Integral Cayley graphs generated by distance sets in vector spaces over finite fields

Nguyen Ngoc Dai

School of Applied Mathematics and Informatics
Hanoi University of Science and Technology

nguyendai236@gmail.com

Nguyen Minh Hai

Faculty of Mathematics, Mechanics and Informatics
Hanoi University of Science
Vietnam National University, Hanoi

nguyenminhhai06@gmail.com

Do Duy Hieu

Faculty of Mathematics, Mechanics and Informatics
Hanoi University of Science
Vietnam National University, Hanoi

duyhieua1t@gmail.com

Le Anh Vinh*

University of Education
Vietnam National University, Hanoi

vinhla@vnu.edu.vn

Submitted: Sep 20, 2012; Accepted: Jan 23, 2013; Published: Feb 5, 2013

Abstract

Si Li and the fourth listed author (2008) considered unitary graphs attached to the vector spaces over finite rings using an analogue of the Euclidean distance. These graphs are shown to be integral when the cardinality of the ring is odd or the dimension is even. In this paper, we show that the statement also holds for the remaining case: the cardinality of the ring is even and the dimension is odd, by showing a sufficient condition for Cayley graphs generated by distance sets in vector spaces over finite fields to be integral.

*This research was supported by Vietnam National Foundation for Science and Technology Development grant 102.01-2012.29.

1 Introduction

Let Γ be an additive group. For $S \subseteq \Gamma$, $0 \notin S$, and $S^{-1} = \{-s : s \in S\} = S$, the Cayley graph $G = C(\Gamma, S)$ is the undirected graph where the vertex set $V(G) = \Gamma$ and the edge set $E(G) = \{(a, b) : a - b \in S\}$. The Cayley graph $G = C(\Gamma, S)$ is regular of degree $|S|$. For any positive integer $n > 1$, let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the finite cyclic ring of n elements. Notice that one can identify $\mathbb{Z}_n$ with $\{0, 1, \ldots, n-1\}$. The unitary Cayley graph $X_n = C(\mathbb{Z}_n, \mathbb{Z}_n^*)$ is defined by the additive group of the ring $\mathbb{Z}_n$ of integers modulo n and the multiplicative group $\mathbb{Z}_n^*$ of its units. So X_n has vertex set $V(X_n) = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and edge set

$$E(X_n) = \{(a, b) : a, b \in \mathbb{Z}_n, \gcd(a - b, n) = 1\}.$$

The graph X_n is regular of degree $|\mathbb{Z}_n^*| = \phi(n)$, where $\phi(n)$ denotes the Euler function. Unitary Cayley graphs are highly symmetric and have some remarkable properties connecting graph theory and number theory. More information about the unitary Cayley graphs can be found in Berrizbeitia and Giudici [3], Dejter and Giudici [5], Fuchs [6], and Klotz and Sander [7].

In [8], Si Li and the fourth listed author studied higher dimensional unitary Cayley graphs over $\mathbb{Z}_n^d$ using an analogue of the Euclidean distance. Precisely, they defined for positive integers n and d the unitary Euclidean graph $T_n^{(d)}$ with vertex set $V(T_n^{(d)}) = \mathbb{Z}_n^d$ and edge set

$$E(T_n^{(d)}) = \left\{ (a, b) : d(a, b) = \sum_{i=1}^{d} (a_i - b_i)^2 \in \mathbb{Z}_n^* \right\}. \tag{1}$$

Note that the Euclidean graph $E_R^{(d)}(r)$ over a finite ring R, $r \in R$, is the Cayley graph with vertex set $V(E_R^{(d)}(r)) = R^d$ and the edge set

$$E(E_R^{(d)}(r)) = \left\{ (a, b) : d(a, b) = \sum_{i=1}^{d} (a_i - b_i)^2 = r \right\}.$$

In [11], Medrano, Myers, Stark and Terras studied the spectrum of the Euclidean graphs over finite fields and showed that these graphs are asymptotically Ramanujan graphs. In [12], these authors studied the same problem for the Euclidean graphs over rings $\mathbb{Z}_q$ for an odd prime power q. They showed that over rings, except for the smallest case, the graphs (with unit distance parameter) are not (asymptotically) Ramanujan.

In [2], Bannai, Shimabukuro and Tanaka showed that the Euclidean graphs over finite fields are always asymptotically Ramanujan for a more general setting (i.e. they replace the Euclidean distance by nondegenerated quadratic forms). The fourth listed author recently applied these results to several interesting combinatorial problems, for example to the Erdős distance problem [14], Szemeredi-Trotter type theorem and sum-product estimate [15], singular matrices with restricted entries over finite fields [16] and explicit constructions of existentially closed graphs [17].

Si Li and the fourth listed author [8] showed that the spectrum of unitary finite-Euclidean graphs consists entirely of integers when n is odd or the dimension d is even.

This property seems to be amazingly widespread among Cayley graphs on abelian groups. One of the first papers in this direction is due to L. Lovász [9], who proved that all Cayley graphs, (cube-like) graphs, on $\mathbb{Z}_2^d$ are integral where $\mathbb{Z}_n$ is the ring of integers modulo n. In this paper, we extend this result by showing a sufficient condition for Cayley graphs generated by distance sets in vector spaces over finite fields are integral. We would like to remark that our result is closely related to the result of W. So in [13].

2 Cayley graphs generated by distance sets

For any $\mathcal{U} \subseteq \mathbb{Z}_n$, the distance graph generated by $\mathcal{U}$ over $\mathbb{Z}_n^l$, $G(\mathbb{Z}_n^l, \mathcal{U})$, is the undirected graph that has the vertex set $V(G) = \mathbb{Z}_n^l$ and the edge set

$$E(G) = \{(\boldsymbol{a}, \boldsymbol{b}) : d(\boldsymbol{a}, \boldsymbol{b}) = \sum_{i=1}^{l} (a_i - b_i)^2 \in \mathcal{U}\}.$$

Let

$$S_{l,n}(\mathcal{U}) = \{\boldsymbol{a} \in \mathbb{Z}_n^l : d(\boldsymbol{a}, \boldsymbol{0}) = a_1^2 + \ldots + a_l^2 \in \mathcal{U}\},$$

then the graph $G(\mathbb{Z}_n^l, \mathcal{U})$ is the Cayley graph $C(\mathbb{Z}_n^l, S_{l,n}(\mathcal{U}))$. Recall that the eigenvalues of Cayley graphs of abelian groups can be computed easily in terms of the characters of the group. This is an old result and easy to prove: the characters of a finite abelian group are eigenfunctions for the convolution operators on the group (see also [11]). This implies that the eigenvalues of the graph $G(\mathbb{Z}_n^l, \mathcal{U})$ are all the numbers

$$\lambda_{\boldsymbol{b}} = \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U})} e_n({}^t\boldsymbol{b} \cdot \boldsymbol{x}), \tag{2}$$

where $\boldsymbol{b} \in \mathbb{Z}_n^l$ and the exponential $e_n(z) = \exp\{2\pi i z/n\}$.

In particular, the unitary Euclidean graph $T_n^{(d)}$ is the Cayley graph generated by the distance set $\mathcal{U} = \mathbb{Z}_n^*$. Using properties of Gauss and Ramanujan's sums over cyclic rings, Si Li and the fourth listed author [8] showed that $T_n^{(d)}$ is an integral graph if n is odd or d is even.

Theorem 1 *([8, Theorem 3.6]) If n is an odd integer or d is an even integer then all eigenvalues of the unitary Euclidean graph $T_n^{(d)}$ are integers.*

They conjectured that the same result also holds in general.

Conjecture 2 *([8, Conjecture 3.7]) For any positive integers n and d all eigenvalues of the unitary Euclidean graph $T_n^{(d)}$ are integers.*

From Theorem 1, the remaining open case of Conjecture 2 is: n even and d odd. In this paper, we will give a simple proof of this conjecture. More precisely, we have the following sufficient condition for Cayley graphs generated by distance sets in vector spaces over finite fields are integral. We conjecture that the given condition is also the necessary condition.

Theorem 3 *Suppose that $d_1, d_2, \ldots, d_r$ are divisors of n. Let*

$$\mathcal{U} = \cup_{j=1}^{r} G_n(d_j), \tag{3}$$

where

$$G_n(d_j) = \{y \in \mathbb{Z}_n : gcd(n, y) = d_j\}.$$

Then we have $\lambda_{\mathcal{U}}(\boldsymbol{b}) \in \mathbb{Z}$ for all $\boldsymbol{b} \in \mathbb{Z}_n^l$.

Proof Let d be a divisor of n. Note that $\boldsymbol{x} \in S_{l,n}(G_n(d))$ then $k \cdot \boldsymbol{x} \in S_{l,n}(G_n(d))$ for any $k \in \mathbb{Z}_n^*$, and if $\boldsymbol{x} \neq \boldsymbol{x'}$ then $k \cdot \boldsymbol{x} \neq k \cdot \boldsymbol{x'}$ for every $k \in \mathbb{Z}_n^*$. Since $S_{d,n}(G_n(d))$ is finite, it follows that

$$kS_{l,n}(G_n(d)) \equiv S_{l,n}(G_n(d)).$$

Hence, $kS_{l,n}(\mathcal{U}) \equiv S_{l,n}(\mathcal{U})$ when $\mathcal{U}$ is of the form (3).

We write $n = p_1^{r_1} \cdots p_t^{r_t}$ for the prime decomposition of n. For any nonempty subset $I \subseteq \{1, \ldots, t\}$, set

$$p_I = \prod_{i \in I} p_i \text{ and } n_I = n/p_I.$$

We have

$$\begin{aligned}
\lambda_{\mathcal{U}}(\boldsymbol{b}) &= \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U})} e_n({}^t\boldsymbol{b} \cdot \boldsymbol{x}) \\
&= \frac{1}{|\mathbb{Z}_n^*|} \sum_{k \in \mathbb{Z}_n^*} \sum_{\boldsymbol{x} \in kS_{l,n}(\mathcal{U})} e_n({}^t\boldsymbol{b} \cdot \boldsymbol{x}) \\
&= \frac{1}{|\mathbb{Z}_n^*|} \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U})} \sum_{k \in \mathbb{Z}_n^*} e_n(k{}^t\boldsymbol{b} \cdot \boldsymbol{x}) \\
&= \frac{1}{|\mathbb{Z}_n^*|} \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U}), {}^t\boldsymbol{b} \cdot \boldsymbol{x} = 0} |\mathbb{Z}_n^*| + \frac{1}{|\mathbb{Z}_n^*|} \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U}), {}^t\boldsymbol{b} \cdot \boldsymbol{x} \neq 0} \sum_{k \in \mathbb{Z}_n^*} e_n(k{}^t\boldsymbol{b} \cdot \boldsymbol{x}) \\
&= \#\{\boldsymbol{x} \in S_{l,n}(\mathcal{U}), {}^t\boldsymbol{b} \cdot \boldsymbol{x} = 0\} \\
&\quad + \frac{1}{|\mathbb{Z}_n^*|} \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U}), {}^t\boldsymbol{b} \cdot \boldsymbol{x} \neq 0} \sum_{k \in \mathbb{Z}_n} e_n(k{}^t\boldsymbol{b} \cdot \boldsymbol{x}) \\
&\quad + \frac{1}{|\mathbb{Z}_n^*|} \sum_{\boldsymbol{x} \in S_{l,n}(\mathcal{U}), {}^t\boldsymbol{b} \cdot \boldsymbol{x} \neq 0} \sum_{I \subseteq \{1, \ldots, t\}} (-1)^{|I|} \sum_{s \in \mathbb{Z}_{n_I}} e_n(p_I s {}^t\boldsymbol{b} \cdot \boldsymbol{x}).
\end{aligned}$$

Since ${}^t\boldsymbol{b} \cdot \boldsymbol{x} \neq 0$, from the orthogonality of exponential sums, we have

$$\sum_{s \in \mathbb{Z}_{n_I}} e_n(p_I s {}^t\boldsymbol{b} \cdot \boldsymbol{x}) = 1$$

if $n = p_1 \cdots p_t$ and $I = \{1, 2, \ldots, t\}$; and

$$\sum_{s \in \mathbb{Z}_{n_I}} e_n(p_I s {}^t\boldsymbol{b} \cdot \boldsymbol{x}) = 0$$

otherwise. This implies that $\lambda_{\mathcal{U}}(\boldsymbol{b}) \in \mathbb{Q}$ for any $\boldsymbol{b} \in \mathbb{Z}_n^l$. Furthermore, the characteristic polynomial of the adjacency matrix of $G(\mathbb{Z}_n^l, \mathcal{U})$ is monic with integer coefficients, so $\lambda_{\mathcal{U}}(\boldsymbol{b}) \in \mathbb{Z}$ for any $\boldsymbol{b} \in \mathbb{Z}_n^l$. This concludes the proof of the theorem. □

Note that Theorem 3 implies Conjecture 2 by setting $r = 1$ and $d_1 = 1$.

Remark 4 *For any distance function $f : \mathbb{Z}_n^l \times \mathbb{Z}_n^l \to \mathbb{Z}_n$ and the distance set $\mathcal{U} \subset \mathbb{Z}_n$, define the generating set*

$$S_{l,n}(f, \mathcal{U}) = \{\boldsymbol{a} \in \mathbb{Z}_n^l : f(\boldsymbol{a}, \boldsymbol{0}) \in \mathcal{U}\}.$$

The above proof of Theorem 3 works transparently for any distance function f that satisfies the condition $kS_{l,n}(\mathcal{U}) \equiv S_{l,n}(\mathcal{U})$ when $\mathcal{U}$ is of the form (3). For example, Theorem 3 still holds if we use the distance function $d(\boldsymbol{a}, \boldsymbol{b}) = \sum_{i=1}^{l} (a_i - b_i)^h$ for any $h \geqslant 1$. Let $l = h = 1$, we obtain alternative proofs of [7, Theorem 16] and [13, Corollary 4.5].

References

[1] J. Angle, B. Shook, A. Terras, C. Trimble and E. Velasquez, Graph spectra for finite upper half planes over rings, *Linear Algebra Applications*, **226-228** (1995), 423–457.

[2] E. Bannai, O. Shimabukuro and H. Tanaka, Finite Euclidean graphs and Ramanujan graphs, *Discrete Mathematics* (to appear).

[3] P. Berrizbeitia and R. E. Giudici, On cycles in the sequence of unitary Cayley graphs, *Discrete Mathematics* **282** 1-3 (2004), 239–243.

[4] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts **21**, John Wiley & Sons (1998).

[5] I. J. Dejter and R. E. Giudici, On unitary Cayley graphs, *J. Combin. Math. Combin. Comput.*, **18** (1995), 121–124.

[6] E. D. Fuchs, Longest induced cycles in circulant graphs, *The Electronic Journal of Combinatorics*, **12** (2005), 1-12.

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

[8] S. Li and L. A. Vinh, On the spectrum of unitary Euclidean graphs, *Ars Combinatoria* (to appear), eprint arxiv.org/abs/0802.1231

[9] L. Lovász, Spectra of graphs with transitive groups, *Periodica Mathematica Hungarica*, **6** (1975), 191-195.

[10] P. J. McCarthy, *Introduction to arithmetical functions*, Universitext. Springer-Verlag, New York, 1994.

[11] A. Medrano, P. Myers, H. M. Stark and A. Terras, Finite analogues of Euclidean space, *Journal of Computational and Applied Mathematics*, **68** (1996), 221–238.

[12] A. Medrano, P. Myers, H. M. Stark and A. Terras, Finite Euclidean graphs over rings, *Proceedings of the American Mathematics Society*, **126** (1998), 701–710.

[13] W. So, Integral circulant graphs, *Discrete Mathematics*, **306** (2006), 153-158.

[14] L. A. Vinh, Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces, *The Electronic Journal of Combinatorics*, **15** (1), 2008, R5.

[15] L. A. Vinh, Szemeredi-Trotter type theorem and sum-product estimate in finite fields, *The European Journal of Combinatorics*, **32**(8), 1177-1181 (2011)

[16] L. A. Vinh, Singular matrices with restricted rows in vector spaces over finite fields, *Discrete Mathematics* **312**(2), 413–418 (2012).

[17] L. A. Vinh, An explicit construction of $(3, k)$-existentially closed graphs, *Discrete Applied Mathematics* (to appear).