# Eigenvalues and energy of restricted unitary Cayley graphs induced from the square mapping

**Yotsanan Meemark, Borworn Suntornpoch**[*]

Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok 10330 Thailand

[*]Corresponding author, e-mail: beyond.my.limit@gmail.com

**ABSTRACT**: Let $R$ be a finite commutative ring with unity $1 \neq 0$. The restricted unitary Cayley graph induced from the squared mapping is the graph whose vertex set is $R$ and whose edge set is $\{\{a, b\} : a, b \in R \text{ and } a - b \in T_R\}$, where $T_R = K_R(R^\times)^2$ and $K_R = \{a \in R^\times : a^2 = 1\}$. We study the structure of our graph $H_R$ and determine its eigenvalues and energy.

**KEYWORDS**: quadratic residues

## PRELIMINARIES

Let $R$ be a finite commutative ring with unity $1 \neq 0$. The *unitary Cayley graph of* $R$, $G_R = \text{Cay}(R, R^\times)$, is the Cayley graph whose vertex set is $R$ and whose edge set is $\{\{a, b\} : a, b \in R \text{ and } a - b \in R^\times\}$, where $R^\times$ denotes the group of units of $R$. Consider the exact sequence of groups

$$1 \longrightarrow K_R \longrightarrow R^\times \overset{\theta}{\longrightarrow} (R^\times)^2 \longrightarrow 1,$$

where $\theta : a \mapsto a^2$ is the square mapping on $R^\times$ with kernel $K_R = \{a \in R^\times : a^2 = 1\}$ and $(R^\times)^2 = \{a^2 : a \in R^\times\}$. Note that $K_R$ consists of the identity and all elements of order two in $R^\times$. Let $T_R = K_R(R^\times)^2$. Define the subgraph $H_R$ of the unitary Cayley graphs by $H_R = \text{Cay}(R, T_R)$, in which two vertices are adjacent if and only if their difference is in $T_R$. Since $-1 \in T_R$, the graph $H_R$ is undirected. In addition, we observe that if $|R^\times|$ is odd, $K_R = \{1\}$ and $R^\times = (R^\times)^2$, so $H_R = G_R$. All finite rings $R$ with group of units $R^\times$ having an odd number of elements are completely determined[1].

The motivation of the graph defined above comes from the quadratic unitary Cayley graph $\text{Cay}(\mathbb{Z}_n, \pm(\mathbb{Z}_n^\times)^2)$ introduced by Beaudrap[2]. He bounded the diameter of such graphs and characterized the conditions on $n$ for $\text{Cay}(\mathbb{Z}_n, \pm(\mathbb{Z}_n^\times)^2)$ to be perfect. When $n = p^s$, where $p$ is a prime and $s \in \mathbb{N}$, his graph and our graph coincide. The main purpose here is to obtain the eigenvalues and energy of the graphs using an approach similar to Ref. 3.

Now we give an example. Let $q$ be a prime power such that $q \equiv 1 \mod 4$. The *Paley graph* is the graph whose vertex set is the finite field $\mathbb{F}_q$ with $q$ elements and whose edge set is $\{\{a, b\} : a, b \in \mathbb{F}_q \text{ and } a - b \in (\mathbb{F}_q^\times)^2\}$. Since $\mathbb{F}_q$ is a field, $K_{\mathbb{F}_q} = \{\pm 1\}$. The congruence condition on $q$ implies that $-1$ is a square in $\mathbb{F}_q$ and hence $T_{\mathbb{F}_q} = (\mathbb{F}_q^\times)^2$. Thus the Paley graph is $H_{\mathbb{F}_q}$.

A $k$-regular graph $G$ with $v$ vertices is said to be *strongly regular* with parameters $(v, k, \lambda, \mu)$ if there are integers $\lambda$ and $\mu$ such that
(i) every two adjacent vertices have $\lambda$ common neighbours, and
(ii) every two non-adjacent vertices have $\mu$ common neighbours.

For a graph $G$, its *eigenvalues* are defined to be the eigenvalues of the adjacency matrix of $G$. The set of all eigenvalues of $G$ is called the *spectrum of* $G$. We can explicitly determine the eigenvalues of a strongly regular graph by using the following lemma.

**Lemma 1 (§10.2 of Ref. 4)** *A strongly regular graph with parameters* $(v, k, \lambda, \mu)$ *has exactly three eigenvalues:*
(i) *$k$ whose multiplicity is 1;*
(ii) *$\frac{1}{2}\left[(\lambda - \mu) + \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\right]$ whose multiplicity is $\frac{1}{2}\left[(v - 1) - (2k + (v - 1)(\lambda - \mu))/(\sqrt{(\lambda - \mu)^2 + 4(k - \mu)})\right]$;*
(iii) *$\frac{1}{2}\left[(\lambda - \mu) - \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\right]$ whose multiplicity is $\frac{1}{2}\left[(v - 1) + (2k + (v - 1)(\lambda - \mu))/(\sqrt{(\lambda - \mu)^2 + 4(k - \mu)})\right]$.*

It is well known that the Paley graph is strongly regular as we recall in the next lemma. Hence we obtain its eigenvalues from Lemma 1. As is standard, if

$\lambda_1, \ldots, \lambda_k$ are eigenvalues of a graph $G$ of respective multiplicities $m_1, \ldots, m_k$, we use the notation

$$\operatorname{spec} G = \begin{pmatrix} \lambda_1 & \ldots & \lambda_k \\ m_1 & \ldots & m_k \end{pmatrix}$$

to describe the spectrum of $G$.

**Lemma 2 (p.221 of Ref. 4)** *Let $q$ be a prime power such that $q \equiv 1 \mod 4$. The Paley graph over the finite field $\mathbb{F}_q$ is strongly regular with parameters $(q, (q-1)/2, (q-5)/4, (q-1)/4)$ and*

$$\operatorname{spec} H_{\mathbb{F}_q} = \begin{pmatrix} \frac{q-1}{2} & \frac{\sqrt{q}-1}{2} & \frac{-\sqrt{q}-1}{2} \\ 1 & \frac{q-1}{2} & \frac{q-1}{2} \end{pmatrix}.$$

The sum of absolute values of all eigenvalues of a graph $G$ is called the *energy of $G$* and denoted by $E(G)$. The energy is a graph parameter stemming from the Hückel molecular orbital approximation for the total $\pi$-electron energy (for a survey on molecular graph energy see, e.g., Ref. 5). This concept was introduced in Ref. 6 and later studied intensively[3, 7–9].

**Lemma 3** *If $q$ is a prime power congruent to 1 modulo 4, then $E(H_{\mathbb{F}_q}) = \frac{1}{2}(q-1)(1+\sqrt{q})$.*

The following theorem gives the eigenvalues and the energy of unitary Cayley graph of $R$.

**Theorem 1 (Proposition 2.1, Theorem 2.4 of Ref. 3)** *Let $R$ be a finite commutative ring.*
(i) *If $R$ is a local ring with maximal ideal $M$, then*

$$\operatorname{spec} G_R = \begin{pmatrix} |R^\times| & -|M| & 0 \\ 1 & \frac{|R|}{|M|} - 1 & \frac{|R|}{|M|}(|M|-1) \end{pmatrix}$$
$$= \begin{pmatrix} |R^\times| & -|M| & 0 \\ 1 & \frac{|R^\times|}{|M|} & \frac{|R|}{|M|}(|M|-1) \end{pmatrix},$$

*and $E(G_R) = 2|R^\times|$. In particular, if $F$ is the field with $q$ elements, then*

$$\operatorname{spec} G_F = \begin{pmatrix} q-1 & -1 \\ 1 & q-1 \end{pmatrix} = \begin{pmatrix} |F^\times| & -1 \\ 1 & |F^\times| \end{pmatrix}$$

*and $E(G_F) = 2(q-1)$.*
(ii) *If $R = R_1 \times R_2 \times \cdots \times R_k$ and $R_i$ is a local ring for all $i \in \{1, 2, \ldots, k\}$, then $E(G_R) = 2^k|R^\times|$.*

For two graphs $G$ and $H$, their *tensor product $G \otimes H$* is the graph with vertex set $V(G) \times V(H)$, where $(u, v)$ is adjacent to $(u', v')$ if and only if $u$ is adjacent to $u'$ in $G$ and $v$ is adjacent to $v'$ in $H$.

**Theorem 2 (Ref. 10)** *Let $G$ and $H$ be graphs. Suppose that $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of $G$ and $\mu_1, \ldots, \mu_m$ are the eigenvalues of $H$ (repetition is possible). Then the eigenvalues of $G \otimes H$ are $\lambda_i \mu_j$, where $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$. In particular, $E(G \otimes H) = E(G)E(H)$.*

In what follows, we shall study the energy of $H_R$ when $R$ is the ring of integers modulo $n$ and $R$ is the quotient ring of polynomials over finite fields. We prove the main theorem in the next section. The final section provides some computational examples using elementary number theory.

**MAIN RESULTS**

Let $R$ be a finite commutative ring. Then $R$ can be expressed as a direct sum of local rings, that is, $R = R_1 \times R_2 \times \cdots \times R_k$, where $R_i$ is a local ring. Note that $R = R_1 \times R_2 \times \cdots \times R_k$ induces the isomorphisms

$$R^\times = R_1^\times \times R_2^\times \times \cdots \times R_k^\times,$$
$$(R^\times)^2 \cong (R_1^\times)^2 \times (R_2^\times)^2 \times \cdots \times (R_k^\times)^2.$$

In addition, $K_R \cong K_{R_1} \times K_{R_2} \times \cdots \times K_{R_k}$. This proves the following decomposition theorem.

**Theorem 3** *Let $R$ be a finite commutative ring. If $R = R_1 \times R_2 \times \cdots \times R_k$ and $R_i$ is a local ring for all $i \in \{1, 2, \ldots, k\}$, then*

$$H_R \cong H_{R_1} \otimes H_{R_2} \otimes \cdots \otimes H_{R_k}.$$

The above theorem tells us that we can concentrate only on $H_R$ when $R$ is a local ring.

Let $R$ be a finite local ring with unique maximal ideal $M$. Then $|R| = p^l$ for some $l \geqslant 1$ and $p$ is a prime number. Note that the kernel of the homomorphism $\varphi : R^\times \to (R/M)^\times$ mapping $a$ to $a + M$ is $1 + M$. Thus we have the isomorphism $R^\times/(1 + M) \cong (R/M)^\times$. Recall that $R/M$ is a field and $(R/M)^\times$ is cyclic. Since $|R^\times| = |R| - |M| = |M|(|R|/|M| - 1)$, $|M| = p^m$ for some $m < l$, and $|M| = |1 + M|$, we have the result that $1 + M$ is the Sylow $p$-subgroup of $R^\times$. Hence, $R^\times \cong (R/M)^\times \times (1 + M)$.

Assume that $p$ is an odd prime. The above observation gives $K_R = \{\pm 1\}$ and leads us to distinguish two cases. If $-1$ is not a square in $R$, then $K_R(R^\times)^2 = R^\times$ and $H_R = G_R$.

Next, we suppose that $-1$ is a square in $R$. Since $|1 + M| = p^m$ and $p$ is an odd prime, we have $(1 + M)^2 = 1 + M$ so that $(R^\times)^2 \cong ((R/M)^\times)^2 \times (1+M)$. Write $R/M = \{r_1+M, r_2+M, \ldots, r_{p^{l-m}}+ M\}$. Then for each $a \in R$, there is a unique $i$ and

$m_a \in M$ such that $a - r_i = m_a$. This yields the bijection $\tau : R \to R/M \times M$ by $\tau : a \mapsto (r_i + M, m_a)$ for all $a \in R$. Thus for all $a, b \in R$, $(a - b) \in (R^\times)^2$ if and only if $\tau(a - b) \in ((R/M)^\times)^2 \times M$. Hence, $\tau$ induces an isomorphism $H_R \cong H_{R/M} \otimes \mathcal{K}_{|M|}$, where $\mathcal{K}_{|M|}$ is the $|M|$-complete graph with a loop on each vertex. Note that $H_{R/M}$ is a Payley graph. Furthermore, we know that the adjacency matrix of the $|M|$-complete graph with a loop on each vertex, $\mathcal{K}_{|M|}$, is the $|M| \times |M|$ matrix of ones, so

$$\operatorname{spec} \mathcal{K}_{|M|} = \begin{pmatrix} |M| & 0 \\ 1 & |M| - 1 \end{pmatrix},$$

and $E(\mathcal{K}_{|M|}) = |M|$. Hence Lemma 3, Theorem 1 and Theorem 2 complete our main conclusions.

**Theorem 4** *Let $R$ be a finite local ring with unique maximal ideal $M$ of characteristic odd prime $p$.*
(i) *If $-1$ is not a square in $R$, then $H_R = G_R$ and $E(H_R) = E(G_R) = 2|R^\times|$.*
(ii) *If $-1$ is a square in $R$, then $H_R \cong H_{R/M} \otimes \mathcal{K}_{|M|}$, where $\mathcal{K}_{|M|}$ is the $|M|$-complete graph with a loop on each vertex. Moreover, if $|R/M| = p^t$, then*

$$\operatorname{spec} H_R =$$
$$\begin{pmatrix} \frac{|R^\times|}{2} & \frac{|M|(p^{t/2}-1)}{2} & \frac{|M|(-p^{t/2}-1)}{2} & 0 \\ 1 & \frac{p^t-1}{2} & \frac{p^t-1}{2} & |R| - p^t \end{pmatrix}$$

*and $E(H_R) = \dfrac{|R^\times|(p^{t/2}+1)}{2}$.*

## EXAMPLES

In this section, we provide two computational examples of Theorem 4 using elementary number theory. We present the results when $R = \mathbb{Z}_n$, the ring of integers modulo $n$ and $R = A/fA$, where $A = \mathbb{F}_q[x]$, $q = p^s$ an odd prime power, $s \geqslant 1$, and $f$ is a non-constant polynomial in $A$.

### Quadratic residues of $n$

Let $n > 1$ be a positive integer. We write $G_n = G_{\mathbb{Z}_n}$ and $H_n = H_{\mathbb{Z}_n}$. We study the structure of the graph $H_n$ and obtain its energy using the results discussed in the previous sections.

As usual, our work will start with the case when $n$ is a prime power. For $p = 2$, if $s = 1$, it is immediate that $H_2 = G_2$. If $s = 2$, we have $\mathbb{Z}_{2^2}^\times = \{\pm 1\} = K_{2^2}$ and $(\mathbb{Z}_{2^2}^\times)^2 = \{1\}$, and thus $T_{2^2} = \{\pm 1\}$ and $H_4 = G_4$. If $s = 3$, we have $\mathbb{Z}_{2^3}^\times = \{\pm 1, \pm 3\} = K_{2^3}$ and $(\mathbb{Z}_{2^3}^\times)^2 = \{1\}$, so $T_{2^3} = \mathbb{Z}_{2^3}^\times$ and $H_8 = G_8$. Finally, let $s \geqslant 4$. We recall the fact that $\mathbb{Z}_{2^s}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{s-2}}$.

Since $(\mathbb{Z}_{2^s}^\times)^2 \cong \mathbb{Z}_{2^{s-3}}$ and $K_{2^s} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we have $K_{2^s}(\mathbb{Z}_{2^s}^\times)^2 \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{s-3}}$. Thus $T_{2^s} = \pm(\mathbb{Z}_{2^s}^\times)^2$. It follows from Lemma 2 of Ref. 2 that $H_{2^s} \cong H_8 \otimes \mathcal{K}_{2^{s-3}}$. Hence, we have proved the next theorem.

**Theorem 5** *The graphs $H_2 = G_2$, $H_4 = G_4$, $H_8 = G_8$ and for $s \geqslant 4$, we have*

$$H_{2^s} \cong H_8 \otimes \mathcal{K}_{2^{s-3}},$$

*where $\mathcal{K}_{2^{s-3}}$ is the $2^{s-3}$-complete graph with a loop on each vertex. Moreover,*

$$\operatorname{spec} H_2 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},$$
$$\operatorname{spec} H_4 = \begin{pmatrix} 2 & -2 & 0 \\ 1 & 1 & 2 \end{pmatrix},$$
$$\operatorname{spec} H_8 = \begin{pmatrix} 2^2 & -2^2 & 0 \\ 1 & 1 & 6 \end{pmatrix},$$
$$\operatorname{spec} H_{2^s} = \begin{pmatrix} 2^{s-1} & -2^{s-1} & 0 \\ 1 & 1 & 2^s - 2 \end{pmatrix}$$

*for all $s \geqslant 4$. Furthermore, $E(H_{2^s}) = 2^s$ for all $s \geqslant 1$.*

Next, let $p$ be an odd prime and $s \geqslant 1$. Recall that $-1$ is a square in $\mathbb{Z}_{p^s}$ if and only if $p \equiv 1 \mod 4$. Theorem 4 directly gives the following results.

**Theorem 6** *Let $p$ be an odd prime and $s \geqslant 1$.*
(i) *If $p \equiv 3 \mod 4$, then $H_{p^s} = G_{p^s}$ and $E(H_{p^s}) = E(G_{p^s}) = 2(p^s - p^{s-1})$.*
(ii) *If $p \equiv 1 \mod 4$, then $H_{p^s} = H_p \otimes \mathcal{K}_{p^{s-1}}$, where $\mathcal{K}_{p^{s-1}}$ is the $p^{s-1}$-complete graph with a loop on each vertex. Moreover,*

$$\operatorname{spec} H_{p^s} =$$
$$\begin{pmatrix} \frac{p^s-p^{s-1}}{2} & \frac{p^{s-1}(\sqrt{p}-1)}{2} & \frac{p^{s-1}(-\sqrt{p}-1)}{2} & 0 \\ 1 & \frac{p-1}{2} & \frac{p-1}{2} & p^s - p \end{pmatrix}$$

*and $E(H_{p^s}) = (p^s - p^{s-1})/2(\sqrt{p} + 1)$.*

### Quadratic residues of $f$

Let $\mathbb{F}_q$ be the finite field with $q = p^s$ elements of characteristic odd prime $p$. Let $A = \mathbb{F}_q[T]$, and let $f \in A$ be a non-constant polynomial. We write $G_f = G_{(A/fA)}$ and $H_f = H_{(A/fA)}$.

Let $P \in A$ be an irreducible polynomial and $e \geqslant 1$. Write $|P|$ for $q^{\deg P}$.

**Theorem 7 (Theorem 1.10 for $d = 2$ of Ref. 11)**
*Let $a \in A$ and $e \geqslant 1$. Then the congruence $x^2 \equiv a \mod P^e$ has a solution if and only if $a^{(|P|-1)/2} \equiv 1 \mod P$ in $A$.*

This theorem gives the following criteria to determine if $-1$ is a square modulo $P^e$.

**Corollary 1** *Let* $\mathbb{F}_q$ *be the finite field with* $q = p^s$ *elements of characteristic odd prime* $p$. *Let* $P \in \mathbb{F}_q[T]$ *be an irreducible polynomial and* $e \geqslant 1$. *Then* $-1$ *is a quadratic non-residue of* $P^e$ *if and only if* $p \equiv 3$ $\mod 4$ *and* $s \deg P$ *is odd. And* $-1$ *is a quadratic residue of* $P^e$ *if and only if (i)* $p \equiv 1 \mod 4$ *or (ii)* $p \equiv 3 \mod 4$ *and* $s \deg P$ *is even.*

Theorem 4 implies eigenvalues and energy of the graph $H_{P^e}$ for all $e \geqslant 1$ as follows.

**Theorem 8** *Let* $\mathbb{F}_q$ *be the finite field with* $q = p^s$ *elements of characteristic odd prime* $p$. *Let* $P \in \mathbb{F}_q[T]$ *be an irreducible polynomial and* $e \geqslant 1$.

(i) *If* $p \equiv 3 \mod 4$ *and* $s \deg P$ *is odd, then* $H_{P^e} = G_{P^e}$ *and* $E(H_{P^e}) = 2(|P|^e - |P|^{e-1})$.

(ii) *If* $p \equiv 1 \mod 4$ *or* $(p \equiv 3 \mod 4$ *and* $s \deg P$ *is even), then* $H_{P^e} \cong H_P \otimes \mathcal{K}_{|P|^{e-1}}$, *where* $\mathcal{K}_{|P|^{e-1}}$ *is the* $|P|^{e-1}$*-complete graph with a loop on each vertex. Moreover,*

$$\operatorname{spec} H_{P^e} = \begin{pmatrix} \frac{|P|^e - |P|^{e-1}}{2} & \frac{|P|^{e-1}(\sqrt{|P|}-1)}{2} \\ 1 & \frac{|P|-1}{2} \\ \frac{|P|^{e-1}(-\sqrt{|P|}-1)}{2} & 0 \\ \frac{|P|-1}{2} & |P|^e - |P| \end{pmatrix}$$

*and* $E(H_{P^e}) = (|P|^e - |P|^{e-1})/2(\sqrt{|P|} + 1)$.

## REFERENCES

1. Dolžan D (2001) Group of units in a finite ring. *J Pure Appl Algebra* **170**, 175–83.
2. Beaudrap N (2010) On restricted unitary Cayley graphs and symplectic transformations modulo $n$. *Electron J Combinator* **17**, #R69.
3. Kiani D, Aghaei M, Meemark Y, Suntornpoch B (2011) Energy of unitary Cayley graphs and gcd-graphs. *Lin Algebra Appl* **435**, 1336–43.
4. Godsil C, Royle G (2001) *Algebraic Graph Theory*, Springer.
5. Gutman I (2001) *The Energy of a Graph: Old and New Results, Algebraic Combinatorics and Applications*, Springer, Berlin.
6. Gutman I (1978) The energy of a graph. *Ber Math Stat Sekt Forschungszent Graz* **103**, 1–22.
7. Ramane HS, Walikar HB, Rao SB, Acharya BD, Hampiholi PR, Jog SR, Gutman I (2005) Spectra and energies of iterated line graphs of regular graphs. *Appl Math Lett* **18**, 679–82.
8. Stevanović D, Indulal G (2009) The distance spectrum and energy of the compositions of regular graphs. *Appl Math Lett* **22**, 1136–40.
9. Ye L (2011) The energy of a type of lattice. *Appl Math Lett* **24**, 145–8.
10. West DB (2000) *Introduction to Graph Theory*, 2nd edn, Prentice-Hall.
11. Rosen M (2002) *Number Theory in Function Fields*, Springer.