

SUMS OF UNITS IN A FINITE RING AND APPLICATIONS TO CAYLEY GRAPHS

JÁN MINÁČ, TUNG T. NGUYEN, NGUYỄN DUY TÂN

ABSTRACT. The question of whether a ring is additively generated by its units has been extensively studied in the literature with various approaches. In this paper, we investigate the connection between this problem and several problems in algebraic graph theory, including the connectedness of gcd-graphs, the existence of perfect state transfer, and the solvability of certain Diophantine equations. Additionally, we discuss a generalization of this question in which only certain normalized units are allowed in the generating set. Our work intersects algebra, number theory, and graph theory, and may be of interest to a broad audience.

1. INTRODUCTION

The question of which rings are generated by their units has a long and rich history, attracting mathematicians working in algebra, number theory, and graph theory. Inspired by the work of Zelinski in [42] on the endomorphism ring of vector spaces, Skorniyakov asked in [37, p.167, Problem 31] for a classification of rings that are additively generated by units. (The main theorem of Zelinski in [42], which states that every matrix is a sum of two invertible matrices, was later reproved in [20] by Lord, who was not aware of Zelinski's work.) More precisely, Skorniyakov asked whether every element of a von Neumann regular ring that does not have $\mathbb{Z}/2$ as a quotient is a sum of units. Shortly after, Bergman gave a counterexample to this question, which led to a series of works on this topic (see [10, 34]). Some further refinements of Skorniyakov's question are investigated in [13, 21]. While [13] takes a purely algebraic approach, [21] looks at it through the lens of graph theory. More precisely, the authors of [21] realize that a finite commutative ring R is additively generated by units if and only if the associated unitary Cayley graph G_R is connected. We recall that G_R is the graph whose vertex set is R and two vertices a, b are adjacent if and only if $a - b$ is a unit. In the same spirit, in [32, 33]

Date: March 21, 2026.

2020 Mathematics Subject Classification. Primary 05C25, 05C50, 05C51.

Key words and phrases. Gcd-graphs, Cayley graphs, prime graphs, perfect graphs, connected graphs, bipartite graphs, Ramanujan sums, integral spectra.

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. TTN is partially supported by an AMS-Simons Travel Grant. NDT is partially supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 101.04-2023.21.

the Waring problem on whether a ring is additively generated by the set of k -th powers of units has also been approached via the so-called generalized Paley graphs.

Our interest in this question stems from previous work on gcd-graphs (see [18, 25, 30]), U -unitary Cayley graphs (see [29]), and the existence of perfect state transfer (PST) on them (see [5, 41, 28]). In these works, the sums of units play a crucial role in understanding the connectedness of these graphs, the explicit calculation of certain arithmetical sums, as well as whether PST can exist between two nodes. In particular, we affirmatively answer Skorniyakov's question when R is a finite ring, which is not necessarily commutative (the case where the ring is commutative is settled in [21]).

In this article, we study some questions in the spirit of Skorniyakov's original problem, but using other subsets S of R . Typically, such an S has an arithmetic origin. Here, the relevant graph that connects algebra and graph theory is the Cayley graph $\Gamma(R, S)$ whose vertex set is R and two vertices a, b are adjacent if $a - b \in S$. As observed in [21], this connection comes from the fact that R is additively generated by S if and only if $\Gamma(R, S)$ is connected. In the special case where S is stable under the left and right actions of R^\times , the Cayley graph $\Gamma(R, S)$ is an example of a gcd-graph, which is widely studied in the literature (see [5, 18, 30, 35, 41]). In this particular case, our result presented here completely resolves the question of when S additively generates R using the geometry of $\Gamma(R, S)$. We also discuss some relationship between gcd-graphs and the total graphs introduced by Anderson and Badawi in [3].

1.1. Outline. In Section 2, we revisit the question of when a ring has the property that every element is a sum of two units. Here, we describe various different interpretations of this property. We also study the inheritance of the 2-sum property under ring homomorphisms and ring extensions. Furthermore, we answer a generalization of Skorniyakov's original problem; namely, we classify all elements in a finite ring that are the sum of two units. We apply this result to calculate precisely the sum of all units in a finite ring. Additionally, we also use it to give a complete classification of connected gcd-graphs. In Section 3, we study a generalization of Skorniyakov's problem where only certain normalized units are allowed in the generating set. We focus our discussion on three standard rings: matrix rings, group rings, and finite fields (in all these cases, there is a natural definition of normalized units). While the study of these rings is encompassed by the framework we laid out, the proofs for each case are quite different in nature. Finally, in Section 4, we use the sums of units to study the *non-existence* of perfect state transfer (PST) on Cayley graphs. We show, in particular, that there is no PST on gcd-graphs defined over a ring that has the n -sum property.

2. SUMS OF UNITS

Let R be a finite unital ring such that $0 \neq 1$. In this article, we follow the convention that a ring homomorphism $\Phi : R \rightarrow R'$ would preserve 1; namely, $\Phi(1) = 1$. We also

say that R' is a quotient of R if there is a surjective ring homomorphism $\Phi : R \rightarrow R'$. We will write \mathbb{F}_q for a finite field with q elements.

2.1. Equivalent conditions for rings with the 2-sum property. Let n be a positive integer. In [13], the authors define the notion of a ring with the n -sum property. Namely, a ring R is said to have the n -sum property if and only if every element in R can be written as the sum of exactly n elements in R^\times . In [1, 13, 21, 30], the authors shows that for a ring R , if \mathbb{F}_2 is not a quotient of R , then R has the 2-sum property. Furthermore, using a graph-theoretic argument, [21] (for finite commutative rings) and [27] (for any finite ring) show that R is additively generated by its units if and only R does not have a quotient of the form $\mathbb{F}_2 \times \mathbb{F}_2$. We discuss below some reformations and applications of these results. The first treats several equivalent conditions for R to have the 2-sum properties, covering its unit group, quotient rings, certain special units, and the unitary Cayley graph defined on R . To do so, we recall that in [24], Nagel introduces the notion of an exceptional unit; namely, a unit u is called exceptional if $1 - u$ is also a unit. We are now ready to state our theorem.

Theorem 2.1. *The following conditions are equivalent*

- (1) R has no quotient of the form \mathbb{F}_2 .
- (2) R has the 2-sum property.
- (3) R has at least one exceptional unit.
- (4) The unitary Cayley graph G_R is not bipartite.

Proof. We will show that (1) \implies (2) \implies (3) \implies (4) \implies (1).

Let us first prove that (1) \implies (2). Let $R^{\text{ss}} = R/\text{Rad}(R)$ be the simplification of R with $\text{Rad}(R)$ being the Jacobson radical of R . Since an element in R is a unit if and only if its image in R^{ss} is a unit, R has the 2-sum property if and only if R^{ss} does (see [9, Proposition 3.40] and [13, Proposition 1.3]). By the Artin-Wedderburn theorem, R^{ss} is isomorphic to a direct product of the form $\prod_{i=1}^r M_{n_i}(F_i)$ where $n_i \geq 1$ and F_i is a finite field. By our assumption, none of these factors is \mathbb{F}_2 . By [20], each of these factors has the 2-sum property. Consequently, R^{ss} and hence R has the 2-sum property.

Let us now prove (2) \implies (3). Since R has the 2-sum property, we can write $1 = u + v$ where $u, v \in R^\times$. By definition, u is an exceptional unit in R .

Next, let us show that (3) \implies (4). Suppose that u is an exceptional unit. Then $\{1, u, 1 + u\}$ forms a triangle in G_R . Therefore, G_R cannot be bipartite.

Finally, let us show that (4) \implies (1). Suppose to the contrary that R has a quotient of the form \mathbb{F}_2 . Let $\Phi : R \rightarrow \mathbb{F}_2$ be such a quotient map. Let $U = \ker(\Phi)$ and $V = 1 + \ker(\Phi)$. Then if x, y both belong to either U or V then $\Phi(x - y) = 0$. As a result, $x - y \notin R^\times$. By definition, U, V form a partition of G_R with the bipartite property. We conclude that Φ cannot exist.

□

Corollary 2.2. *Suppose that there is a ring map $\Phi : R \rightarrow R'$. If R has the 2-sum property, then so does R' .*

Proof. Since R has the 2-sum property, R has an exceptional unit u . Then $\Phi(u)$ is an exceptional unit in R' . By Theorem 2.1, R' has the 2-sum property as well. \square

Remark 2.3. The converse of Corollary 2.2 is not true. Here is a counterexample: R' be a ring with the 2-sum property, $R = \mathbb{F}_2 \times R'$ and $\Phi : R \rightarrow R'$ is the canonical projection map.

Even under the assumption that R is a subring of R' , the converse is also not true. For example, let $R = \mathbb{F}_2 \times \mathbb{F}_2$ and $R' = M_2(\mathbb{F}_2)$. Let Φ be the diagonal embedding of $\mathbb{F}_2 \times \mathbb{F}_2$ into $M_2(\mathbb{F}_2)$. In this case R' has the 2-sum property but R does not. Below, we discuss various situations where the converse of Corollary 2.2 holds.

First, we deal with the study of rings that are additively generated by units. In general, it is not true that under the same assumption in Corollary 2.2, R' is additively generated by units when R is. For example, let $R = \mathbb{F}_2$, $R' = \mathbb{F}_2 \times \mathbb{F}_2$, and $\Phi : R \rightarrow R'$ be the diagonal embedding; namely $\Phi(a) = (a, a)$. Then R is generated by units but R' is not. However, this statement would be true if R' is a quotient of R .

Proposition 2.4. *Suppose that R' is a quotient of R . If R is additively generated by units, then R' is also additively generated by units.*

Proof. We give two proofs for this statement. The first one is purely algebraic. Suppose that $r \in R'$. Let \hat{r} be a lift of r to R . Then, \hat{r} is a sum of units in R . By projecting this property to R' and observing this projection sends units to units, we conclude that r is also a sum of units in R' .

The second proof is also along the same line, but it is somewhat more *geometric*. The quotient map between R and R' induces a graph morphism between G_R and $G_{R'}$ which is surjective at the vertex level. Since G_R is connected, $G_{R'}$ is connected as well. Consequently, R' is additively generated by units. \square

Next, we discuss the converse of Corollary 2.2 and Proposition 2.4 for certain classes of ring extensions. First, we study the case of group rings.

Proposition 2.5. *Let G be a finite group and S a finite ring. Then, the following statements hold*

- (1) $S[G]$ is additively generated by units if and only if S is additively generated by units.
- (2) If S has the 2-sum property if and only if $S[G]$ has the 2-sum property.

Proof. Let us first focus on (1). Suppose that $S[G]$ is generated by units. Since the augmentation map $\epsilon : S[G] \rightarrow S$ is surjective, Proposition 2.4 implies that S is also additively generated by units. Conversely, suppose that S is additively generated by units.

We claim that $S[G]$ is also additively generated by units. In fact, let us consider a basic element of $S[G]$ of the form sg where $s \in S$ and $g \in G$. Because S is additively generated by units, we can write $s = \sum_{u \in S^\times} u$. Therefore

$$sg = \sum_{u \in S^\times} ug.$$

By definition $ug \in S[G]^\times$. Therefore, ug belongs to the abelian group generated by elements of $S[G]^\times$. Since each element of $S[G]$ is a sum of basic elements of the form ug , we conclude that $S[G]$ is additively generated by units.

Let us now focus on (2). Suppose that S has the 2-sum property. Since S is a subring of $S[G]$, Corollary 2.2 implies that $S[G]$ also has the 2-sum property. Conversely, if $S[G]$ has the 2-sum property then using the augmentation map $\epsilon : S[G] \rightarrow S$ and Corollary 2.2, we conclude that S also has the 2-sum property. □

When S is a finite field, we have the following simple yet interesting result. We remark that the third property follows from our graph-theoretic argument. We are not aware of any purely algebraic proof for it.

Corollary 2.6. *Let F be a finite field and G a finite group.*

- (1) $F[G]$ is generated by units.
- (2) $F[G]$ has the 2-sum property if and only if $F \neq \mathbb{F}_2$.
- (3) When $F = \mathbb{F}_2$, $\mathbb{F}_2[G]$ has no quotient of the form $\mathbb{F}_2 \times \mathbb{F}_2$.

Another class of rings where the converse of Corollary 2.2 holds is the following.

Proposition 2.7. *Let $\Phi : R \rightarrow R'$ be an infinitesimal extension; namely, Φ is surjective, and the kernel of Φ is a nilpotent ideal. If R' has the 2-sum property, then so does R .*

Proof. We first claim that if $x \in R'$ and \hat{x} is a lift of x to R then \hat{x} is a unit in R . In fact, let y be the inverse of x and \hat{y} is a lift of y . Then $\Phi(\hat{x}\hat{y}) = xy = 1 = \Phi(1)$. This implies that $(\hat{x}\hat{y} - 1) \in \ker(\Phi)$. Consequently, $\hat{x}\hat{y} = 1 + m$ where $m \in \ker(\Phi)$. Because $\ker(\Phi)$ is nilpotent, $1 + m \in R^\times$ and hence $\hat{x} \in R^\times$.

Because R' has the 2-sum property, Theorem 2.1 implies that it has an exceptional unit u . Let \hat{u} be a lift of u to R . Since $\ker(\Phi)$ is nilpotent, both $\hat{u}, 1 - \hat{u}$ are units in R . By definition, \hat{u} is an exceptional unit in R . Therefore, R has the 2-sum property. □

2.2. Elements in a finite ring which are the sum of two units. In this section, we study the following question: which elements in a finite ring R can be written as a sum of 2 units? Let us first start with a motivational problem; namely, we study the sum of all units in a finite ring R . The case where R has the 2-sum property is relatively easy.

Proposition 2.8. *Suppose that R has the 2-sum property. Let S be a set which is stable under the left (or right) action of R^\times ; namely, $R^\times S \subset S$. Then*

$$T_S = \sum_{s \in S} s = 0.$$

In particular

$$T_{R^\times} = \sum_{u \in R^\times} u = 0.$$

Proof. Since S is stable under the action of R^\times ,

$$uT_S = \sum_{s \in S} us = \sum_{s \in S} s = T_S.$$

Therefore, $(u - 1)T_S = 0$ for all $u \in R^\times$. Furthermore, since R has the 2-sum property, by Theorem 2.1, it has an exceptional unit u . Since $u - 1 \in R^\times$, this would imply that $T_S = 0$. \square

One may wonder what happens in Proposition 2.8 if R does not have the 2-sum property. The argument given above shows that for all $u, v \in R^\times$, $(u + v)T_S = 0$. We see that, in order to answer this question, we need to dive a bit deeper into Skornyakov's problem. More precisely, we will need to answer the question raised at the beginning of this section: which elements of a ring R can be written as the sum of two units? In [30], we study this problem when the ring R is finite and commutative. We will show below that the same argument works for any finite ring as well. Let us recall that by the Artin-Wedderburn theorem, R^{ss} is isomorphic to a product of matrix rings $M_{n_i}(F_i)$ where $n_i \geq 1$ and F_i is a finite field. Let r be the number of factors of R^{ss} such that $n_i = 1$ and $F_i = \mathbb{F}_2$. Then $R^{\text{ss}} = \mathbb{F}_2^r \times S$, where S does not have \mathbb{F}_2 as a quotient. In particular, S has the 2-sum property by Theorem 2.1. We are now ready to state our result.

Proposition 2.9. *Let Φ be the composition $R \rightarrow R^{\text{ss}} := \mathbb{F}_2^r \times S \rightarrow \mathbb{F}_2^r$ where r is as above. Let $\ker(\Phi)$ be its kernel. Then, every element of $\ker(\Phi)$ is the sum of two units. Conversely, an element of R can be written as the sum of two units if and only if it is in $\ker(\Phi)$.*

Proof. Suppose that $x \in \ker(\Phi)$. Let \bar{x} be the image of x in $R^{\text{ss}} = \mathbb{F}_2^r \times S$. Because $\bar{x} \in \ker(\Phi)$, \bar{x} is of the form $(0, s)$ where $s \in S$. We know that S has the 2-sum property, so we can write $s = u_1 + u_2$ where $u_1, u_2 \in S^\times$. We then see that \bar{x} has the following presentation as the sum of two units

$$\bar{x} = (1, u_1) + (1, u_2).$$

Let v_1 (respectively v_2) be the lift of $(1, u_1)$ (respectively $(1, u_2)$) to R . Then $v_1, v_2 \in R^\times$ and $x = v_1 + v_2 + m$ for some $m \in \text{Rad}(R)$. Since $m \in \text{Rad}(R)$, $v_2 + m \in R^\times$. By letting $v_3 = v_2 + m$, we see that x is the sum of two units; namely v_1 and v_3 .

Conversely, suppose that x is the sum of two units. Then $\Phi(x)$ is also the sum of two units. Since the only unit in \mathbb{F}_2^r is 1, we conclude that $\Phi(x) = 1 + 1 = 0$. Equivalently, $x \in \ker(\Phi)$. □

Let us keep the same notation as in Proposition 2.9. We then have the following corollary.

Corollary 2.10. *Suppose that S is stable under the action of R^\times . Let*

$$T_S = \sum_{s \in S} s.$$

Then $aT_S = 0$ for all $a \in \ker(\Phi)$.

Proof. The fact that $aT_S = 0$ follows from the same argument as in Proposition 2.8 and the fact that every element in $\ker(\Phi)$ is the sum of two units. □

When $S = R^\times$, we can calculate T_{R^\times} explicitly.

Proposition 2.11. *$T_{R^\times} = \sum_{u \in R^\times} u \neq 0$ only if R is one of the following rings.*

- (1) $2 = 0$ in R , $|\text{Rad}(R)| = 2$ and $R/\text{Rad}(R) \cong \mathbb{F}_2^r$ for some $r \geq 1$. In this case, $T_{R^\times} = e$ where e is the unique non-zero element in $\text{Rad}(R)$.
- (2) $\text{Rad}(R) = 0$ and $R \cong \mathbb{F}_2^r \times (\prod_{i=1}^t F_i)$ where $r \geq 1$, F_i is a finite field of characteristics 2 and $|F_i| > 2$ for each $1 \leq i \leq t$. In this case $T_{R^\times} = (1_{\mathbb{F}_2^r}, 0)$.

Proof. First, we observe that if $R = R_1 \times R_2$ then

$$T_{R^\times} = |R_1^\times| |R_2^\times| (T_{R_1^\times}, T_{R_2^\times}).$$

In fact

$$\begin{aligned} T_{R^\times} &= \sum_{u_1 \in R_1^\times, u_2 \in R_2^\times} (u_1, u_2) = \sum_{u_1 \in R_1^\times} \sum_{u_2 \in R_2^\times} (u_1, u_2) \\ &= \sum_{u_1 \in R_1^\times} |R_2^\times| (u_1, T_{R_2^\times}) = |R_1^\times| |R_2^\times| (T_{R_1^\times}, T_{R_2^\times}). \end{aligned}$$

We consider three cases.

Case 1. $2 \neq 0$ in R . Then, we can decompose the set of units into pairs $\{u, -u\}$. In this case, $T_{R^\times} = 0$.

Case 2. $2 = 0$ in R and $\text{Rad}(R) \neq 0$. Let $e \in \text{Rad}(R)$. Then, we can decompose R^\times into pairs $\{u, u + e\}$. We then see that

$$T_{R^\times} = \frac{|R^\times|}{2} e.$$

We remark that there is an exact sequence of (multiplicative) abelian groups

$$1 \rightarrow 1 + \text{Rad}(R) \rightarrow R^\times \rightarrow (R/\text{Rad}(R))^\times \rightarrow 1.$$

Furthermore, since $2 = 0$ in R , $1 + \text{Rad}(R)$ is a 2-group. Therefore, we can conclude that that $\frac{|R^\times|}{2} \neq 0$ in R if and only if $|R^\times| = 2$. By the above exact sequence, this happens if and only if $|\text{Rad}(R)| = 2$ and $|(R/\text{Rad}(R))^\times| = 1$. The second condition only happens if $R/\text{Rad}(R) \cong \mathbb{F}_2^r$. In this case, $T_{R^\times} = e$.

Case 3. $2 = 0$ in R and $\text{Rad}(R) = 0$. In this case $R = \prod_{i=1}^d M_{n_i}(F_i)$ where $n_i \geq 1$ and F_i is a finite field of characteristics 2. We then have

$$T_{R^\times} = \left(\prod_{i=1}^d |M_{n_i}(F_i)^\times| \right) (T_{M_{n_1}(F_1)^\times}, \dots, T_{M_{n_d}(F_d)^\times}).$$

We know that

$$|M_{n_i}(F_i)^\times| = \prod_{i=0}^{n_i-1} (|F_i|^n - |F_i|^i),$$

which is even unless $n_i = 1$. Since $2 = 0$ in R , this would imply that $T_{R^\times} = 0$. Let us now assume that $n_i = 1$ for all $1 \leq i \leq d$. Then $|M_{n_i}(F_i)^\times| = |F_i^\times| = |F_i| - 1$ which is odd. We then have

$$T_{R^\times} = (T_{M_{n_1}(F_1)^\times}, \dots, T_{M_{n_d}(F_d)^\times}).$$

We know that $T_{F_i^\times} = 0$ if $|F_i| > 2$ and $T_{F_i} = 1$ if $F_i = \mathbb{F}_2$. Therefore, $T_{R^\times} \neq 0$ if and only if there exists $1 \leq i \leq d$ such that $F_i = \mathbb{F}_2$. □

We now utilize Proposition 2.9 to give a complete classification of gcd-graphs that are connected. We recall that a Cayley graph $\Gamma(R, S)$ is called a gcd-graph if S is stable under the left and right actions of R ; namely, $R^\times S R^\times = S$. This kind of graph is widely studied in the literature, starting with the work of Klotz-Sander on gcd-graphs over the cyclic ring \mathbb{Z}/n . Later developments study gcd-graphs over polynomial rings, unique factorization domains, finite chain rings (see [17, 23, 40]), and culminating with the most general definition in [30].

Let S_1, \dots, S_m be the orbits of the double coset $R^\times \backslash R / R^\times$. Then as explained in [29], $\Gamma(R, S)$ is a gcd-graph if S is a disjoint union of some of the cosets S_i 's. Namely, there exists a subset $I \subset \{1, 2, \dots, m\}$ such that $S = \bigsqcup_{i \in I} S_i$.

For each $x \in R$, we denote by I_x to be the two sided ideal generated by x . By definition, I_x is the following set

$$I_x = \left\{ \sum_i a_i x b_i \mid a_i, b_i \in R \right\}.$$

We remark that if x and y belong to the same coset; namely $x = u y v$ where $u, v \in R^\times$ then then $I_x = I_y$.

Theorem 2.12. *Let \mathbb{F}_2^r be the largest \mathbb{F}_2 -type quotient of R and $\Phi : R \rightarrow \mathbb{F}_2^r$ be the quotient map. Let $\Gamma(R, S)$ be a gcd-graph over R where $S = \bigsqcup_{i \in I} S_i$ for some $I \subset \{1, 2, \dots, m\}$. Let I_i*

be the two-sided ideals generated by $x_i \in S_i$ (I_i is independent of the choice of x_i). Then $\Gamma(R, S)$ is connected if and only if the following conditions hold

- (1) $\sum_{i \in I} I_i = R$.
- (2) The cube-like graph $\Gamma(\mathbb{F}_2^r, \Phi(S))$ is connected.

Proof. Suppose that $\Gamma(R, S)$ is connected. The map Φ induces a graph morphism $\Gamma(R, S) \rightarrow \Gamma(\mathbb{F}_2^r, \Phi(S))$. We note that, $\Phi(S)$ may contain 0. In this case, $\Gamma(\mathbb{F}_2^r, \Phi(S))$ will have a simple loop at each vertex, which does not affect its connectivity. Since $\Gamma(R, S)$ is connected and Φ is surjective at the vertex level, $\Gamma(\mathbb{F}_2^r, \Phi(S))$ is connected as well.

Let H be the abelian group generated by S . Then, H is the set of elements of the form $\sum_k n_k s_k$ where $n_k \in \mathbb{Z}$ and $s_k \in S$. We see that $H \subset \sum_{i \in I} I_i$. Furthermore, since $\Gamma(R, S)$ is connected, $H = R$. This shows that $\sum_{i \in I} I_i = R$ as well.

Conversely, suppose that both of the above conditions are satisfied. Let $r \in R$. We will show that $r \in H$. In fact, since $\Gamma(\mathbb{F}_2^r, \Phi(S))$ is connected, we can write $\Phi(r) = \sum_k n_k \Phi(s_k)$, where $n_k \in \mathbb{Z}$ and $s_k \in S$. By definition $(r - \sum_k n_k s_k) \in \ker(\Phi)$. Since $\sum_k n_k s_k \in H$, it is sufficient to show that $\ker(\Phi) \subset H$. In fact, let $t \in \ker(\Phi)$. Because $\sum_{i \in I} I_i = R$, we can write $1 = \sum_{i \in I} \sum_k a_{ik} x_i b_{ik}$, where $a_{ik}, b_{ik} \in R, x_i \in S$. Furthermore, as we explained previously, since $\Gamma(\mathbb{F}_2^r, \Phi(S))$ is connected, we can also write $1 = p + \sum_k m_k s_k$ where $p \in \ker(\Phi), s_k \in S$ and $m_k \in \mathbb{Z}$. We then have $t = \sum_k m_k (tx_k) + tp$. Since $t \in \ker(\Phi)$, t is a sum of two units; say $t = u + v$ where $u, v \in R^\times$. Then $tx_k = ux_k + vx_k$. By definition $ux_k, vx_k \in S$ and hence $tx_k \in H$. We claim that $tp \in H$ as well. In fact

$$tp = t(1)p = \sum_{i \in I} \sum_k (ta_{ik}) x_i (b_{ik} p).$$

Since ta_{ik} and $b_{ik} p$ is in the kernel of Φ , each of them is a sum of two units. Furthermore, since $R^\times S R^\times = S$, we conclude that $(ta_{ik}) x_i (b_{ik} p)$ is the sum of four elements in S . In particular, $(ta_{ik}) x_i (b_{ik} p) \in H$. This shows that $tp \in H$. We conclude that $t \in H$ and hence $H = R$. In other words, $\Gamma(R, S)$ is connected. \square

Finally, we conclude this section with some discussion of the unit graph (see [14] for a survey on this topic). This type of graphs and their variants, such as total graphs, have been extensively studied in the literature (see, for example, [3, 4]). We recall that the unit graph U_R is the graph whose vertex set is R . Additionally, two vertices a, b are adjacent if $a + b \in R^\times$. By a direct analogy with gcd-graphs, we can define the notion of a total gcd-graph as follows.

Definition 2.13. Let S be a set which is stable under the left and right action of R^\times . The total gcd-graph of R with respect to S , denoted by $T(R, S)$ is the graph whose vertex set is R . Furthermore, a and b are adjacent if and only if $a + b \in S$.

While it is not true in general that $T(R, S)$ and $\Gamma(R, S)$ are isomorphic (see [39, 36] for some study on the relationship between these two graphs), the following statement holds.

Proposition 2.14. *The following conditions are equivalent.*

- (1) $\Gamma(R, S)$ is connected.
- (2) S additively generates R .
- (3) $T(R, S)$ is connected.

Proof. The equivalence between (1) and (2) is well-known. The equivalence between (1) and (3) follows from an identical argument given in [2, Theorem 4.1]. \square

3. SUMS OF NORMALIZED UNITS

In this section, we study the n -sum property of R with respect to a general subset of R . In particular, we investigate the case where these subsets have arithmetic origins. To do so, we introduce the following formal definition.

Definition 3.1. Let S be a subset of R . We say that R has the n -sum property with respect to S if every element of R can be written as a sum of exactly n elements in S .

The case $S = R^\times$ is precisely Skornyakov's question. On the other hand, if $S = (R^\times)^k$ where k is a positive integer, our definition is directly related to the Waring problem (see [32, 33] for some work on this topic where the authors also approach this problem via graph theory). We remark that if $S \subset S'$ and R has the n -sum property with respect to S , then R also has the n -sum property with respect to S' . In particular, if $S \subset R^\times$, then R has the 2-sum property with respect to S only if R has no quotient of the form \mathbb{F}_2 . For the rest of this article, we will denote by U a subgroup of R^\times . Since we only deal with undirected graphs, we will also assume that $-1 \in U$.

We first discuss a general result that studies the n -sum property with respect to a quotient map.

Proposition 3.2. *Let R be a finite ring, and R' is a quotient of R equipped a quotient map $\Phi : R \rightarrow R'$. Let U be a subgroup of $(R')^\times$ and $U_\Phi = \{r \in R^\times \mid \Phi(r) \in U\}$. Suppose that $\ker(\Phi) \subset \text{Rad}(R)$. Then R has the n -sum property with respect to U_Φ if and only if R' has the n -sum property with respect to U .*

Proof. Suppose that R has the n -sum property with respect to U_Φ . Let $u \in R'$ and \hat{u} be a lift of u to R . Since R has the n -sum property with respect to U_Φ we can write $\hat{u} = \sum_{i=1}^n x_i$ where $x_i \in U_\Phi$. We then have $u = \Phi(\hat{u}) = \sum_{i=1}^n \Phi(x_i)$. By definition, $\Phi(x_i) \in U$. We conclude that R' has the n -sum property with respect to U .

Conversely, suppose that R' has the n -sum property with respect to U . We will show that R also has the n -sum property with respect to U_Φ .

First, we claim that if $y \in (R')^\times$ and \hat{y} is a lift of y then $\hat{y} \in R^\times$. In fact, let t be the inverse of y ; namely $yt = ty = 1$. Let \hat{t} be a lift of t . Then $\hat{y}\hat{t} = 1 + a$ for some $a \in \ker(\Phi)$. By our assumption, $\ker(\Phi) \subset \text{Rad}(R)$, so $1 + a \in R^\times$. This implies that $\hat{y} \in R^\times$ as well. As a consequence of this observation, we conclude that $U_\Phi = \Phi^{-1}(U)$.

Now, let $v \in R$, then $\Phi(v) = \sum_{i=1}^n y_i$ for $y_i \in U$. We then have $v = m + \sum_{i=1}^n \hat{y}_i = (m + y_1) + \sum_{i=2}^n \hat{y}_i$ where \hat{y}_i is a lift of y_i in R and $m \in \ker(\Phi)$. Since $U_\Phi = \Phi^{-1}(U)$, we know that $\hat{y}_1 + m \in U_\Phi$ and $\hat{y}_i \in U_\Phi$ for $2 \leq i \leq n$. We conclude that v can be written as the sum of n elements in U_Φ . We conclude that R has the n -sum property with respect to U_Φ . \square

We discuss below some partial results for standard choices of R and U in the literature.

3.1. Sums of normalized units in matrix rings. First, we deal with the case of matrix rings with coefficients in a finite field.

Proposition 3.3. *Let F be a finite field and $n \geq 2$. Let $R = M_n(F)$ and $U = \pm SL_n(F)$ where $SL_n(F) = \{A \in M_n(F) \mid \det(A) = 1\}$. Then R has the 2-sum property with respect to U .*

Proof. Let $C \in M_n(F)$. We claim there exist $A, B \in SL_n(F)$ such that

$$C = A - B.$$

Let $r = \text{rank}(C)$. By the theory of Gauss eliminations, there exist $P, Q \in GL_n(F)$ with

$$PCQ = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = I_r \oplus 0_{n-r}.$$

Write $C' := PCQ$. It suffices to write $C' = A' - B'$ with $\det(A') = \det(B') = \alpha$ where $\alpha = \det(P) \det(Q)$, since then

$$C = P^{-1}A'Q^{-1} - P^{-1}B'Q^{-1}$$

and $P^{-1}A'Q^{-1}, P^{-1}B'Q^{-1} \in SL_n(F)$.

Our approach is based on the following determinant identity for an $n \times n$ matrix of the cyclic form

$$\det \begin{bmatrix} x_1 & a_1 & & & \\ & x_2 & a_2 & & \\ & & \ddots & \ddots & \\ & & & x_{n-1} & a_{n-1} \\ a_n & & & & x_n \end{bmatrix} = x_1 x_2 \cdots x_n + (-1)^{n+1} a_1 a_2 \cdots a_n.$$

In this matrix, every other entry is 0. We construct matrices A' and B' of the same cyclic type so that $A' - B' = I_r \oplus 0_{n-r}$. Concretely, choose entries x_i and a_i and set

$$A' = \begin{bmatrix} 1+x_1 & a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1+x_2 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1+x_r & a_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & a_{r+1} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-1} \\ a_n & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where the first r diagonal entries are $1+x_1, \dots, 1+x_r$ and the remaining $(n-r)$ diagonal entries are 0. Similarly, define

$$B' = \begin{bmatrix} x_1 & a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & x_2 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x_r & a_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & a_{r+1} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-1} \\ a_n & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Then $A' - B' = I_r \oplus 0_{n-r}$. We consider two cases.

Case 1: $r = n$. Choose

$$x_1 = -1, \quad x_2 = \cdots = x_n = 0, \quad a_1 = (-1)^{n+1}\alpha, \quad a_2 = \cdots = a_n = 1,$$

Because $x_1 + 1 = 0$

$$\det(A') = (1+x_1) \cdots (1+x_n) + (-1)^{n+1}a_1 \cdots a_n = \alpha,$$

Similarly $\det(B') = \alpha$.

For example, when $n = 3$,

$$I_3 = \begin{bmatrix} 0 & \alpha & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} - \begin{bmatrix} -1 & \alpha & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Case 2: $r < n$. Take $x_{r+1} = \cdots = x_n = 0$, and set

$$a_1 = (-1)^{n+1}\alpha, \quad a_2 = \cdots = a_n = 1.$$

Then

$$\det(A') = (1+x_1) \cdots (1+x_r) \cdot 0 + (-1)^{n+1}a_1 \cdots a_n = \alpha,$$

$$\det(B') = x_1 \cdots x_r \cdot 0 + (-1)^{n+1}a_1 \cdots a_n = \alpha,$$

For example, for $n = 3$ and $r = 2$, we have

$$I_2 \oplus 0_1 = \begin{bmatrix} 1 & \alpha & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & \alpha & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

□

By the same argument as in Proposition 2.8, we have the following corollary.

Corollary 3.4. *Let $n \geq 2$ and F be a finite field. Then $\sum_{u \in SL_n(F)} u = 0$.*

3.2. Sum of units in a group ring. Let F be a finite field and $U \subset F^\times$ such that F has the n -sum properties with respect to U . This necessarily implies that $F \neq \mathbb{F}_2$ and we will make this assumption throughout this section.

Let G be a finite group and $R = F[G]$ be the group algebra of G with coefficients in F . Let $\varepsilon_G : F[G] \rightarrow F$ be the augmentation map and $U_{\varepsilon_G} = \{r \in F[G]^\times \mid \varepsilon(r) \in U\}$. In this section, we study the following question.

Question 3.5. Suppose that F has the n -sum property with respect to U . Is it true that $F[G]$ also has the n -sum property with respect to U_{ε_G} ?

Remark 3.6. We can easily show that $F[G]$ always has the N -sum property with respect to U_{ε_G} where $N = n|G|$. In fact, a basic element of $F[G]$ is of the form $\sum_g a_g g$. We can write each a_g as the sum of n -terms in U . Each of these terms when multiplied by g is an element of U_{ε_G} . Question 3.5 asks for a stronger statement, namely $F[G]$ has the n -sum property.

First, we deal with the easy case where $|G|$ is a p -group with $p = \text{char}(F)$. In this case the answer to Question 3.5 is affirmative.

Proposition 3.7. *Suppose that G is a p -group with $p = \text{char}(F)$. Then $F[G]$ has the n -sum property.*

Proof. It is well-known that if G is a p -group and $p = \text{char}(F)$ then $\text{Rad}(F[G]) = \Delta(G)$ where $\Delta(G) = \ker(\varepsilon_G)$. Since $F[G]/\Delta(G) \cong F$ has the n -sum property with respect to U , by Proposition 3.2, $F[G]$ has the n -sum property with respect to U_{ε_G} . □

Next, we study Question 3.5 in the other direction: namely, when $F[G]$ is semisimple or close to being semisimple. To do so, we need to introduce some terminology. Let H be a normal subgroup of G . We will denote by $\varepsilon_{G,H}$ the augmentation map $F[G] \rightarrow F[G/H]$. The kernel of $\varepsilon_{G,H}$ will be denoted by $\Delta(G, H)$.

Proposition 3.8. *Suppose that $H \triangleleft G$ and $|H|$ is invertible in F . If $F[G/H]$ has the n -sum property with respect to $U_{\varepsilon_{G/H}}$, then $F[G]$ has the n -sum property with respect to U_{ε_G} .*

Proof. Let $e_H = \frac{1}{|H|} \sum_{h \in H} h$. As explained in [22, Proposition 3.6.7], e_H is a central idempotent of $F[G]$ and we have the following isomorphism of rings

$$F[G] \cong F[G]e_H \oplus F[G](1 - e_H).$$

Furthermore, $F[G]e_H \cong F[G/H]$ and $F[G](1 - e_H) \cong \Delta(G, H)$. Under this isomorphism, the restriction of the augmentation map ε_G on $F[G/H]$ is nothing but $\varepsilon_{G/H}$. On the other hand, the restriction of ε_G on $\Delta(G, H)$ is 0. We then see that

$$U_\varepsilon = U_{\varepsilon_{G/H}} \oplus \Delta(G, H)^\times.$$

By Corollary 2.6, $F[G]$ has the 2-sum property with respect to $F[G]^\times$. Consequently, by Corollary 2.2, $\Delta(G, H)$ also has the 2-sum property with respect to $\Delta(G, H)^\times$. Since $n \geq 2$, $\Delta(G, H)$ has the n -sum property with respect to $\Delta(G, H)^\times$ as well. By our assumption, $F[G/H]$ has the n -sum property with respect to $U_{\varepsilon_{G/H}}$. We conclude that $F[G]$ has the n -sum property with respect to U_ε . \square

We discuss some corollaries of Proposition 3.8.

Corollary 3.9. *Suppose that $|G|$ is invertible in F . Then $F[G]$ has the n -sum property with respect to U_ε .*

Proof. In this case, we can take $G = H$ as in Proposition 3.8. Then, $F[G/H] = F$, which has the 2-sum property with respect to U by our assumption. \square

By Proposition 3.7 and Corollary 3.9, we have the following proposition.

Proposition 3.10. *If G is a p -group then $F[G]$ has the n -sum property with respect to U_{ε_G} .*

Proof. The case $p = \text{char}(F)$ is proved in Proposition 3.7 and the case $p \neq \text{char}(F)$ is proved in Corollary 3.9. \square

We discuss another corollary where the answer to Question 3.5 is affirmative.

Corollary 3.11. *Suppose that $H \triangleleft G$ and $|H|$ is invertible in F . Assume further that G/H is a p -group. Then $F[G]$ has the n -sum property with respect to U_{ε_G} .*

Proof. This statement follows from Proposition 3.7 and Proposition 3.8. \square

We discuss another orthogonal variant of Proposition 3.8.

Proposition 3.12. *Suppose that H is a normal p -subgroup of G where $p = \text{char}(F)$. If $F[G/H]$ has the n -sum property with respect to $U_{\varepsilon_{G/H}}$, then $F[G]$ has the n -sum property with respect to U_{ε_G} . In particular, if H is a normal p -Sylow subgroup of G and $F[G/H]$ has the n -sum property with respect to $U_{\varepsilon_{G/H}}$, then $F[G]$ has the n -sum property with respect to U_{ε_G} .*

Proof. By [31, Theorem 16.6] and the fact that H is a p -group, we know that $\Delta(G, H) \subset \text{Rad}(F(G))$. This first statement then follows from Proposition 3.2.

The second statement follows from Proposition 3.2 and Corollary 3.9. \square

Other than the above scenerios, it is unclear to us whether Question 3.5 has an affirmative answer for all finite groups G . We provide below a class of groups which we know the answer to.

Proposition 3.13. *Suppose that G is either an abelian group or a dihedral group. Then $F[G]$ has the n -sum property with respect to U_{ε_G}*

Proof. We will give a proof for the case $G = D_{2n}$ where $n \geq 1$. The case where G is abelian is easier and can be proved in the same way. For $n = 1$ or $n = 2$, D_{2n} is a 2-group so the statement holds by Proposition 3.10. Suppose that it has been proved for all $m < n$. We will show that it also holds for D_{2n} . If n is a power of 2 then the statement holds by Proposition 3.10. Otherwise, suppose that there exists $p \mid n$ such that $p \neq 2$. Let $\alpha = v_p(n)$. Then, we can find an exact sequence of the form

$$1 \rightarrow \mathbb{Z}/p^\alpha \rightarrow D_{2n} \rightarrow D_{2n/p^\alpha} \rightarrow 1.$$

If $p = \text{char}(F)$, then our statement follows from Proposition 3.12 and our induction hypothesis applied to D_{2n/p^α} . On the other hand, if $p \neq \text{char}(F)$, then it follows from Proposition 3.8 and the induction hypothesis applied to D_{2n/p^α} . \square

3.3. Sums of normalized units in a finite extension of fields. In this section, we discuss another situation where normalized units appear quite naturally. More precisely, we are interested in the following question.

Question 3.14. Let L/F be a non-trivial finite field extension of finite fields. Let $N : L \rightarrow F$ be the norm map, $U_{L/F} = \{u \in L^\times \mid N(u) = 1\}$ and $U_{L/F}^\pm = \{\pm u \mid u \in U_{L/F}\}$. Does there exist a positive integer n such that L has the n -sum property with respect to $U_{L/F}^\pm$?

We remark that we need to consider $U_{L/F}^\pm$ to ensure that the graph $\Gamma(L, U_{L/F}^\pm)$ is undirected. Additionally, if $[L : F]$ is even, then $N(-1) = 1$ and hence $U_{L/F} = U_{L/F}^\pm$.

While we do not have a complete answer for Question 3.14, we will prove some partial results. More precisely, we will prove the following theorem.

Theorem 3.15. *Let $F = \mathbb{F}_q$ and L/F be a non-trivial finite field extension. Let $U_{L/F}^\pm$ be as above. The following statements hold*

- (1) L is additively generated by $U_{L/F}^\pm$. In particular, the Cayley graph $\Gamma(L, U_{L/F}^\pm)$ is always connected.
- (2) If $[L : F] \geq 4$, then L has the 2-sum property with respect to $U_{L/F}^\pm$.
- (3) If $[L : F] = 3$, then L has the 4-sum property with respect to $U_{L/F}^\pm$. Furthermore, if the equation $x^{q-1} + y^{q-1} + z^{q-1} = 0$ has a solution in L^\times , then L has the 3-sum property with respect to $U_{L/F}^\pm$.

We will prove Theorem 3.15 by a series of results in field theory, which might be of independent interest.

Proposition 3.16. *Let L/F be a finite Galois extension of fields (which might not need to be finite). Let K be a proper subfield of L and $\sigma \in \text{Gal}(L/K)$ such that $\sigma \neq 1$. Then, there exists $x \in L^\times$ such that $\frac{\sigma(x)}{x} \notin K$. In particular, $U_{L/F} \not\subset K$.*

Proof. Suppose to the contrary that $\sigma(x)/x \in K$ for all $x \in L^\times$. We claim that this would lead to the equality that $L = L^{\sigma=1} \cup K$, which is a contradiction.

For each x , there exists $f(x) \in K$ such that $\sigma(x) = f(x)x$. Similarly, we have $\sigma(x+1) = f(x+1)(x+1)$. This implies that

$$(x+1)f(x+1) - xf(x) = \sigma(x+1) - \sigma(x) = 1.$$

We can rewrite this as

$$x[f(x+1) - f(x)] = 1 - f(x+1).$$

If $f(x+1) - f(x) \neq 0$ then $x \in K$. Otherwise, if $f(x+1) = f(x)$, then $1 - f(x+1) = 0$ and hence $f(x) = 1$. This would imply that $\sigma(x) = x$; or equivalently $x \in L^{\sigma=1}$. In all cases, $x \in L^{\sigma=1} \cup K$. □

Proposition 3.17. *Let L be a finite field and $U \subset L^\times$. The following conditions are equivalent*

- (1) $\Gamma(L, U)$ is connected.
- (2) $U \not\subset K$ for all proper subfield K of L .

Proof. Let S be the abelian group generated by U . We know that $U \subset S$. Furthermore, we can check that S is a subring of L . Since L is a field, S is even a subfield of L . By our assumption, for each proper subfield K of L , $U \not\subset K$, and hence $S \not\subset K$. This must imply that $S = L$. Therefore, $\Gamma(L, U)$ is connected. □

We then see that the first part of Theorem 3.15 follows from Proposition 3.16 and Proposition 3.17. Let us now prove the second part of Theorem 3.15. By Hilbert 90, every normalized units in L/F is of the form $\frac{\sigma_q(x)}{x} = x^{q-1}$ where $q = |F|$ and σ_q is the Frobenius map $\sigma_q(x) = x^q$. The second part of Theorem 3.15 follows from the following result.

Lemma 3.18. *Let $F = \mathbb{F}_q$ and $[L : F] \geq 4$. Then for each $b \in L$, there exists $x, y \in L^\times$ such that either $x^{q-1} - y^{q-1} = b$ or $x^{q-1} + y^{q-1} = b$.*

Proof. If $b = 0$ then we can take $x = y = 1$, and we have $1^{q-1} - 1^{q-1} = 0$. Let us suppose that $b \neq 0$. We will show that we can find $x, y \in L^\times$ such that $x^{q-1} + y^{q-1} = b$.

Let $k = [L : F]$ and hence $L = \mathbb{F}_{q^k}$. We modify the proof given in [6, Theorem 3]. Let $N_2(b)$ be the number of solutions of the equation $x^{q-1} + y^{q-1} = b$. Let $M_2(b)$ be the number of solutions such that $x, y \in L^\times$. We need to show that $M_2(b) > 0$ for

each $b \in L$. For each b , the equation $x^{q-1} = b$ has at most $q - 1$ solutions. Therefore $M_2(b) \geq N_2(b) - 2(q - 1)$. On the other hand, by [16, Corollary 1, p. 57], we have

$$|N_2(b) - q^k| \leq (q - 1)^2 q^{k/2}.$$

This shows that $N_2(b) \geq q^k - (q - 1)^2 q^{k/2}$ and hence

$$M_2(b) \geq q^k - (q - 1)^2 q^{k/2} - 2(q - 1).$$

If $k \geq 4$ then

$$M_2(b) \geq [q^2 - (q - 1)^2] q^{k/2} - 2(q - 1) = (2q - 1) q^{k/2} - 2(q - 1) > (2q - 1) - 2(q - 1) = 1.$$

□

Remark 3.19. We can show that if k is odd then we cannot find $x, y \in L^\times$ such that $0 = x^{q-1} + y^{q-1}$. In fact, if we let $z = x/y$ then $z^{q-1} = -1$. We then have

$$1 = z^{q^k-1} = (z^{q-1})^{\frac{q^k-1}{q-1}} = -1.$$

This would contradict the fact that q is odd. Therefore, it is important to use $U_{L/F}^\pm$ instead of $U_{L/F}$.

The last part of Theorem 3.15 follows from the following lemma.

Lemma 3.20. *Suppose that $F = \mathbb{F}_q$ and $[L : F] = 3$. Then for each $b \in L^\times$,*

$$x_1^{q-1} + \dots + x_3^{q-1} = b,$$

has a solution such that $x_1, x_2, \dots, x_4 \in L^\times$.

Proof. If $q = 2$, then $U_{L/F} = L^\times$. Since L has the 2-sum property with respect to L^\times , the above statement holds. We will assume that $q \geq 3$. We will prove this statement using a similar argument as in the proof of Lemma 3.18. Let $N_m(b)$ be the number of solutions of the equation

$$x_1^{q-1} + x_2^{q-1} + \dots + x_m^{q-1} = b.$$

Similarly, let $M_m(b)$ be the number of solutions such that $x_1, x_2, \dots, x_m \in L^\times$. As before, our goal is to show that $M_3(b) > 0$. We have the following lower bound for $M_m(b)$

$$M_m(b) \geq N_m(b) - mN_{m-1}(b).$$

By [16, Corollary 1, p. 57], we have the following estimate

$$|M_m(b) - q^{k(m-1)}| \leq (q - 1)^m q^{k \frac{m-1}{2}}.$$

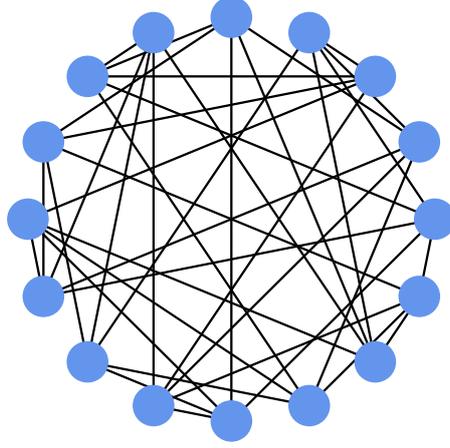


FIGURE 1. The Cayley graph $\Gamma(\mathbb{F}_{16}, U_{\mathbb{F}_{16}/\mathbb{F}_4}^\pm)$

In our particular case where $[L : F] = 3$, we have $N_3(b) \geq q^6 - q^3(q-1)^3$. Similarly, we have $N_2(b) \leq q^3 + q^3(q-1)^{1.5}$. We conclude that

$$\begin{aligned} M_3(b) &\geq q^6 - q^3(q-1)^3 - 3(q^3 + q^3(q-1)^{1.5}) \\ &> q^6 - q^3(q-1)^3 - 6q^{4.5} \\ &> q^3(q^3 - (q-1)^3 - q^{1.5}) = q^3(3q^2 - 3q + 1 - 6q^{1.5}) \end{aligned}$$

We can see that if $q \geq 4$, then $M_3(b) > 0$. On the other hand, when $q = 3$, we can check directly that $M_3(b) > 0$ as well. □

One may ask whether similar statements in Theorem 3.15 hold when $[L : F] = 2$. Unfortunately, they are not, but there are some patterns. For example, let $F = \mathbb{F}_4$ and $L = \mathbb{F}_{16}$. Here $[L : K] = 2$ and the graph $\Gamma(L, U_{L/F}^\pm)$ is shown in Fig. 1. Brute-force computations in SageMath show that L does not have the 3-sum property with respect to $U_{L/F}^\pm$. A visual proof of this fact is that, if one squints enough at Fig. 1, there are no 3-cycles in $\Gamma(L, U_{L/F}^\pm)$.

The n -sum properties for $n \in \{2, 3\}$ for other values of q are summarized in Table 1. The data suggest when that when q is odd, L has the 3-sum property with respect to U_{L/F_q}^\pm only if $q \not\equiv 1 \pmod{6}$. On the other hand, the data also suggest that the 2-sum property with respect to $U_{L/F}^\pm$ fails for $q \geq 4$ (note that in this case $U_{L/F} = U_{L/F}^\pm$ since $N(-1) = (-1)^2 = 1$). We will provide below an explanation for these observations for the case $q \equiv 1 \pmod{6}$. (see Lemma 3.21.)

When $[L : F] = 3$, as explained in Remark 3.19, L does not have the 2-sum property with respect to $U_{L/F}$. Theorem 3.15, on the other hand, shows that L has the 3-sum property with respect to $U_{L/F}^\pm$. Our numerical data shows that for $2 \leq q \leq 32$, L has the 2-sum property with respect to $U_{L/F}^\pm$. It would be interesting to either prove or disprove

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27	29	31	32
2-sum property	T	T	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
3-sum property	T	T	F	T	F	F	T	T	F	F	T	F	T	F	T	T	F	T

TABLE 1. n -sum property when $[L : F] = 2$.

this statement for all q . If it is true, then for each b , at least one of the following equations has a solution in $(L^\times)^2$:

$$x_1^{q-1} - x_2^{q-1} = b, x_1^{q-1} + x_2^{q-1} = b, x_1^{q-1} + x_2^{q-1} = -b.$$

Lemma 3.21. *If $q \equiv 1 \pmod{6}$, then the equation*

$$x_1^{q-1} + x_2^{q-1} = 1,$$

has no solution such that $x_1, x_2 \in \mathbb{F}_{q^2}^\times$. Similarly, the equation

$$x_1^{q-1} + x_2^{q-1} + x_3^{q-1} = 0,$$

has no solution such that $x_1, x_2, x_3 \in \mathbb{F}_{q^2}^\times$.

Proof. Suppose $x_1, x_2 \in \mathbb{F}_{q^2}^\times$ such that $x_1^{q-1} + x_2^{q-1} = 1$. Then, applying the Frobenius automorphism σ_q to both sides, we get $x_1^{q(q-1)} + x_2^{q(q-1)} = 1$. Since $x_1, x_2 \in \mathbb{F}_{q^2}$, $x_1^{q^2-1} = x_2^{q^2-1} = 1$. This shows that $x_1^{q(q-1)} = 1/x_1^{q-1}$ and $x_2^{q(q-1)} = 1/x_2^{q-1}$. We then see that

$$x_1^{q-1} + x_2^{q-1} = (x_1^{q-1})(x_2^{q-1}) = 1.$$

Therefore, $u_1 := x_1^{q-1}, u_2 := x_2^{q-1}$ are roots of the equation $T^2 - T + 1 = 0$. Since $T^3 + 1 = (T + 1)(T^2 - T + 1)$, we conclude that $u_1^6 = u_2^6 = 1$. On the other hand, $u_1^{q+1} = x_1^{q^2-1} = 1$. Since $q + 1 \equiv 2 \pmod{6}$, we must have $u_1^2 = 1$. Similarly, $u_2^2 = 1$. This would imply that $u_1, u_2 \in \{1, -1\}$. However, it would contradict the fact that $u_1 + u_2 = 1$.

For the second equation, we can homogenize the equation by dividing both sides by u^{q-1} where $u \in \mathbb{F}_{q^2}^\times$ such that $x_3^{q-1} = -u^{q-1}$ (this is possible since $N(-1) = (-1)^2 = 1$). The result then follows from the first part. \square

4. SUMS OF UNITS AND PERFECT STATE TRANSFER ON GRAPHS

Let G be an undirected simple graph with adjacency matrix A_G . The continuous-time quantum walk on G is given by $F(t) = \exp(iA_G t)$. Perfect state transfer (PST) occurs in graph G when there exist distinct vertices a and b and some positive real number t such that $|F(t)_{ab}| = 1$. This phenomenon is first studied in [8] within the framework of quantum spin networks. Following this foundational work, numerous articles have investigated PST on arithmetic graphs (see [5, 7, 11, 35] among others in this research direction). It is known that any regular graph exhibiting PST must be integral—that is, all its eigenvalues are integers (see [11, 35]). Cayley graphs are, therefore, particularly

relevant because there is a rather complete classification of integral Cayley graphs (see [12, 18, 26, 38]). In this section, we study the relationship between the *non-existence* of PST on a Cayley graph defined over a ring R and the n -property of R . To do spectral analysis, we will restrict ourselves to a class of rings called the \mathbb{Z}/m -symmetric Frobenius rings (see [15, 19]). We remark that every finite ring is an algebra over \mathbb{Z}/m for some m (for example, m could be the characteristics of R). This kind of ring was first studied by Lamprecht in his investigation into Gauss sums and Ramanujan sums. We recall that a \mathbb{Z}/m -algebra R is called a finite symmetric Frobenius ring if it is equipped with a linear functional $\psi : R \rightarrow \mathbb{Z}/m$ such that

- (1) $\psi(ab) = \psi(ba)$ for $a, b \in R$.
- (2) ψ is non-degenerate, meaning that the kernel of ψ does not contain any left-ideal in R .

Associated to ψ , we can define a complex-valued character χ of $(R, +)$ by the rule $\chi(a) = \zeta_m^{\psi(a)}$ where ζ_m is a fixed primitive m -root of unity. The non-degenerate property of ψ implies that each character of $(R, +)$ is of the form χ_r where $\chi_r : R \rightarrow \mathbb{C}^\times$ such that $\chi_r(a) = \chi(ra)$. All examples that we discussed in Section 3 are symmetric Frobenius rings. Furthermore, all finite semisimple rings are symmetric Frobenius rings (see [15]).

For a Cayley graph $\Gamma(R, S)$ over R , its spectrum is parametrized by R . More precisely, the spectrum is the multiset $\{\lambda_r\}_{r \in R}$ where

$$\lambda_r = \sum_{s \in S} \chi_r(s) = \sum_{s \in S} \chi(rs) = \sum_{s \in S} \zeta_m^{\psi(rs)}.$$

In [27], following the method of [5], we prove the following

Proposition 4.1. ([27, Theorem 4.1]) *Let $s \in R \setminus \{0\}$. There exists perfect state transfer from 0 to s at time t if and only if for all $r_1, r_2 \in R$*

$$(\lambda_{r_1} - \lambda_{r_2}) \frac{t}{2\pi} + \frac{\psi((r_1 - r_2)s)}{m} \equiv 0 \pmod{1}.$$

Let us now explain the connection between the existence of PST on a Cayley graph and the n -sum property. Let Δ be the abelian group generated the difference $r_1 - r_2$ whenever $\lambda_{r_1} = \lambda_{r_2}$. Proposition 4.1 implies that if there exists a PST between 0 and s at time t , then $\psi(ds) = 0$ for each $d \in \Delta$. In particular, $\Delta = R$, then the non-degeneracy of ψ implies that $s = 0$, which is a contradiction.

Let U be a subgroup of R^\times such that $-1 \in U$. The Cayley graph $\Gamma(R, S)$ is called an U -unitary Cayley graph if S is stable under the left and right action of U (when $U = R^\times$, we recover the definition of a gcd-graph as explained in Section 2.) In [27, Proposition 3.6], using supercharacter theory, we show that if $r_1 = u_1 r_2 u_2$ where $u_1, u_2 \in U$, then $\lambda_{r_1} = \lambda_{r_2}$. Consequently, if we denote Δ_U to be the abelian group generated by $r_1 - r_2$ where $r_1, r_2 \in U$, then $\Delta_U \subset \Delta$. We then have the following theorem.

Theorem 4.2. *Let $U \subset R^\times$ such that $-1 \in U$. Suppose that R has the n -sum property with respect to U . Let $\Gamma(R, S)$ be an U -unitary Cayley graph. Then $\Gamma(R, S)$ has no PST.*

Proof. We claim that $\Delta_U = R$. In fact, there exists a positive integer m such that R has the $2m$ -sum property with respect to U (we can take $m = \lceil n/2 \rceil$.) By definition, $\Delta_U = R$. Since $\Delta_U \subset \Delta$, this shows that $\Delta = R$ as well. Consequently, there is no PST on $\Gamma(R, S)$. \square

We have the following immediate corollary.

Corollary 4.3. *Let R be a finite ring with the 2-sum property. Let $\Gamma(R, S)$ be a gcd-graph over R . Then $\Gamma(R, S)$ has no PST.*

Finally, we show that there is no PST on the graph $\Gamma(L, U_{L/F}^\pm)$ studied in Section 3.

Proposition 4.4. *Let L/F be a finite extension of finite fields such that $L \neq F$. Then, the graph $\Gamma(L, U_{L/F}^\pm)$ has no PST.*

Proof. If $[L : F] \geq 3$, then L has the 3-sum property with respect to $U_{L/F}^\pm$. Therefore, by Theorem 4.2, $\Gamma(L, U_{L/F}^\pm)$ has no PST. Unfortunately, this argument does not work when $[L : F] = 2$ since we do not know whether L has the n -sum property with respect to $U_{L/F}^\pm$. We will use another argument which works for all cases.

Let Δ_2 be the abelian group generated by elements of the form $r_1 - r_2$ where $r_1, r_2 \in L^\times$ and $N_{L/F}(r_1) = N_{L/F}(r_2)$. By definition, $r_1 = ur_2$ where $N(u) = 1$ and hence, $u \in U_{L/F}^\pm$. We conclude that r_1 and r_2 give rise to the same eigenvalue of $\Gamma(L, U_{L/F}^\pm)$; namely $\lambda_{r_1} = \lambda_{r_2}$. This shows that $\Delta_2 \subset \Delta$. We claim that Δ_2 is an ideal in L . Clearly, Δ_2 is closed under addition. Let us now show that $a\Delta_2 \subset \Delta_2$ for each $a \in L$. In fact, we have $a(r_1 - r_2) = (ar_1) - (ar_2)$. Since $N(ar_1) = N(ar_2)$, we conclude that $a(r_1 - r_2) \in \Delta_2$ and hence $a\Delta_2 \subset \Delta_2$. This shows that Δ_2 is an ideal in L . However, since L is a field, we must have $\Delta_2 = L$ and hence $\Delta = L$. We conclude that there is no PST on $\Gamma(L, U_{L/F}^\pm)$. \square

ACKNOWLEDGEMENTS

We thank Sunil Chebolu for alerting us to the work [20], which initiated our study in this line of research. We thank Professor David Anderson for his insightful correspondence on his work on total graphs.

REFERENCES

1. R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel, and D. Pritikin, *On the unitary Cayley graph of a finite ring*, Electron. J. Combin. **16** (2009), no. 1, Research Paper 117, 13 pages.
2. Eman Alluqmani, *Unit graphs of group rings*, AIMS Mathematics **11** (2026), no. 1, 2907–2934.
3. David F Anderson and Ayman Badawi, *The total graph of a commutative ring*, Journal of algebra **320** (2008), no. 7, 2706–2719.

4. N. Ashrafi, H. R. Maimani, M. R. Pournaki, and S. Yassemi, *Unit graphs associated with rings*, *Comm. Algebra* **38** (2010), no. 8, 2851–2871. MR 2730284
5. M. Bašić, M. D. Petković, and D. Stevanović, *Perfect state transfer in integral circulant graphs*, *Applied Mathematics Letters* **22** (2009), no. 7, 1117–1121.
6. Vitaly Bergelson, Andrew Best, and Alex Iosevich, *Sums of powers in large finite fields: a mix of methods*, *The American Mathematical Monthly* **128** (2021), no. 8, 701–718.
7. Wang-Chi Cheung and Chris Godsil, *Perfect state transfer in cubelike graphs*, *Linear Algebra and Its Applications* **435** (2011), no. 10, 2468–2474.
8. Matthias Christandl, Nilanjana Datta, Artur Ekert, and Andrew J Landahl, *Perfect state transfer in quantum spin networks*, *Physical review letters* **92** (2004), no. 18, 187902.
9. Maria Chudnovsky, Michal Cizek, Logan Crew, Ján Mináč, Tung T. Nguyen, Sophie Spirkl, and Nguyen Duy Tân, *On prime Cayley graphs*, *J. Comb.* **17** (2026), no. 2, 223–252. MR 5030071
10. G. Ehrlich, *Unit-regular rings*, *Portugaliae Mathematica* **27** (1968), 209–212.
11. Chris Godsil, *State transfer on graphs*, *Discrete Mathematics* **312** (2012), no. 1, 129–147.
12. Chris Godsil and Pablo Spiga, *Integral normal Cayley graphs*, *Journal of Algebraic Combinatorics* **62** (2025), no. 1, 20.
13. Brendan Goldsmith, Simone Pabst, and Audrey Scott, *On unit sum number of rings and modules*, (1998).
14. Ralph P. Grimaldi, *Graphs from rings*, *Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing* (Boca Raton, FL, 1989), vol. 71, 1990, pp. 95–103. MR 1041619
15. Thomas Honold, *Characterization of finite Frobenius rings*, *Archiv der Mathematik* **76** (2001), no. 6, 406–415.
16. Jean-René Joly, *Equations et varietes algebriques sur un cops fini*, *L'Enseignement mathématique* **19** (1973), 1–117.
17. Dariush Kiani, Mohsen Molla Haji Aghaei, Yotsanan Meemark, and Borworn Suntornpoch, *Energy of unitary Cayley graphs and gcd-graphs*, *Linear algebra and its applications* **435** (2011), no. 6, 1336–1343.
18. Walter Klotz and Torsten Sander, *Some properties of unitary Cayley graphs*, *The Electronic Journal of Combinatorics* **14** (2007), no. 1, R45, 12 pages.
19. Erich Lamprecht, *Allgemeine theorie der Gaußschen Summen in endlichen kommutativen Ringen*, *Mathematische Nachrichten* **9** (1953), no. 3, 149–196.
20. N. J. Lord, *Matrices as sums of invertible matrices*, *Mathematics Magazine* (1987).
21. HR Maimani, MR Pournaki, and S Yassemi, *Rings which are generated by their units: a graph theoretical approach*, *Elemente der Mathematik* **65** (2010), no. 1, 17–25.
22. César Polcino Milies and Sudarshan K Sehgal, *An introduction to group rings*, vol. 1, Springer Science & Business Media, 2002.
23. Ján Mináč, Tung T Nguyen, and Nguyen Duy Tân, *On the gcd-graphs over polynomial rings*, *Canadian Journal of Mathematics* (2024), 1–28.
24. Trygve Nagell, *Sur un type particulier d'unités algébriques*, *Arkiv för Matematik* **8** (1970), no. 2, 163–184.
25. Tung T. Nguyen and Nguyen Duy Tân, *On certain properties of the p-unitary Cayley graph over a finite ring*, arXiv preprint arXiv:2403.05635 (2024).
26. ———, *Integral Cayley graphs over a finite symmetric algebra*, *Archiv der Mathematik* **124** (2025), 615–623.
27. ———, *On U-unitary Cayley graphs over finite rings*, preprint (2025).
28. ———, *Perfect state transfer on gcd-graphs over a finite Frobenius ring*, arXiv preprint arXiv:2504.00404 (2025).

29. ———, *Supercharacters of finite abelian groups and applications to spectra of u -unitary Caley graphs*, arXiv preprint arXiv:2508.10348 (2025).
30. ———, *On gcd-graphs over finite commutative rings*, *Journal of Algebra and Its Applications* (2026).
31. D.S. Passman, *Infinite group rings*, *Lecture notes in pure and applied mathematics*, M. Dekker, 1971.
32. Ricardo A. Podestá and Denis E. Videla, *The Waring's problem over finite fields through generalized Paley graphs*, *Discrete Mathematics* **344** (2021), no. 5, 112324.
33. ———, *Connected components and non-bipartiteness of generalized Paley graphs*, *Annals of Combinatorics* (2025), 1–25.
34. R. Raphael, *Rings which are generated by their units*, *J. Algebra* **28** (1974), 199–205.
35. Nitin Saxena, Simone Severini, and Igor E Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, *International Journal of Quantum Information* **5** (2007), no. 03, 417–430.
36. Mohammad Hadi Shekarriz, MH Shirdareh Haghighi, and Habib Sharif, *On the total graph of a finite commutative ring*, *Communications in algebra* **40** (2012), no. 8, 2798–2807.
37. L. A. Skornyakov, *Complemented modular lattices and regular rings*, Oliver & Boyd, Edinburgh–London, 1964.
38. Wasin So, *Integral circulant graphs*, *Discrete Mathematics* **306** (2006), no. 1, 153–158.
39. Huadong Su and Gaohua Tang, *When unit graphs are isomorphic to unitary Cayley graphs of rings?*, *J. Algebra Appl.* **24** (2025), no. 11, Paper No. 2550267, 9. MR 4909024
40. Borworn Suntornpoch and Yotsanan Meemark, *Caley graphs over a finite chain ring and gcd-graphs*, *Bulletin of the Australian Mathematical Society* **93** (2016), no. 3, 353–363.
41. Issaraporn Thongsomnuk and Yotsanan Meemark, *Perfect state transfer in unitary Cayley graphs and gcd-graphs*, *Linear Multilinear Algebra* **67** (2019), no. 1, 39–50. MR 3885879
42. Daniel Zelinsky, *Every linear transformation is a sum of nonsingular ones*, *Proceedings of the American Mathematical Society* **5** (1954), no. 4, 627–630.

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
Email address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, ELMHURST UNIVERSITY, ELMHURST, ILLINOIS, USA
Email address: tung.nguyen@elmhurst.edu

FACULTY OF MATHEMATICS AND INFORMATICS, HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY, 1 DAI CO VIET ROAD, HANOI, VIETNAM
Email address: tan.nguyenduy@hust.edu.vn