involve
a journal of mathematics

Connectedness of digraphs from quadratic polynomials

Siji Chen and Sheng Chen

msp

2020 vol. 13, no. 2

INVOLVE 13:2 (2020)
dx.doi.org/10.2140/involve.2020.13.357

Connectedness of digraphs from quadratic polynomials

Siji Chen and Sheng Chen

(Communicated by Vadim Ponomarenko)

Suppose that $f(x)=x(x-k)$, where k is an odd positive integer. First, an infinite digraph $G_k=(V,E)$ is defined, where the vertex set is $V=\mathbb{Z}$ and the edge set is $E=\{(x,y)\mid x,y\in\mathbb{Z},\ f(x)=f(2y)\}$. Then the following results are proved: if $k=1$, then the digraph G_k is weakly connected; if p is a safe prime, i.e., both p and $q=(p-1)/2$ are primes, then the number w_p of weakly connected components of the digraph G_p is 2. Finally, a conjecture that there are infinitely many primes p such that $w_p=2$ is presented.

1. Introduction

Denote by $\mathrm{Int}(\mathbb{Z})=\{f(x)\in\mathbb{Q}[x]\mid f(\mathbb{Z})\subseteq\mathbb{Z}\}$ the ring of integer-valued polynomials on $\mathbb{Z}$. Chapman and Ponomarenko [2011] completely characterized the pairs of polynomials (f,g) in $\mathrm{Int}(\mathbb{Z})$ such that $f(\mathbb{Z})=g(\mathbb{Z})$. Motivated by this work, in this paper we study the digraph $G_k=(V,E)$ defined by

$$V=\mathbb{Z},\qquad E=\{(x,y)\mid x,y\in\mathbb{Z},\ f(x)=g(y)\},$$

where $f(x)=x(x-k)$ and $g(x)=f(2x)$. If k is odd, then by Lemma 1 in [Chapman and Ponomarenko 2011], it is easy to see that the digraph G_k is an infinite digraph in which each vertex has out-degree 1 and in-degree 2. In fact, on one hand, since $f(x)=f(k-x)$, for every vertex $x\in\mathbb{Z}$ we have (x,y) is the unique edge from x where

$$y=\begin{cases}x/2 & \text{if } x \text{ is even},\\ (k-x)/2 & \text{if } x \text{ is odd},\end{cases}$$

and on the other hand, for every vertex y, there are two edges $(2y,y)$ and $(k-2y,y)$ into y.

For general definitions about digraphs, we can refer to [Bang-Jensen and Gutin 2009]. Recall that a digraph is weakly connected if the underlying graph is connected.

MSC2010: primary 05C25; secondary 05C40, 05C20.
Keywords: connectivity, digraph, prime.

2. Results

Theorem 1. *If $k = 1$, then the digraph G_k is weakly connected.*

Proof. To prove the result, it suffices to prove the following statement by induction on positive integer n: every vertex $x \in \mathbb{Z}$ such that $|x/2| \le n$ is weakly connected to the vertex 0.

If $n = 1$, then $|x/2| \le n$ implies $x = -2,\ x = -1,\ x = 0,\ x = 1$, or $x = 2$. Since $(-2, -1),\ (-1, 1),\ (2, 1),\ (1, 0)$, and $(0, 0)$ are edges in G_1, the statement is true.

Suppose the statement is true for some $n \ge 1$, that is, every vertex $x \in \mathbb{Z}$ such that $|x/2| \le n$ is weakly connected to the vertex 0. Then for a vertex $x \in \mathbb{Z}$ such that $n < |x/2| \le n + 1$, we have $x = 2n{+}2,\ 2n{+}1, -2n{-}2$, or $-2n{-}1$. Note that the following are edges in G_1:

$$(2n+2, n+1), \quad (2n+1, -n), \quad (-2n-2, -n-1), \quad (-2n-1, n+1).$$

Since $|n/2| \le n$ and $|(n{+}1)/2| \le n$, we know that vertex x such that $n < |x/2| \le n{+}1$ is connected to some vertex y such that $|y/2| \le n$. Therefore it is weakly connected to the vertex 0. □

Theorem 2. *If p is a safe prime, that is, both p and $q = (p - 1)/2$ are primes, then the digraph G_p has precisely two weakly connected components.*

Proof. Suppose that $p = 2q + 1$ is a safe prime. We prove the result in four steps.

Step 1: Take

$$U_1 = \{x \in \mathbb{Z} \mid p \text{ divides } x\},$$
$$U_2 = \{x \in \mathbb{Z} \mid p \text{ does not divide } x\}.$$

We use G_{p,U_1} and G_{p,U_2} to denote the two subdigraphs induced by the vertex subsets U_1 and U_2 respectively. Since there is no edge (x, y) such that $x \in U_1$ and $y \in U_2$, or $x \in U_2$ and $y \in U_1$, we know G_p is a disjoint union of the subdigraphs G_{p,U_1} and G_{p,U_2}.

Step 2: There is an isomorphism of digraphs from G_{p,U_1} to G_1 defined by the mapping of vertex sets: $U_1 \to \mathbb{Z} : x \mapsto x/p$. By Theorem 1, we know that G_{p,U_1} is weakly connected.

Step 3: Take $W = \{1, 2, \dots, p - 1\}$. In this step, we aim to prove the following statement by induction on positive integers n:

Every vertex $x \in U_2$ with $|x/p| < n$ can be weakly connected to some vertex $y \in W$.

First, if $n = 1$, then the condition $x \in U_2$ with $|x/p| < 1$ is equivalent to $x \in \mathbb{Z}$ with $-p < x < 0$ or $0 < x < p$. If $x \in U_2$ is odd, then x is connected to $y = (p - x)/2 \in W$. Otherwise, $x \in U_2$ is even, say $x = 2^r s$, where r is a nonnegative integer and s is an odd integer. Then x is connected to s and thus connected to some vertex in W, and thus the statement is true for $n = 1$.

Next, suppose the statement is true for some positive integer n, that is, every $x \in U_2$ with $|x/p| < n$ is weakly connected to some vertex $y \in W$. For even $x \in U_2$ with $n < |x/p| < n+1$, the terminal vertex $y = x/2$ of the unique edge from x satisfies $|y/p| < (n+1)/2 \le n$. For odd $x \in U_2$ with $n < |x/p| < n+1$, both (x, z) and (z, y) are edges, where $z = (p - x)/2$, and one of the following holds: $y = (p - z)/2$ or $y = z/2$. So $y = (p \pm x)/4$, which satisfies $|y/p| < (1 + (n + 1))/4 < n$. Therefore $x \in U_2$ is always weakly connected to some vertex in W. Thus the statement is true for $n + 1$.

<u>Step 4</u>: Denote by $G_{p,W}$ the subdigraph induced by the vertex set

$$W = \{1, 2, \ldots, p - 1\} = \{1, 2, \ldots, 2q\}.$$

The edge set of $G_{p,W}$ is

$$\{(2y, y) \mid y = 1, 2, \ldots, q\} \cup \{(p - 2y, y) \mid y = 1, 2, \ldots, q\}.$$

For any $x \in W$, we have some $y \in \{1, 2, \ldots, q\}$ such that both (x, y) and $(p-x, y)$ are edges in $G_{p,W}$. So $x \in W$ is weakly connected to $p-x \in W$. For any $y \in \{1, 2, \ldots, q\}$, we have $(2y, y)$ is an edge in $G_{p,W}$ and thus y is weakly connected to $2y$. For any $y \in \{q + 1, q + 2, \ldots, q + q\}$, we know $(2p - 2y, p - y)$ is an edge in $G_{p,W}$ and thus $y,\ p - y,\ 2p - 2y,\ p - (2p - 2y) = 2y - p$ are weakly connected. That is to say, any $y \in W$ is weakly connected to $2y \in W$ or $2y - p \in W$.

Denote by $U(\mathbb{F}_p)$ the multiplicative group of the invertible elements of the finite field $\mathbb{F}_p = (\mathbb{Z}, +, \cdot)/p\mathbb{Z}$. Since p is a safe prime, the unit group $U(\mathbb{F}_p)$ is a cyclic group of order $p-1 = 2q$, which can be generated by the set $S = \{-1, 2\}$. Therefore the digraph $C(U(\mathbb{F}_p), S)$ with vertex set $U(\mathbb{F}_p)$ and edge set

$$\{(a, b) \mid a, b \in U(\mathbb{F}_p),\ a = -b \text{ or } a = 2b\}$$

is connected.

Using elementary number theory, it follows that $G_{p,W}$ is weakly connected. □

3. A conjecture

Safe primes appear in many places of mathematical theory and applications; see, e.g., [OEIS; von zur Gathen and Shparlinski 2013]. Although a folklore conjecture states that infinitely many Sophie Germain primes q exist, i.e., q and $p = 2q + 1$ are prime, a proof of this conjecture is not yet in sight; see [von zur Gathen and Shparlinski 2013]. Since we do not know whether the conjecture that there are infinitely many safe primes is true or not, we present the following slightly weaker *conjecture*:

Conjecture. There are infinitely many primes p such that the digraph G_p has exactly two weakly connected components.

Remark. For primes $p = 13$, $p = 17$, $p = 31$, which are not safe primes, the number of weakly connected components of G_p are 2, 3, 4 respectively. We may use the result in [Chen and Chen 2015] to study the number of weakly connected components of G_k for general nonprime odd integers k. However, an explicit formula for w_k seems out of reach.

Acknowledgement

The authors would like to thank the editor and referee for valuable comments and suggestions which greatly improve the presentation the paper.

References

[Bang-Jensen and Gutin 2009] J. Bang-Jensen and G. Gutin, *Digraphs: theory, algorithms and applications*, 2nd ed., Springer, 2009. MR Zbl

[Chapman and Ponomarenko 2011] S. T. Chapman and V. Ponomarenko, "On image sets of integer-valued polynomials", *J. Algebra* **348** (2011), 350–353. MR Zbl

[Chen and Chen 2015] S. Chen and X. Chen, "Weak connectedness of tensor product of digraphs", *Discrete Appl. Math.* **185** (2015), 52–58. MR Zbl

[von zur Gathen and Shparlinski 2013] J. von zur Gathen and I. E. Shparlinski, "Generating safe primes", *J. Math. Cryptol.* **7**:4 (2013), 333–365. MR Zbl

[OEIS] N. Sloane, "Safe primes p: $(p-1)/2$ is also prime", entry A005385 in *The online encyclopedia of integer sequences*.

Received: 2020-02-02 Revised: 2020-03-10 Accepted: 2020-03-14

1756474535@qq.com *RDFZ Xishan AP Center, RDFZ Xishan School, Beijing, China*

schen@hit.edu.cn *Department of Mathematics, Harbin Institute of Technology, Harbin, China*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US $205/year for the electronic version, and $275/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2020 vol. 13 no. 2

1944-4176(2020)13:2;1-S