PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 92(106) (2012), 35–41 DOI: 10.2298/PIM1206035L

DIGRAPHS ASSOCIATED WITH FINITE RINGS

Aleksandar T. Lipkovski

Communicated by Žarko Mijajlović

Abstract. Let A be a finite commutative ring with unity (ring for short). Define a mapping $\varphi : A^2 \to A^2$ by $(a,b) \mapsto (a+b, ab)$. One can interpret this mapping as a finite directed graph (digraph) $G = G(A)$ with vertices A^2 and arrows defined by φ. The main idea is to connect ring properties of A to graph properties of G. Particularly interesting are rings $A = \mathbb{Z}/n\mathbb{Z}$. Their graphs should reflect number-theoretic properties of integers. The first few graphs $G_n = G(\mathbb{Z}/n\mathbb{Z})$ are drawn and their numerical parameters calculated. From this list, some interesting properties concerning degrees of vertices and presence of loops are noticed and proved.

1. Introduction

Finite rings have been studied for a long time (e.g., [**1**, **2**]). Also, there have been some connections made between rings and graphs, more specifically, the graph of zero-divisors [**3**–**5**] and the unitary Cayley graph [**6**] of a ring. In the present paper, however, a completely different connection between finite rings and graphs is proposed and studied. This also has possible connections to elementary number theory. For basic algebraic and number-theoretic notions used here, see [**7**, **8**].

Let A be a finite commutative ring with unity (ring for short). Define a mapping $\varphi : A^2 \to A^2$ by $(a,b) \mapsto (a+b, ab)$. Intuitively, it reflects the ring structure of A. One can interpret this mapping as a finite directed graph (digraph) $G = G(A)$ with vertices A^2 and arrows defined by φ. The main idea is to deduce, if possible, ring properties of A from graph properties of G (e.g., the number of components, the lengths of longest paths and longest loops, the maximal degree of vertices, etc.).

Since A is finite, it has integer characteristic $\operatorname{char} A \in \mathbb{N}$. If n is not a prime, then A has zero-divisors and $A[X]$ is not a unique factorization ring (if $ab = 0$, $a \neq 0$, $b \neq 0$, then $(X-a)(X-b) = X[X-(a+b)]$ are two distinct, nonassociated factorizations of $X^2 - (a+b)X$). If $n = p$ is prime, then A nevertheless could have

2010 *Mathematics Subject Classification:* Primary 11T99, Secondary 05C90.
Key words and phrases: finite rings; finite graphs; symmetric polynomials.
Supported by Ministry of Science and Education of Serbia, project OI-174020.

zero-divisors (e.g., $\mathbb{Z}_2 \times \mathbb{Z}_2$). However, if A is a (finite) domain, then it must be a field, and in such case, $A = GF(p^k)$ and $A[X]$ is a UFD.

Particularly interesting are the rings $A = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Their graphs should reflect some number-theoretic properties of the integers. From the above remark, we see that either n is prime, $\mathbb{Z}_n$ is a field and $\mathbb{Z}_n[X]$ is a UFD, or n is not prime, $\mathbb{Z}_n$ has zero-divisors and $\mathbb{Z}_n[X]$ does not have the UF property. The first few graphs $G_n = G(\mathbb{Z}_n)$ can be explicitly drawn (see Fig. 1 and Fig. 2). Already from this list, some interesting properties can be noticed, concerning the degrees of vertices and the presence of loops.

2. Degrees of vertices

Consider the degrees of vertices in G. As usual, the outgoing (incoming) degree of the vertex (a, b) is by definition the number of arrows beginning (ending) in this vertex. Since G is a graph of a function, the outgoing degree of each vertex (a, b) equals one. What is the incoming degree of the vertex (a, b)?

Proposition 2.1. *The incoming degree of the vertex* $(a, b) \in G$ *equals the number of distinct roots of the quadratic polynomial* $X^2 - aX + b \in A[X]$.

Proof. If there is an arrow $(x, y) \longrightarrow (a, b)$, then $x + y = a$, $xy = b$, and by substitution we deduce that both x and y are roots of this polynomial. Conversely, if x is a root of this polynomial, then there is an arrow $(x, a - x) \longrightarrow (a, b)$, and for distinct roots such arrows are also distinct. In fact, if $x_1, \dots, x_k$ are all the distinct roots of the polynomial, then there is a permutation $\sigma \in S_k$ such that $a - x_i = x_{\sigma(i)}$. $\square$

In the case of G_p for prime p, the incoming degree of a vertex (a, b) can be either 0 (if $X^2 - aX + b$ is irreducible, i.e., $0 \neq 4b - a^2 \in \mathbb{Z}_p$ is a quadratic nonresidue modulo p), or 1 (if $4b - a^2 = 0$), or 2 (if $4b - a^2 \neq 0$ is a quadratic residue modulo p).

In the case of G_n for nonprime n, the incoming degree of a vertex (a, b) can be greater than 2, which depends on the different factorizations of $X^2 - aX + b$.

3. Components and closed loops

Consider closed paths, or loops, in G. Up to cyclic permutations, the loops are described by the corresponding arrow sequences.

Definition. The sequence

$$(a_1, b_1) \longrightarrow (a_2, b_2) \longrightarrow \cdots \longrightarrow (a_k, b_k) \tag{3.1}$$

of arrows in G defines a loop of length k (or a k-loop) if $(a_k + b_k, a_k b_k) = (a_1, b_1)$ and $(a_i + b_i, a_i b_i) \neq (a_j, b_j)$ for all $j \leqslant i < k$.

We see from Fig. 1 that there may exist loops of length 1 as well as longer loops. Also, some graphs G_n do contain G_1 as a (weakly) connected component and some do not. The definition also implies that if $k > 1$, then every $b_i \neq 0$.

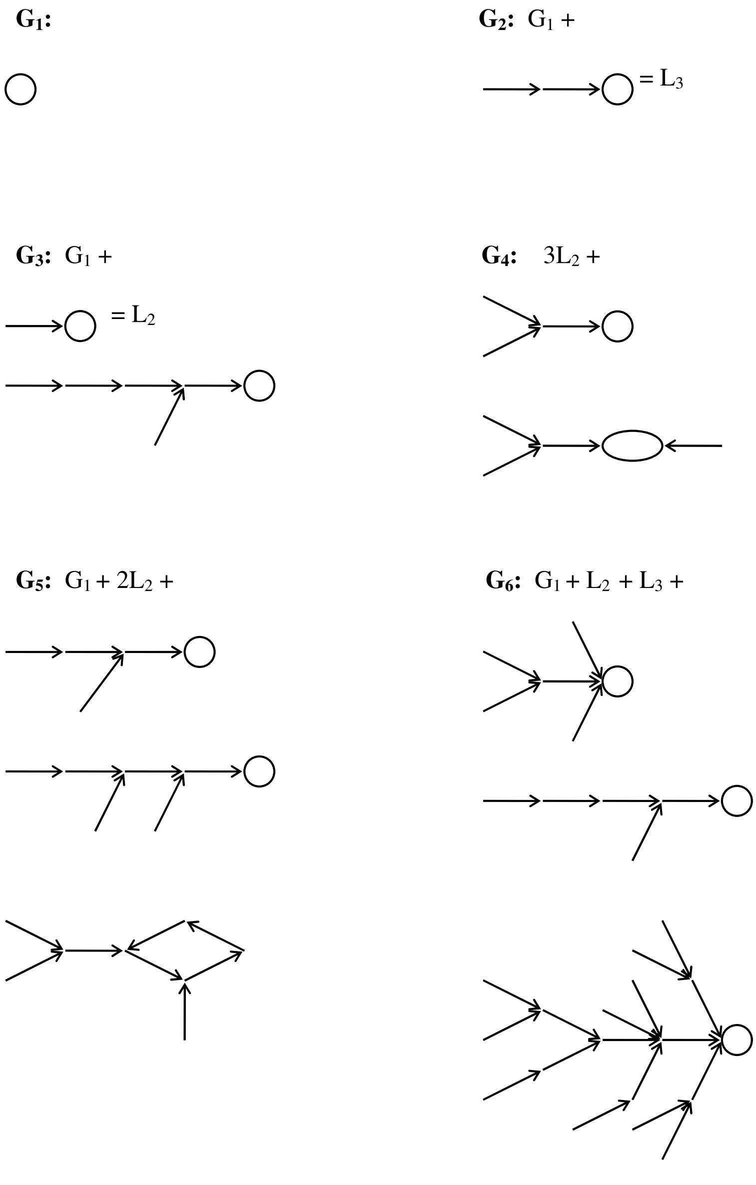

FIGURE 1

PROPOSITION 3.1. 1) *There are exactly* $n = \# A$ *loops of length* 1 *in* G*, and they correspond to the vertices* $(a, 0)$.

2) *Each connected component of* G *contains exactly one loop, and the number of connected components is* $n + \#\{$*loops of length* $> 1\}$.

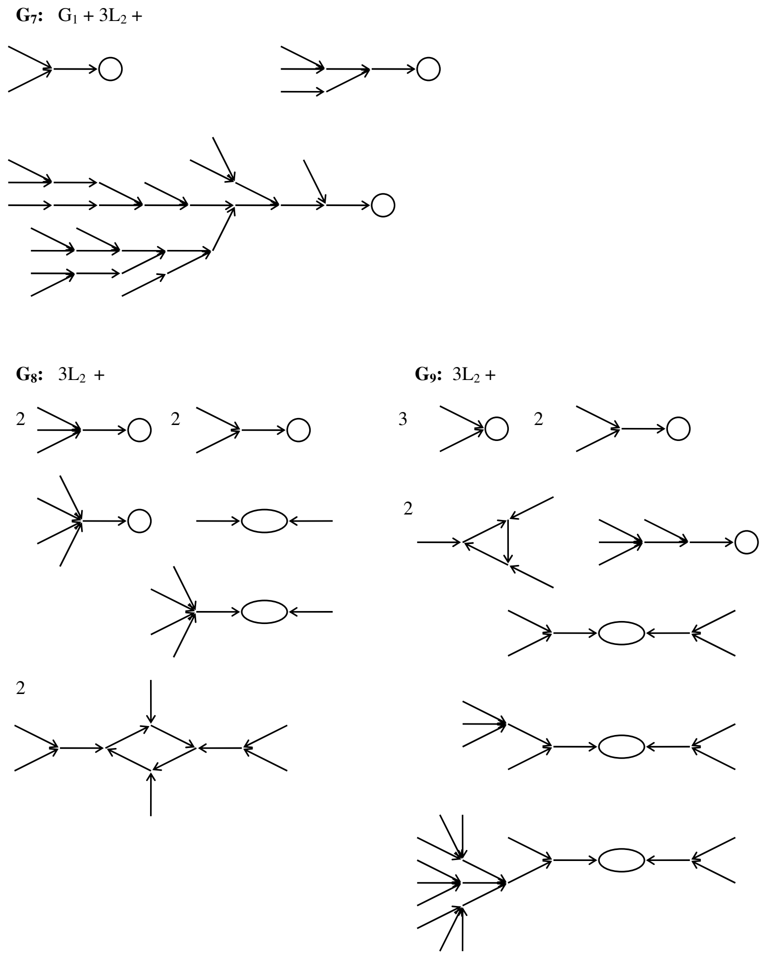

FIGURE 2

3) *The graph G_1 is a (weakly) connected component of G if and only if A has no nontrivial nilpotent elements.*

PROOF. First note that if $(a,b) \to (a,b)$ is a 1-loop, then $b = 0$ (and conversely). Therefore 1) follows. Since each component must end with a loop, 2) follows. Now if $a \neq 0$, then the incoming degree of the vertex $(a,0)$ is at least 2, since $(0,a) \longrightarrow (a,0) \longleftarrow (a,0)$. Therefore, the only vertex which could be in the component G_1 is $(0,0)$. But if $(x,y) \longrightarrow (0,0)$, then $x^2 = 0$, and if $x \neq 0$, then x is a nontrivial nilpotent element. □

What is the meaning of loops longer than 1? A closer look leads to necessary conditions which generalize the condition for 1-loops.

Proposition 3.2. *If the sequence* (3.1) *is a k-loop, then*

$$\sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0, \quad (\sigma_k(a) - 1)\,\sigma_k(b) = 0$$

where $\sigma_m(X) = \sigma_m(X_1, \dots, X_k)$ are the usual elementary symmetric polynomials in k variables.

Proof. There is an arrow $(a_{i-1}, b_{i-1}) \longrightarrow (a_i, b_i)$ if and only if one has the equality $X^2 - a_i X + b_i = (X - a_{i-1})(X - b_{i-1})$ in the polynomial ring $A[X]$. Therefore, the loop condition implies the equality

$$\prod_{i=1}^{k}(X^2 - a_i X + b_i) = \prod_{i=1}^{k}(X - a_i)(X - b_i)$$

in the polynomial ring $A[X]$. After a straightforward multiplication, one obtains

$$\begin{aligned} X^{2k} - \sigma_1(a)X^{2k-1} + \big[\sigma_2(a) + \sigma_1(b)\big]X^{2k-2} - \big[\sigma_3(a) + \textstyle\sum_{i\neq j} a_i b_j\big]X^{2k-3} + \dots + \sigma_k(b) \\ = X^{2k} - \big[\sigma_1(a) + \sigma_1(b)\big]X^{2k-1} + \big[\sigma_2(a) + \sigma_1(a)\,\sigma_1(b) + \sigma_2(b)\big]X^{2k-2} \\ - \big[\sigma_3(a) + \sigma_2(a)\,\sigma_1(b) + \sigma_1(a)\,\sigma_2(b) + \sigma_3(b)\big]X^{2k-3} + \dots + \sigma_k(a)\,\sigma_k(b) \end{aligned}$$

where $\sigma_m(x) = \sigma_m(x_1, \dots, x_k) = \sum_{1\leqslant j_1 < \dots < j_m \leqslant k} x_{j_1} \cdots x_{j_m}$. Comparing coefficients, one first obtains $\sigma_1(b) = 0$, and then $\sigma_2(b) = 0$. Finally, observing that $\sum_{i\neq j} a_i b_j = \sigma_1(a)\,\sigma_1(b) - \sum_i a_i b_i = \sigma_1(a)\,\sigma_1(b) - \sigma_1(b)$ one has $\sigma_3(b) = 0$. Comparison of constant terms gives the last condition. □

For $k \leqslant 3$, nice characterizations of loops can be obtained.

Proposition 3.3. *For $k = 1$, the "sequence" (3.1) is a 1-loop $\Leftrightarrow \sigma_1(b) = 0$.*
For $k = 2$, the sequence (3.1) is a 2-loop $\Leftrightarrow \sigma_1(b) = \sigma_2(b) = 0$.
For $k = 3$, the sequence (3.1) is a 3-loop $\Leftrightarrow \sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$.

Proof. The case $k = 1$ was already discussed above: $b_1 = 0 \Leftrightarrow (a_1, b_1) \longrightarrow (a_1, b_1)$. For $k = 2$, we have $b_1 + b_2 = 0$ and $b_1 b_2 = 0$. It is also easy to check that these two conditions imply $(a_2, b_2) \longrightarrow (a_1, b_1)$. Finally, for $k = 3$, one needs to prove that conditions $\sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$ imply $(a_3, b_3) \longrightarrow (a_1, b_1)$. Suppose that in the sequence $(a_1, b_1) \longrightarrow (a_2, b_2) \longrightarrow (a_3, b_3)$ one has $b_1 + b_2 + b_3 = b_1 b_2 + b_1 b_3 + b_2 b_3 = b_1 b_2 b_3 = 0$. This implies that $(X - b_1)(X - b_2)(X - b_3) = X^3$. Now $a_3 + b_3 = a_2 + b_2 + b_3 = a_1 + \sigma_1(b) = a_1$. Using these two facts and comparing the coefficients of X^4 in the polynomial identity

$$(X^2 - a_1 X + a_3 b_3)(X^2 - a_2 X + b_2)(X^2 - a_3 X + b_3) = (X - a_1)(X - a_2)(X - a_3)X^3,$$

one obtains $\sigma_2(a) + a_3 b_3 + b_2 + b_3 = \sigma_2(a)$, and finally $a_3 b_3 = b_1$. □

Remark. 1) It is easy to see that there exists a 2-loop $\Leftrightarrow$ the ring A has nontrivial nilpotent elements. For, since $(a_2, b_2) \neq (a_1, b_1)$, we have $b_1 \neq 0$, $b_1^2 = 0$ and this is a nilpotent in A. Conversely, if c is a nilpotent, $c^{k-1} \neq 0$, $c^k = 0$ for $k > 1$, take $b = c^{k-1}$. Then $b^2 = 0$ and there is a 2-loop $(-1, b) \longrightarrow (b - 1, -b) \longrightarrow (-1, b)$. Therefore, the existence of nilpotents in A is visible in the graph G in two different, equivalent ways: the absence of a G_1-component and the presence of 2-loops.

2) In the case $A = \mathbb{Z}_n$, this is equivalent to the condition that n is not square-free, since $\mathbb{Z}_n$ has no nontrivial nilpotents if and only if n is square-free. This leads to an (inefficient) algorithm for deciding whether a given integer n is square-free: look for 2-loops in the corresponding graph G_n.

3) The existence of a 3-loop implies that the ring A has zero-divisors, since in such case $b_1 b_2 b_3 = 0$ and all $b_i \neq 0$.

4) Proposition 5 suggests a tempting conjecture: if the sequence (3.1) is a k-loop, then $\sigma_1(b) = \sigma_2(b) = \cdots = \sigma_k(b) = 0$. However, as the example $A = \mathbb{Z}_5$ shows (see Fig. 1), it is already false for $k = 4$: there is a 4-loop $(2,2) \longrightarrow (4,4) \longrightarrow (3,1) \longrightarrow (4,3)$ such that $\sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$ and $\sigma_4(b) \neq 0$. In this case, $\sigma_4(a) = 1$ in accordance with the proposition.

4. Computer calculations

A computer program has been written and run on a PC to calculate some properties of the graph G_n, such as the number c_n of components, the length p_n of the longest path (including the loop closing the path) and l_n of the longest loop. The values of c_n, p_n, and l_n for $n \leqslant 50$ are shown in the following table.

n	c_n	p_n	l_n	n	c_n	p_n	l_n	n	c_n	p_n	l_n
1	1	1	1	18	28	6	3	35	42	12	4
2	2	3	1	19	20	34	8	36	73	8	6
3	3	5	1	20	31	6	4	37	39	49	24
4	5	4	2	21	21	9	1	38	40	34	8
5	6	6	4	22	24	14	6	39	42	22	4
6	6	5	1	23	24	32	10	40	80	8	4
7	7	9	1	24	36	8	4	41	45	63	22
8	12	6	4	25	50	12	5	42	42	9	1
9	14	6	3	26	28	22	4	43	48	98	11
10	12	6	4	27	63	10	9	44	61	15	6
11	12	14	6	28	35	10	2	45	87	14	12
12	15	6	2	29	32	35	14	46	48	32	10
13	14	22	4	30	36	8	4	47	50	60	12
14	14	9	1	31	32	44	18	48	90	12	8
15	18	8	4	32	72	18	16	49	118	10	7
16	30	10	8	33	36	14	6	50	100	12	5
17	19	18	10	34	38	18	10				

From the table, it is evident that local peaks of p_n and l_n appear for (some, but not all) primes n and the peaks of l_n appear also for $n = 2^k$. Why? This and many other similar questions can be raised and answered.

We give here two very rough estimates for c_n and p_n. Consider $n = 2^k$ ($k \geqslant 3$). Suppose that $p, q \in \mathbb{Z}_n$ are not divisible by 2, and let $m \geqslant 2$. There exists an arrow $(2p, 2^m q) \longrightarrow (2p', 2^{m+1} q')$ where $p' = p + 2^{m-1} q$, $q' = pq$ are again not divisible by 2. This gives a path

$$(2, 2^2) \longrightarrow \cdots \longrightarrow (2p, 2^{k-1}q) \longrightarrow (2p', 0) \circlearrowleft$$

of length $k-1$. This means that in the case considered, $p_n \geqslant k-1$. Similar arguments can be used in the general case for any prime factor of n, which means that $p_n \geqslant k-1$ where k is the maximal multiplicity of any prime factor of n. However, as the table shows, this rough lower estimate is not very close to p_n.

The starting vertices (a, b) (with incoming degree 0) correspond to irreducible quadratic polynomials $X^2 - aX + b$ in $\mathbb{Z}_n[X]$. It can easily be seen that the number i of irreducible quadratic polynomials is $i \geqslant n^2 - \binom{n+1}{2} = \frac{n(n-1)}{2}$ ($\mathbb{Z}_n[X]$ has unique factorization exactly when n is prime, and then the equality holds), therefore the number of starting vertices is i. This gives a rough upper estimate for the number of components $c_n \leqslant i$. Again, as the table shows, this is not very close to c_n.

5. Graphs for $1 \leqslant n \leqslant 9$

Here are the first nine digraphs G_n. The components which appear several times in the same and/or different graphs are denoted by the same letter (these are G_1, L_2, L_3) and drawn only by their first appearance. The number to the left of the component is the number of times this component appears in the whole graph. The sign + denotes the (disjoint) union of components.

References

1. C. Fletcher, *Rings of small order*, Math. Gazette 64 (1980), 9-22
2. B. Fine, *Classification of finite rings of order* p^2, Math. Magazine 66 (1993), 248-252
3. D. F. Anderson, P. S. Livingston, *The zero-divisor graph of commutative ring*, J. Algebra 217 (1999), 434-447
4. D. F. Anderson, M. C. Axtell, J. A. Stickles Jr., *Zero-divisor graphs in commutative rings.* (In: *Commutative Algebra, Noetherian and Non-Noetherian Perspectives*, Fontana M., Kabbaj S.-E., Olberding B., Swanson I., eds., Springer New York, 2011, 23-45)
5. M. Axtell, J. Stickles, *Graphs and zero-divisors*, College Math. J. 41 (2010), 396-399
6. R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jimenez, R. Karpman, A. Kinzel, D. Pritikin, *On the unitary Cayley graph of a finite ring*, El. J. Combinatorics 216 (2009), #R117
7. T. Hungerford, *Algebra* (GTM v. 73), Springer, 1980
8. A. Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, 1985

Faculty of Mathematics
University of Belgrade
Belgrade, Serbia
acal@matf.bg.ac.rs

(Received 31 03 2011)
(Revised 10 04 2012)