ_i, ν_i satisfying

$$a_i = \mu_i d_i,\ 1 \leq \mu_i < \frac{m_i}{d_i},\ \gcd(\mu_i, \frac{m_i}{d_i}) = 1;\ \ b_i = \nu_i d_i,\ 1 \leq \nu_i < \frac{m_i}{d_i},\ \gcd(\nu_i, \frac{m_i}{d_i}) = 1. \tag{13}$$

Inserting a_i and b_i for $i = 1, \ldots, r$ from (13) in (12) yields

$$\nu_1 d_1 \equiv \lambda \mu_1 d_1 \mod m_1, \ldots, \nu_r d_r \equiv \lambda \mu_r d_r \mod m_r.$$

We divide the i-th congruence by d_i and multiply with κ_i, the multiplicative inverse of μ_i modulo m_i/d_i. Thus each congruence is solved for λ and we arrive at the following system equivalent to (12).

$$\lambda \equiv \kappa_1 \nu_1 \mod \frac{m_1}{d_1}, \ldots, \lambda \equiv \kappa_r \nu_r \mod \frac{m_r}{d_r} \tag{14}$$

To prove the solvability of (14) by Lemma 5 we first notice that $\gcd(m_i, m_j) \leq 2$ for $i \neq j$ implies $\gcd((m_i/d_i), (m_j/d_j)) \leq 2$ for $i, j = 1, \ldots, r$. Suppose now that m_i/d_i is even. As $\gcd(\mu_i, (m_i/d_i)) = 1$, see (13), μ_i must be odd. Also κ_i is odd because of $\gcd(\kappa_i, (m_i/d_i)) = 1$. If for $i \neq j$ both m_i/d_i and m_j/d_j are even, then both $\kappa_i \nu_i$ and $\kappa_j \nu_j$ are odd, because all involved integers κ_i, ν_i, κ_j, ν_j are odd. We conclude now by Lemma 5 that (14) is solvable, which finally confirms $b \in [a]$. □

Lemma 6. *Let $\Gamma = Z_{m_1} \otimes \cdots \otimes Z_{m_r}$ be isomorphic to $\Gamma' = Z_{n_1} \otimes \cdots \otimes Z_{n_s}$, $\Gamma \simeq \Gamma'$. Then Γ is a gcd-group, if and only if Γ' is a gcd-group.*

Proof. We may assume $m_i \geq 2$ for $i = 1, \ldots, r$ and $n_j \geq 2$ for $j = 1, \ldots, s$. For the following isomorphy and more basic facts about abelian groups we refer to Cohn [6].

$$Z_{pq} \simeq Z_p \otimes Z_q,\ \text{if}\ \gcd(p, q) = 1 \tag{15}$$

If the positive integer m is written as a product of pairwise coprime prime powers, $m = u_1 \cdots u_h$, then

$$Z_m \simeq Z_{u_1} \otimes \cdots \otimes Z_{u_h}. \tag{16}$$

We apply the decomposition (16) to every factor $Z_{m_i},\ i = 1, \ldots, r$, of Γ and to every factor $Z_{n_j},\ j = 1, \ldots, s$, of Γ'. So we obtain the "prime power representation" Γ^*, which is the same for Γ and for Γ', if the factors are e. g. arranged in ascending order.

$$\Gamma \simeq \Gamma^* = Z_{q_1} \otimes \cdots \otimes Z_{q_t} \simeq \Gamma',\ q_j \text{ a prime power for } j = 1, \ldots, t$$

The following equivalences are easily checked.

$$\begin{aligned} & \gcd(m_i, m_j) \le 2 \text{ for every } i \ne j,\ i, j = 1, \ldots, r \\ \Leftrightarrow\quad & \gcd(q_k, q_l) \le 2 \text{ for every } k \ne l,\ k, l = 1, \ldots, t \\ \Leftrightarrow\quad & \gcd(n_i, n_j) \le 2 \text{ for every } i \ne j,\ i, j = 1, \ldots, s \end{aligned} \tag{17}$$

Theorem 2 and (17) imply that Γ is a gcd-group, if and only if Γ^*, respectively Γ', is a gcd-group. □

Every finite abelian group $\tilde{\Gamma}$ can be represented as the direct product of cyclic groups.

$$\tilde{\Gamma} \simeq Z_{m_1} \otimes \cdots \otimes Z_{m_r} = \Gamma \tag{18}$$

We define $\tilde{\Gamma}$ to be a gcd-group, if Γ is a gcd-group. Although the representation (18) may not be unique, this definition is correct by Lemma 6.

Theorem 3. *The finite abelian group Γ is a gcd-group, if and only if Γ is cyclic or Γ is isomorphic to a group Γ' of the form*

$$\Gamma' = Z_2 \otimes \cdots \otimes Z_2 \otimes Z_n,\ n \ge 2.$$

Proof. If Γ is isomorphic to a group Γ' as stated in the theorem, then Γ is a gcd-group by Theorem 2.

To prove the converse, let Γ be a gcd-group. We may assume that Γ is not cyclic. The prime power representation Γ^* of Γ is established as described in the proof of Lemma 6. We start this representation with those orders which are a power of 2, followed possibly by odd orders.

$$\Gamma \simeq \Gamma^* = Z_2 \otimes \cdots \otimes Z_2 \otimes Z_{2^\alpha} \otimes Z_{u_1} \otimes \cdots \otimes Z_{u_s},\quad \alpha \ge 1,\ u_i \text{ odd for } i = 1, \ldots, s \tag{19}$$

Theorem 2 implies that there is at most one order 2^α with $\alpha \ge 2$. Moreover, all odd orders $u_1, \ldots, u_s$ must be pairwise coprime. As $2^\alpha, u_1, \ldots, u_s$ are pairwise coprime integers, we deduce from (15) that

$$Z_{2^\alpha} \otimes Z_{u_1} \otimes \cdots \otimes Z_{u_s} \simeq Z_n \text{ for } n = 2^\alpha u_1 \cdots u_s.$$

Now (19) implies

$$\Gamma \simeq \Gamma' = Z_2 \otimes \cdots \otimes Z_2 \otimes Z_n.$$

□

3 Integral Cayley graphs over gcd-groups

The following method to determine the eigenvectors and eigenvalues of Cayley graphs over abelian groups is due to Lovász [13], see also our description in [10]. We outline the main features of this method, which will be applied in this section.

The finite, additive, abelian group $\Gamma,\ |\Gamma| = n \geq 2$, is represented as the direct product of cyclic groups,

$$\Gamma \ = \ Z_{m_1} \otimes \cdots \otimes Z_{m_r},\ m_i \geq 2 \text{ for } 1 \leq i \leq r. \tag{20}$$

We consider the elements $x \in \Gamma$ as elements of the cartesian product $Z_{m_1} \times \cdots \times Z_{m_r}$,

$$x = (x_i),\ x_i \in Z_{m_i} = \{0, 1, \ldots, m_i - 1\},\ 1 \leq i \leq r.$$

Addition is coordinatewise modulo m_i. A *character* ψ of Γ is a homomorphism from Γ into the multiplicative group of complex n-th roots of unity. Denote by e_i the unit vector with entry 1 in position i and entry 0 in every position $j \neq i$. A character ψ of Γ is uniquely determined by its values $\psi(e_i),\ 1 \leq i \leq r$.

$$x = (x_i) \ = \ \sum_{i=1}^{r} x_i e_i, \quad \psi(x) \ = \ \prod_{i=1}^{r} (\psi(e_i))^{x_i} \tag{21}$$

The value of $\psi(e_i)$ must be an m_i-th root of unity. There are m_i possible choices for this value. Let ζ_i be a fixed primitive m_i-th root of unity for every $i,\ 1 \leq i \leq r$. For every $\alpha = (\alpha_i) \in \Gamma$ a character ψ_α can be uniquely defined by

$$\psi_\alpha(e_i) \ = \ \zeta_i^{\alpha_i},\ 1 \leq i \leq r. \tag{22}$$

Combining (21) and (22) yields

$$\psi_\alpha(x) \ = \ \prod_{i=1}^{r} \zeta_i^{\alpha_i x_i} \quad \text{for } \alpha = (\alpha_i) \in \Gamma \text{ and } x = (x_i) \in \Gamma. \tag{23}$$

Thus all $|\Gamma| = m_1 \cdots m_r = n$ characters of the abelian group Γ can be obtained.

Lemma 7. *Let $\psi_0, \ldots, \psi_{n-1}$ be the distinct characters of the additive abelian group $\Gamma = \{w_0, \ldots, w_{n-1}\},\ S \subseteq \Gamma,\ 0 \notin S,\ -S = S$. Assume that $A(G) = A = (a_{i,j})$ is the adjacency matrix of $G = Cay(\Gamma, S)$ with respect to the given ordering of the vertex set $V(G) = \Gamma$.*

$$a_{i,j} \ = \ \begin{cases} 1, & \text{if } w_i \text{ is adjacent to } w_j \\ 0, & \text{if } w_i \text{ and } w_j \text{ are not adjacent} \end{cases},\ 0 \leq i \leq n-1,\ 0 \leq j \leq n-1$$

Then the vectors $(\psi_i(w_j))_{j=0,\ldots,n-1},\ 0 \leq i \leq n-1$, represent an orthogonal basis of $\mathbb{C}^n$ consisting of eigenvectors of A. To the eigenvector $(\psi_i(w_j))_{j=0,\ldots,n-1}$ belongs the eigenvalue

$$\psi_i(S) = \sum_{s \in S} \psi_i(s).$$

There is a unique character ψ_{w_i} associated with every $w_i \in \Gamma$ according to (23). So we may assume in Lemma 7 that $\psi_i = \psi_{w_i}$ for $i = 0, \ldots, n-1$. Let us call the $n \times n$-matrix

$$H(\Gamma) = (\psi_{w_i}(w_j)),\ 0 \le i \le n-1,\ 0 \le j \le n-1,$$

the *character matrix* of Γ with respect to the given ordering of the elements of Γ. Here we always assume that Γ is represented by (20) as a direct product of cyclic groups and that the elements of Γ are ordered lexicographically increasing. Then w_0 is the zero element of Γ. Moreover, by (23) the character matrix $H(\Gamma)$ becomes the Kronecker product of the character matrices of the cyclic factors of Γ,

$$\Gamma \;=\; Z_{m_1} \otimes \cdots \otimes Z_{m_r} \text{ implies } H(\Gamma) = H(Z_{m_1}) \otimes \cdots \otimes H(Z_{m_r}). \tag{24}$$

We remind that the Kronecker product $A \otimes B$ of matrices A and B is defined by replacing the entry $a_{i,j}$ of A by $a_{i,j}B$ for all i, j. For every Cayley graph $G = Cay(\Gamma, S)$ the rows of $H(\Gamma)$ represent an orthogonal basis of $\mathbb{C}^n$ consisting of eigenvectors of G, respectively $A(G)$. The corresponding eigenvalues are obtained by $H(\Gamma)c_{S,\Gamma}$, the product of $H(\Gamma)$ and the characteristic (column) vector $c_{S,\Gamma}$ of S in Γ,

$$c_{S,\Gamma}(i) \;=\; \begin{cases} 1, & \text{if } w_i \in S \\ 0, & \text{if } w_i \notin S \end{cases} \;,\ 0 \le i \le n-1.$$

Consider the situation, when Γ is a cyclic group, $\Gamma = Z_n,\ n \ge 2$. Let ω_n be a primitive n-th root of unity. Setting $r = 1$ and $\zeta_1 = \omega_n$ in (23) we establish the character matrix $H(Z_n) = F_n$ according to the natural ordering of the elements $0, 1, \ldots, n-1$.

$$F_n = ((\omega_n)^{ij}),\ 0 \le i \le n-1,\ 0 \le j \le n-1$$

Observe that all entries in the first row and in the first column of F_n are equal to 1. For a divisor δ of $n,\ 1 \le \delta \le n$, we simplify the notation of the characteristic vector of the gcd-set $S_{Z_n}(\delta)$ in Z_n to $c_{\delta,n}$,

$$c_{\delta,n}(i) \;=\; \begin{cases} 1, & \text{if } \gcd(i,n) = \delta \\ 0, & \text{otherwise} \end{cases} \;,\ 0 \le i \le n-1.$$

For $\delta < n$ we have $0 \notin S_{Z_n}(\delta)$. So the Cayley graph $Cay(Z_n, S_{Z_n}(\delta))$ is well defined. It is integral by Corollary 1. The eigenvalues of this graph are the entries of $F_n c_{\delta,n}$. Therefore, this vector is integral, which is also trivially true for $\delta = n$,

$$F_n c_{\delta,n} \in Z^n \text{ for every positive divisor } \delta \text{ of } n. \tag{25}$$

The only quadratic primitive root is -1. This implies that $H(Z_2) = F_2$ is the elementary Hadamard matrix (see [12])

$$F_2 \;=\; \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} .$$

By (24) the character matrix of the r-fold direct product $Z_2 \otimes \cdots \otimes Z_2 = Z_2^r$ is

$$H(Z_2^r) \;=\; F_2 \otimes \cdots \otimes F_2 \;=\; F_2^{(r)},$$

the r-fold Kronecker product of F_2 with itself, which is also a Hadamard matrix consisting of orthogonal rows with entries ± 1.

From now on let Γ be a gcd-group. By Theorem 3 we may assume

$$\Gamma \;=\; Z_2^r \otimes Z_n,\;\; r \geq 0,\;\; n \geq 2. \tag{26}$$

If we set $p = n-1$ and $q = 2^r - 1$, then we have $|\Gamma| - 1 = 2^r n - 1 = qn + p$. We order the elements of Z_2^r, and Γ lexicographically increasing.

$$\begin{array}{l} Z_2^r \;=\; \{a_0, a_1, \ldots, a_q\}, \\ a_0 = (0,\ldots,0,0),\;\; a_1 = (0,\ldots,0,1),\;\; \ldots\;\; , a_q = (1,\ldots,1,1); \\ \Gamma \;=\; \{w_0, w_1, \ldots, w_{qn+p}\}, \\ w_0 = (a_0,0),\;\; w_1 = (a_0,1), \ldots,\;\; w_p = (a_0,p), \\ \cdots\cdots \\ w_{qn} = (a_q,0),\;\; w_{qn+1} = (a_q,1), \ldots,\;\; w_{qn+p} = (a_q,p). \end{array} \tag{27}$$

The character matrix $H(\Gamma)$ with respect to the given ordering of elements becomes the Kronecker product of the character matrix $F_2^{(r)}$ of Z_2^r and the character matrix F_n of Z_n,

$$H(\Gamma) \;=\; F_2^{(r)} \otimes F_n.$$

This means that $H(\Gamma)$ consists of disjoint submatrices $\pm F_n$, because $F_2^{(r)}$ has only entries ± 1. The structure of $H(\Gamma)$ is displayed in Figure 1. Rows and columns are labelled with the elements of Γ. Observe that a label α at a row stands for the unique character ψ_α. The sign $\epsilon(j,l) \in \{1,-1\}$ of a submatrix F_n is the entry of $F_2^{(r)}$ in position $(j,l),\; 0 \leq j \leq q,\; 0 \leq l \leq q$.

	$(a_0,0)\cdots(a_0,p)$	$\cdots$	$(a_l,0)\cdots(a_l,p)$	$\cdots$	$(a_q,0)\cdots(a_q,p)$
$(a_0,0)$		$\cdots$		$\cdots$	
$\cdots$	$\epsilon(0,0)F_n$	$\cdots$	$\epsilon(0,l)F_n$	$\cdots$	$\epsilon(0,q)F_n$
(a_0,p)		$\cdots$		$\cdots$	
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(a_j,0)$		$\cdots$		$\cdots$	
$\cdots$	$\epsilon(j,0)F_n$	$\cdots$	$\epsilon(j,l)F_n$	$\cdots$	$\epsilon(j,q)F_n$
(a_j,p)		$\cdots$		$\cdots$	
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(a_q,0)$		$\cdots$		$\cdots$	
$\cdots$	$\epsilon(q,0)F_n$	$\cdots$	$\epsilon(q,l)F_n$	$\cdots$	$\epsilon(q,q)F_n$
(a_q,p)		$\cdots$		$\cdots$	

Figure 1: The structure of $H(Z_2^r \otimes Z_n)$.

Let $m = (m_1, \ldots, m_r, m_{r+1}),\ m_1 = \ldots = m_r = 2,\ m_{r+1} = n$. Suppose that $d = (d_1, \ldots, d_{r+1})$ is a tuple of positive divisors of $m_1, \ldots, m_{r+1},\ d_i \in \{1, 2\}$ for $i = 1, \ldots, r$, $d_{r+1} = \delta$ divides n. If $x = (x_1, \ldots, x_{r+1}) \in \Gamma = Z_2^r \otimes Z_n$ and $\gcd(x, m) = d$, then $x_1, \ldots, x_r$ are uniquely determined,

$$x_i \ = \ \begin{cases} 1, \text{ if } d_i = 1 \\ 0, \text{ if } d_i = 2 \end{cases} \quad \text{for } i = 1, \ldots, r.$$

This means that the divisor tuple d of m determines a unique element $a_l \in Z_2^r$ such that

$$\begin{aligned} S_\Gamma(d) \ &= \ \{(a_l, b) :\ b \in Z_n,\ \ \gcd(b, n) = \delta\} \\ &= \ \{w_i \in \Gamma :\ i = ln + b,\ 0 \le b \le p = n - 1,\ \ \gcd(b, n) = \delta\}. \end{aligned}$$

The characteristic vector $c_{d,\Gamma}$ of $S_\Gamma(d)$ in Γ may have nonzero entries only for positions $i = ln + b,\ b \in Z_n$. Its restriction to these positions is $x_{\delta,n}$, the characteristic vector of $S_{Z_n}(\delta)$ in Z_n. The vector $H(\Gamma)c_{d,\Gamma}$ is composed of 2^r disjoint vectors $\pm F_n c_{\delta,n}$, which by (25) have only integral entries. So $H(\Gamma)c_{d,\Gamma}$ has also only integral entries,

$$H(\Gamma)c_{d,\Gamma} \in Z^{|\Gamma|} \text{ for every divisor tuple } d \text{ of } m. \tag{28}$$

For different divisor tuples $d^{(1)}, \ldots, d^{(k)}$ of m the sets of positions of $c_{d^{(1)},\Gamma}, \ldots, c_{d^{(k)},\Gamma}$ with entries 1 are pairwise disjoint. Therefore, these vectors are linearly independent in the rational space $\mathbb{Q}^{|\Gamma|}$.

From now on we abbreviate $H(\Gamma) = H,\ H = (h_{\alpha,\beta}),\ 0 \le \alpha \le |\Gamma| - 1,\ 0 \le \beta \le |\Gamma| - 1$. We continue to use the notation established for (27). By $\tilde{D}$ we denote the set of all positive divisor tuples of $m = (2, \ldots, 2, n)$. The transpose of a vector v is v^T. It is easily verified that

$$\mathcal{A} \ = \ \{v \in \mathbb{Q}^{|\Gamma|} :\ Hv \in \mathbb{Q}^{|\Gamma|}\}$$

is a subspace of the rational space $\mathbb{Q}^\Gamma$. By (28) we see that

$$\mathcal{D} = \operatorname{span}\{c_{d,\Gamma} :\ d \in \tilde{D}\} \ \subseteq \ \mathcal{A}. \tag{29}$$

As $\{c_{d,\Gamma} :\ \ d \in \tilde{D}\}$ is a basis of $\mathcal{D}$, we have $\dim(\mathcal{D}) = |\tilde{D}| = 2^r\tau(n)$, where $\tau(n)$ is the number of positive divisors of n. The next lemma will enable us to show $\mathcal{D} = \mathcal{A}$.

Lemma 8. *Let the elements of* $\Gamma = Z^r \otimes Z_n$ *be ordered as in (27),* $\Gamma = \{w_0, \ldots, w_{qn+p}\}$, $q = 2^r - 1,\ p = n - 1$, *and let the character matrix* $H = (h_{\alpha,\beta})$ *of* Γ *be established with respect to this ordering of the elements (Figure 1). Moreover, let* $v = (v_0, \ldots, v_{qn+p})^T \in \mathcal{A}$, $u = (u_0, \ldots, u_{qn+p})^T = Hv$. *Then*

$$\gcd(w_s, m) = \gcd(w_t, m) \ \textit{implies}\ u_s = u_t \ \textit{for every}\ s, t \in \{0, 1, \ldots, qn + p\}.$$

Proof. Notice that $v \in \mathcal{A}$ and $u = Hv$ implies that the entries of v and u are rationals. Suppose $\gcd(w_s, m) = \gcd(w_t, m) = d,\ d = (d_1, \ldots, d_{r+1}),\ d_i \in \{1, 2\}$ for $i = 1, \ldots, r$,

$d_{r+1} = \delta$ a positive divisor of n. As explained earlier, d uniquely determines elements $a_l \in Z_2^r$ and $b_1, b_2 \in Z_n$ such that

$$w_s = (a_l, b_1),\ w_t = (a_l, b_2),\ s = ln + b_1,\ t = ln + b_2,\ \gcd(b_1, n) = \gcd(b_2, n) = \delta. \quad (30)$$

Rows s and t of H belong to the same row of submatrices $\epsilon(l, g)F_n$, $0 \leq g \leq q$ in Figure 1. We remind that $F_n = (\omega_n^{ij})$, ω_n a primitive n-th root of unity, $0 \leq i \leq p$, $0 \leq j \leq p$, $p = n - 1$.

$$u_s = \sum_{k=0}^{qn+p} h_{s,k} v_k = \sum_{g=0}^{q} \sum_{f=0}^{p} h_{ln+b_1, gn+f}\ v_{gn+f}\ ,$$

$$u_s = \sum_{g=0}^{q} \epsilon(l, g) \sum_{f=0}^{p} \omega_n^{b_1 f}\ v_{gn+f}\ . \quad (31)$$

Similarly we deduce

$$u_t = \sum_{g=0}^{q} \epsilon(l, g) \sum_{f=0}^{p} \omega_n^{b_2 f}\ v_{gn+f}\ . \quad (32)$$

Setting $\omega_n^{b_1} = x$ in (31) shows that $\omega_n^{b_1}$ is a root of the rational polynomial

$$\psi(x) = \sum_{g=0}^{q} \epsilon(l, g) \sum_{f=0}^{p} x^f\ v_{gn+f} - u_s.$$

As $\gcd(b_1, n) = \delta$ by (30), we know that $\omega_n^{b_1}$ is an $(n/\delta) = \delta'$-th root of unity. The irreducible polynomial over the rationals for a δ'-th root of unity is the cyclotomic polynomial $\Phi_{\delta'}$ (see [6]). Therefore, we have $\psi(x) = M(x)\Phi_{\delta'}(x)$ with a rational polynomial $M(x)$. Now we see by (30), $\gcd(b_2, n) = \delta$, that $\omega_n^{b_2}$ is also a δ'-th root of unity. So $\omega_n^{b_2}$ is also a root of $\Phi_{\delta'}(x)$ and consequently also of $\psi(x)$.

$$\psi(\omega_n^{b_2}) = \sum_{g=0}^{q} \epsilon(l, g) \sum_{f=0}^{p} \omega_n^{b_2 f}\ v_{gn+f} - u_s = 0.$$

Finally, (32) implies $u_s = u_t$. □

Corollary 2. *Assume that the conditions of Lemma 8 are satisfied. Let $\tilde{D}$ be the set of all positive divisor tuples of $m = (2, \ldots, 2, n)$. For $d \in \tilde{D}$ denote by $c_{d,\Gamma}$ the characteristic vector of $S_\Gamma(d) = \{w \in \Gamma :\ \gcd(w, m) = d\}$ in Γ, $\mathcal{D} = span\{c_{d,\Gamma} :\ d \in \tilde{D}\}$. Then we have*

$$u = Hv \in \mathcal{D} \text{ for every } v \in \mathcal{A}.$$

Proof. Suppose $d \in \tilde{D}$. By Lemma 8 the vector $u = Hv$ has the same entry λ_d in every position j, $w_j \in S_\Gamma(d)$. The sets $S_\Gamma(d)$, $d \in \tilde{D}$ induce a partition of the set of all possible positions $\{0, 1, \ldots, |\Gamma| - 1\} = Z_{|\Gamma|}$ into disjoint subsets.

$$S_{|\Gamma|} = \bigcup_{d \in \tilde{D}} \{j \in Z_{|\Gamma|} :\ w_j \in S_\Gamma(d)\}$$

This implies

$$u \;=\; \sum_{d\in\tilde{D}} \lambda_d c_{d,\Gamma} \;\in \mathcal{D}.$$

□

Lemma 9. *With the notations introduced for Lemma 8 and its corollary we have $\mathcal{D} = \mathcal{A}$.*

Proof. By (29) $\mathcal{D}$ is a subspace of the linear space $\mathcal{A} \subseteq \mathbb{Q}^{|\Gamma|}$. Consider the mapping Δ defined by $\Delta(v) = Hv$ for $v \in \mathcal{A}$. Corollary 2 shows that Δ maps $\mathcal{A}$ in $\mathcal{D}$. As the rows of H are pairwise orthogonal and nonzero, this matrix is regular. Therefore, Δ is bijective, $\dim(\mathcal{D}) = \dim(\mathcal{A})$, $\mathcal{D} = \mathcal{A}$. □

As before let $\tilde{D}$ be the set of all positive divisor tuples d of $m = (2,\ldots,2,n)$. Remember that $\{c_{d,\Gamma} :\ d \in \tilde{D}\}$ is a basis of $\mathcal{D} = \mathcal{A}$, $\dim(\mathcal{A}) = |\tilde{D}|$.

Lemma 10. *Let $\Gamma = Z_2^r \otimes Z_n,\ S \subseteq \Gamma,\ 0 \notin S,\ -S = S$. The Cayley graph $G = Cay(\Gamma, S)$ is integral, if and only $S = \emptyset$ or if there are positive divisor tuples $d^{(1)},\ldots,d^{(k)}$ of $m = (2,\ldots,2,n)$ such that $S = S_\Gamma(D)$ for $D = \{d^{(1)},\ldots,d^{(k)}\}$.*

Proof. For $S = S_\Gamma(D)$ the Cayley graph $G = Cay(\Gamma, S)$ is a gcd-graph, which is integral by Corollary 1.

To prove the converse, we skip the trivial case of G being edgeless and assume that G is integral, $S \neq \emptyset$. Let $c_{S,\Gamma}$ be the characteristic vector of S with respect to the same ordering of the elements of Γ which we used to establish the character matrix $H = H(\Gamma)$, see Figure 1. By Lemma 7 the entries of $Hc_{S,\Gamma}$ are the eigenvalues of G, which are integral. This means $c_{S,\Gamma} \in \mathcal{A}$. Lemma 9 implies that there are positive, distinct divisor tuples $d^{(1)},\ldots,d^{(k)}$ of m such that

$$c_{S,\Gamma} \;=\; \lambda_1 c_{d^{(1)},\Gamma} + \cdots + \lambda_k c_{d^{(k)},\Gamma}\ ,\ \lambda_j \in \mathbb{Q},\ \lambda_j \neq 0\ \text{ for } j = 1,\ldots,k.$$

All vectors $c_{d^{(1)},\Gamma},\ldots,c_{d^{(k)},\Gamma}$ have only 0,1-entries and their sets of positions with entries 1 are pairwise disjoint. As $c_{S,\Gamma}$ has also only 0,1-entries, we must have $\lambda_1 = \cdots = \lambda_k = 1$. Then S becomes the disjoint union

$$S = S_\Gamma(d^{(1)}) \cup \cdots \cup S_\Gamma(d^{(k)}) = S_\Gamma(D).$$

□

Theorem 4. *Let Γ be a gcd-group, $S \subseteq \Gamma,\ 0 \notin S,\ -S = S$. The Cayley graph $G = Cay(\Gamma, S)$ is integral, if and only if S belongs to the Boolean algebra $B(\Gamma)$ generated by the subgroups of Γ.*

Proof. In [10] we showed that $S \in B(\Gamma)$ implies that G is integral.

To prove the converse, we assume $S \neq \emptyset$ and $G = Cay(\Gamma, S)$ integral. By Theorem 3 we know that there is a group $\Gamma' = Z_2^r \otimes Z_n$ and a group isomorphism $\varphi : \Gamma \to \Gamma'$. If we set $S' = \varphi(S)$ and $G' = Cay(\Gamma', S')$, then φ becomes also a graph isomorphism $\varphi : G \to G'$. Therefore, G' is integral and S' is a gcd-set of Γ' by Lemma 10, $S' \in B_{gcd}(\Gamma') = B(\Gamma')$. The group isomorphism φ provides a bijection between the sets in $B(\Gamma')$ and in $B(\Gamma)$. So we conclude $S \in B(\Gamma)$. □

Example. We have shown that for a gcd-group Γ the integral Cayley graphs over Γ are exactly the gcd-graphs over Γ. For an arbitrary group Γ the number of integral Cayley graphs over Γ may be considerably larger than the number of gcd-graphs over Γ.

Let p be a prime number, $p \geq 5$. We determine the number of nonisomorphic gcd-graphs over $\Gamma = Z_p \otimes Z_p$. There are three possible divisor tuples of (p, p) for the construction of a gcd-graph over Γ: $(1, 1)$, $(1, p)$, $(p, 1)$. From these tuples we can form 8 sets of divisor tuples:

$$D_1 = \emptyset,\ D_2 = \{(1,1)\},\ D_3 = \{(1,p)\},\ D_4 = \{(p,1)\},\ D_5 = \{(1,1),(1,p)\},$$
$$D_6 = \{(1,1),(p,1)\},\ D_7 = \{(1,p),(p,1)\},\ D_8 = \{(1,1),(1,p),(p,1)\}.$$

Obviously, D_3 and D_4 generate isomorphic gcd-graphs over Γ, so do D_5 and D_6. Therefore, we cancel D_4 and D_6. The cardinalities $|S_\Gamma(D_i)|$ for $i \in \{1, 2, 3, 5, 7, 8\} = M$ are in ascending order:

$$0,\ p-1,\ 2(p-1),\ (p-1)^2,\ p(p-1),\ p^2-1.$$

These are the degrees of regularity of the corresponding gcd-graphs $Cay(\Gamma, S_\Gamma(D_i))$, $i \in M$. As the above degree sequence is strictly increasing for $p \geq 5$, there are exactly 6 nonisomorphic gcd-graphs over $\Gamma = Z_p \otimes Z_p$.

Every element of $\Gamma = Z_p \otimes Z_p$ has order p except for the zero element $(0, 0)$. Denote by $[a]$ the cyclic subgroup generated by a. There are nonzero elements $a_1, \ldots, a_{p+1}$ in Γ such that

$$\Gamma = U_1 \cup \cdots \cup U_{p+1},\ U_i = [a_i],\ U_i \cap U_j = \{(0,0)\} \text{ for } i \neq j.$$

The sets

$$S_0 = \emptyset,\ S_i = (U_1 \cup \cdots \cup U_i) \backslash \{(0,0)\},\ 1 \leq i \leq p+1,$$

belong to the Boolean algebra $B(\Gamma)$. Therefore, the Cayley graphs $G_i = Cay(\Gamma, S_i)$, $0 \leq i \leq p+1$, are integral. They are nonisomorphic, because they have pairwise distinct degrees of regularity: $\text{degree}(G_i) = i(p-1)$, $0 \leq i \leq p+1$. As there are exactly 6 nonisomorphic gcd-graphs over Γ, we conclude that there are at least $(p+2) - 6 = p - 4$ nonisomorphic integral Cayley graphs over Γ, which are not gcd-graphs. An interesting task would be to determine for every prime number p the number of all nonisomorphic integral Cayley graphs over $\Gamma = Z_p \otimes Z_p$.

References

[1] Abdollahi, A., and Vatandoost, E. Which Cayley graphs are integral? *Electronic J. Comb. 16(1)* (2009), R122, 1–17.

[2] Ahmadi, O., Alon, N., Blake, L. F., and Shparlinski, I. E. Graphs with integral spectrum. *Linear Alg. Appl. 430* (2009), 547–552.

[3] Balinska, K., Cvetković, D., Rodosavljević, Z., Simić, S., and Stevanović, D. A survey on integral graphs. *Univ. Beograd, Publ. Elektrotehn. Fak. Ser. Mat 13* (2003), 42–65.

[4] Basić, M., Petković, M., and Stevanović, D. Perfect state transfer in integral circulant graphs. *Appl. Math. Letters 22* (2009), 1117–1121.

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

[6] Cohn, P. M. *Basic Algebra.* Springer, London, 2003.

[7] Godsil, C., and Royle, G. *Algebraic graph theory.* Graduate Texts in Mathematics. Vol 207. Springer, 2001.

[8] Harary, F., and Schwenk, A. J. Which graphs have integral spectra? *Lecture Notes in Mathematics 406*, Springer Verlag (1974), 45–50.

[9] Ilić, A. The energy of unitary cayley graphs. *Linear Algebra and its Applications 431* (2009), 1881–1889.

[10] Klotz, W., and Sander, T. Integral Cayley graphs over abelian groups. *Electronic J. Combinatorics 17* (2010), R81, 1–13.

[11] Klotz, W., and Sander, T. Some properties of unitary Cayley graphs. *Electronic J. Combinatorics 14* (2007), R45, 1–12.

[12] van Lint, J. H., and Wilson, R. M. *A course in combinatorics.* Cambridge University Press, 1992.

[13] Lovász, L. Spectra of graphs with transitive groups. *Priodica Mathematica Hungarica 6* (1975), 191–195.

[14] Rose H. E. *A course in number theory.* Oxford Science Publications. Oxford University Press, 1994.

[15] Saxena, N., Severini, S., and Shparlinski, I. Parameters of integral circulant graphs and periodic quantum dynamics. *Intern. Journ. of Quantum Information 5* (2007), 417–430.

[16] So, W. Integral circulant graphs. *Discrete Mathematics 306* (2005), 153–158.