AKCE Int. J. Graphs Comb., 11, No. 2 (2014), pp. 133-148

Additive Operations on Flow Graphs

Bilal Khan
Department of Mathematics and Computer Science
John Jay College (CUNY)
New York, USA.
e-mail: *bkhan@jjay.cuny.edu*
and
Kiran R. Bhutani
Department of Mathematics
The Catholic University of America
Washington DC, USA.
e-mail: *bhutani@cua.edu*

Communicated by: S. Arumugam
Received 17 January 2013; revised 22 November 2013; accepted 18 March 2014

Abstract

This paper extends the theory of *graphic arithmetic*, an extension of classical arithmetic on $\mathbb{N}$ to a larger model $\mathcal{F}$ defined on the set of all flow graphs—finite directed connected multigraphs having a pair of distinguished vertices. We give a graph-theoretic characterization for a flow graph to be reducible into a proper sum, and use this to develop a canonical decomposition of flow graphs into irreducible summands. Such decompositions enable us to characterize commutativity conditions for addition, which in turn, reveal the structure of additive centralizers in $\mathcal{F}$.

Keywords: multi-graphs, flow graphs, canonical decomposition, graph arithmetic.

2010 Mathematics Subject Classification: 05C99.

1. Introduction

There have been previous attempts to define algebraic structures on the set of all graphs, notably via ordinals and partially ordered sets [3, 4, 11, 13, 8], the classical operations on graphs [15], including graph products [6]. In considering binary operations on graphs, considerable prior work has addressed the Cartesian product [12], Kronecker products [14], tensor products [1], zig-zag and sandwich products [10], and the rooted product [5], and others. For each of these, there is, of course, a corresponding nascient algebraic theory. With respect to Cartesian products, for example, Li considers the problem of enumerating prime graphs [9], while Kaveh and Laknejadi recently addressed issues surrounding factorization [7], In our own prior work [2], we generalized arithmetic (classically defined over

the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$), to the set F consisting of all *flow graphs*, providing within the larger model an interpretation of the *language of arithmetic* $\mathcal{L}$ which consists of two constants 0 and 1, one binary relation $\leqslant$, and two binary operations $+$ and $\times$. We give a brief synopsis of these prior results on *graphic arithmetic* below.

Following [2], a *flow graph* $A = (G, s_A, t_A)$ is a finite directed connected multigraph $G = (V[A], E[A])$ together with vertices $s_A, t_A \in V[A]$ which are designated as the *source* and *target* of A. The standard model $\mathcal{N} = \langle \mathbb{N}, 0, 1, \leqslant, +, \times \rangle$ embeds into a model on the set of flow graphs $\mathcal{F} = \langle F, \mathring{0}, \mathring{1}, \lhd, \oplus, \otimes \rangle$ via an embedding $i : \mathcal{N} \hookrightarrow \mathcal{F}$ which maps each natural number n to flow the graph $F_n = (P_n, s_n, t_n)$ in which P_n is the directed chain of on $n+1$ vertices and s_n (resp. t_n) is the unique vertex with in-degree (resp. out-degree) 0. The addition of A with another flow graph $B = (H, s_B, t_B)$ is carried out by taking $A \oplus B$ to be the graph obtained upon identifying t_A with s_B and taking s_A and t_B as the source and target vertices in $A \oplus B$, respectively. Scalar left multiplication of flow graphs by positive integers is interpreted by taking kA as shorthand for the flow graph obtained when A is added to itself k times. Addition (illustrated in Figure 1) is an associative operation in $\mathcal{F}$, though not generally commutative. We take $i(1) = F_1 = \mathring{1}$ and $i(0) = F_0 = \mathring{0}$, referring to the latter as the *trivial* flow graph. Inside $\mathcal{F}$, the flow graphs $\mathring{0}$ serves as the unique additive identity. We say that a non-trivial flow graph is *infinitesimal* if its source and target vertices coincide. The sum of two flow graphs is infinitesimal if and only if both summands are infinitesimal. We say $A \lhd B$ if flow graph B can be transformed into A by a series of edge contractions. Results relating the theorems of classical arithmetic (including the interplay of addition and multiplication) to the theory of $\mathcal{F}$ are found in [2].

Certainly the theory of natural numbers has had a profound historical impact in the development of computability theory, which, in turn, has yielded many practical applications in cryptography. Given that the natural numbers $\mathcal{N}$ are a submodel of $\mathcal{F}$, it is our hope that in advancing a deeper understanding of the larger ambient structure we will obtain theorems that provide new insights and richer perspectives on the results of classical number theory. Towards such objectives, in this paper, we further develop the theory of the additive semigroup in $\mathcal{F}$, obtaining a description of the structure of the (additive) centralizers of an arbitrary flow graph. Specifically, we show here that if two flow graphs A and B commute with respect to $\oplus$ then they must both necessarily be scalar multiples of some flow graph C. Along the way, we present a graph-theoretic criterion for a flow graph to be irreducible as a proper sum of (non-trivial) flow graphs, and use this as the foundation for defining the canonical decomposition of a flow graph in terms of irreducible summands. Such decompositions also enable us to formally demonstrate (additive) cancellation laws for $\mathcal{F}$.

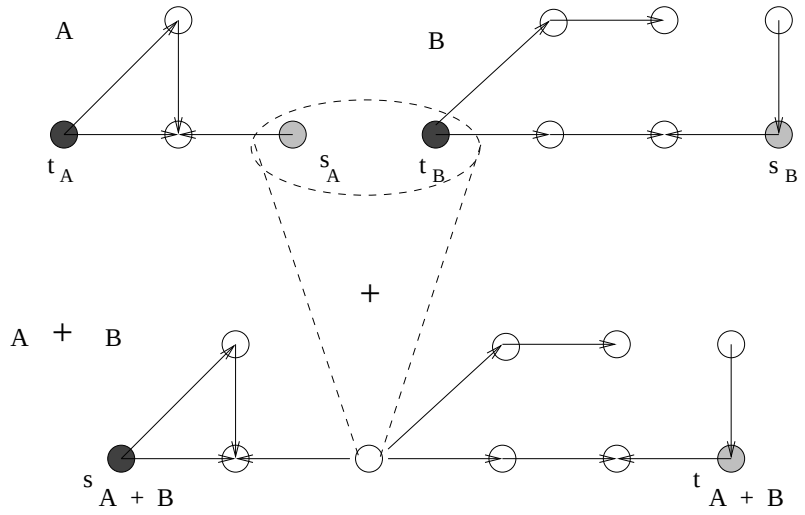

Figure 1: Flow graph addition.

2. Results

A flow graph A is called $\oplus$-*reducible* if there exist non-trivial flow graphs B, C, for which $A = B \oplus C$. Otherwise, A is called $\oplus$-*irreducible*. Towards a graph-theoretic characterization of $\oplus$-irreducibility, we introduce the operation of $*$-*deletion* on graphs.

Definition 2.1 ($*$-deletion)**.** *Let $G = (V, E)$ be directed connected multigraph, and fix a vertex $w \in V$. Let $G \backslash_* w = \{G_1^*, \ldots, G_{k(w)}^*\}$ be defined as the outcome of the following 7 step process:*

1. *For each edge $e = (w, u)$ where $u \neq w$, add a vertex v_e, and replace e by edges (w, v_e), (v_e, u).*
2. *For each edge $e = (u, w)$ where $u \neq w$, add a vertex v_e, and replace e by edges (u, v_e), (v_e, w).*
3. *For each edge $e = (w, w)$, add a vertex v_e, and replace e by edges (w, v_e), (v_e, v_e).*
4. *Delete w and all incident edges, denote resulting components as $G_1, \ldots, G_{k(w)}$.*
5. *Let P be the vertices added in (1-3) and define relation $(v_1, v_2) \in R$ iff v_1, v_2 are in the same component G_i.*
6. *Identify the vertices in P that are related by R and denote the resulting components as $G_1^*, \ldots, G_{k(w)}^*$.*
7. *Index the elements of P/R_w as $\{w_1, w_2, \ldots, w_{k(w)}\}$ so that w_i lies in G_i^* for $i = 1, \ldots, k(w)$.*

The first four steps depicted in Figure 3 (pp. 137) and Figure 2 (pp. 136) illustrate the process of $*$-deletion.

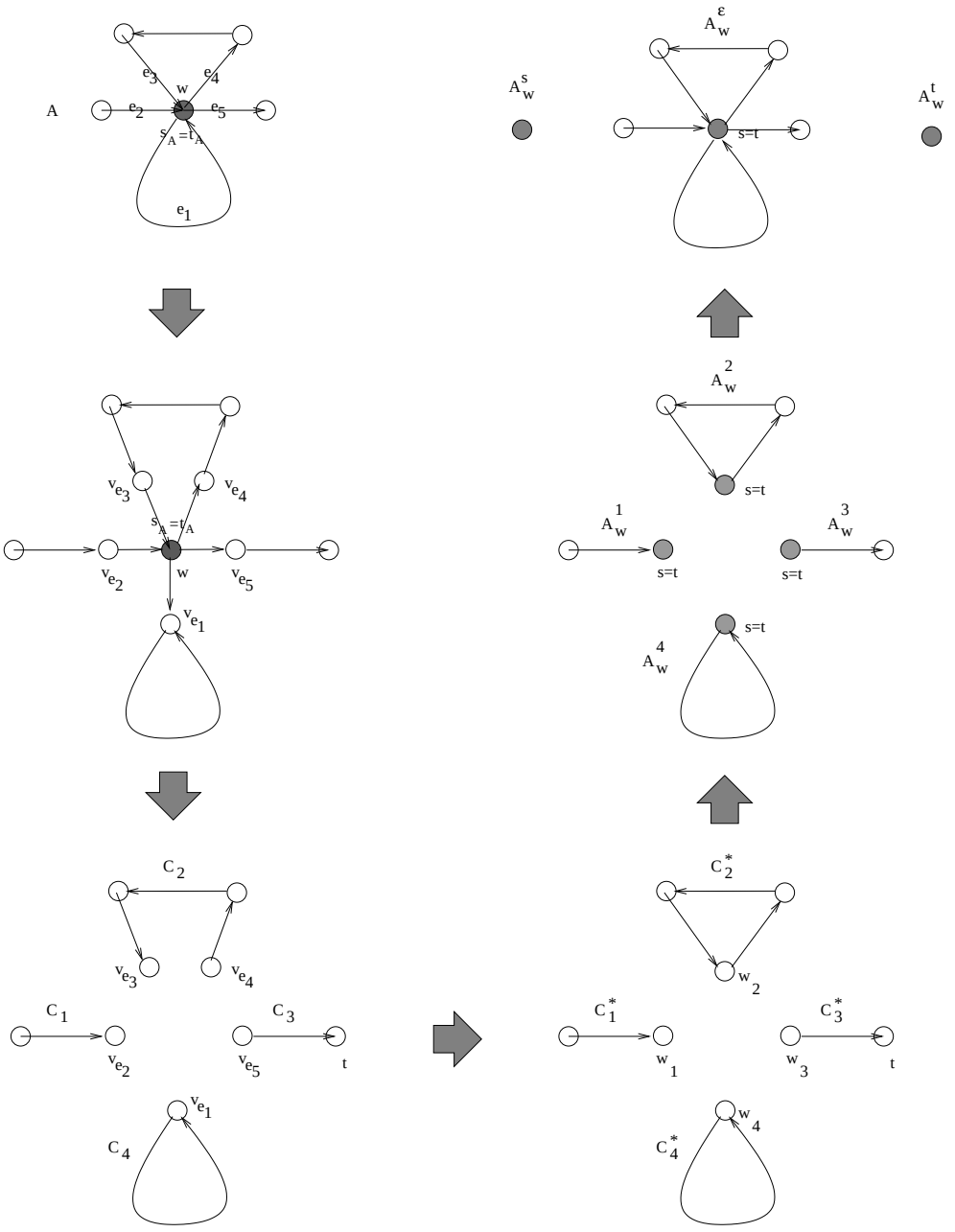

Figure 2: The w-splitting of an infinitesimal flow graph A, yielding a trivial splitting.

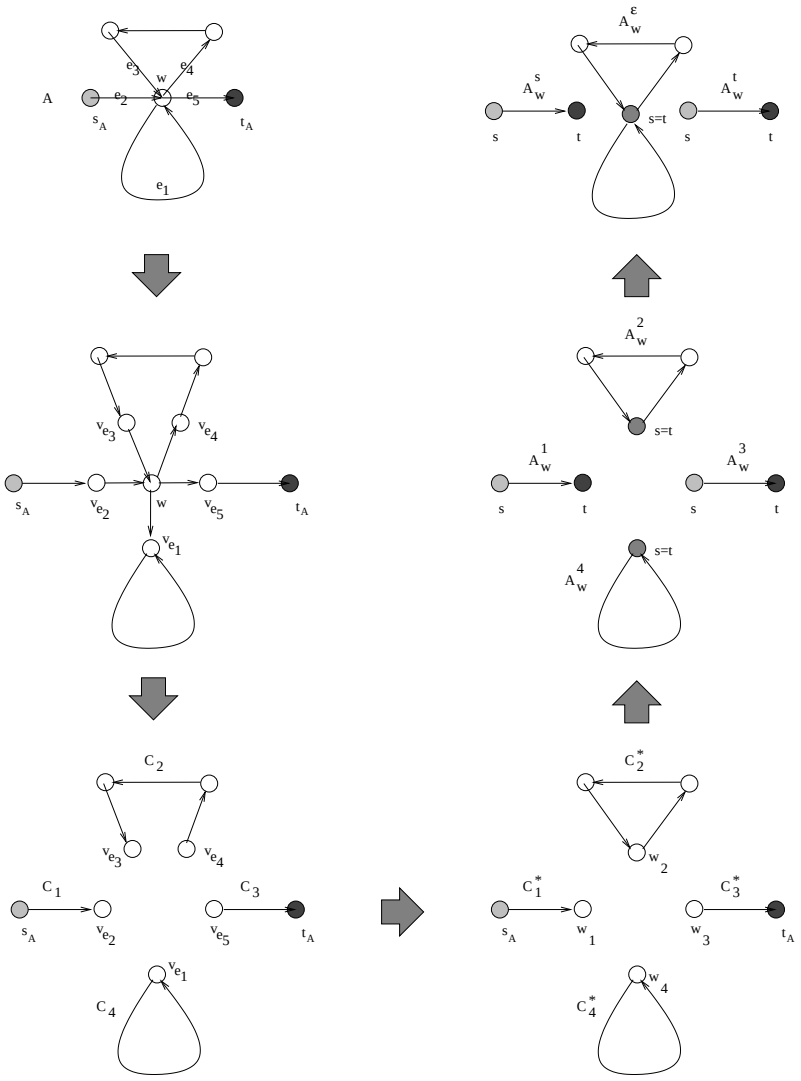

Figure 3: The w-splitting of a non-infinitesimal flow graph A resulting in a non-trivial splitting.

Definition 2.2 (Splitting vertex)**.** *Given a flow graph $A = (G, s_A, t_A)$, with $G = (V[A], E[A])$ and $w \in V[A]$, let $G\backslash_* w = (G^*_1, \ldots, G^*_{k(w)})$ be the $*$-deletion of w from G. We say that w is a* splitting vertex *of A if either:*

1. *$s_A \neq w \neq t_A$, and s_A and t_A lie in distinct members of $G\backslash_* w$; or*
2. *$w = s_A$ or $w = t_A$ (or both), and $k(w) \geqslant 2$.*

Let $\chi(A) \subset V[G]$ be the set of all splitting vertices of A.

Remark 2.3. *If A is an infinitesimal flow graph, then $s_A = t_A$, so if w is a splitting vertex of A then it must satisfy condition (2) of Definition 2.2. Thus, necessarily $w = s_A = t_A$ and $G\backslash_* w$ contains at least two components.*

Remark 2.4. *If w is a splitting vertex of a flow graph $A = (G, s_A, t_A)$ then w is a cut vertex in the graph G. The converse is false, as seen in the flow graph B in Figure 1 (pp. 135) which contains two cut vertices at distance 1 from t_A, of which only one is a splitting vertex.*

Definition 2.5 (w-Splitting of a flow graph)**.** *Let $A = (G, s_A, t_A)$ be a flow graph and w a splitting vertex of A.*
Let $G\backslash_* w = (G_1^*, \ldots, G_{k(w)}^*)$ be the $*$-deletion of w from G. Define flow graphs

$$A_w^i = \begin{cases} (G_i^*, s_A, w_i) & \text{if } s_A \in V[G_i^*] \\ (G_i^*, w_i, t_A) & \text{if } t_A \in V[G_i^*] \\ (G_i^*, w_i, w_i) & \text{otherwise.} \end{cases} \qquad i = 1, \ldots k(w)$$

*Let $\epsilon_w = \{i \mid s_A, t_A \notin V[G_i^*]\}$; we define the w-*splitting *of A, denoted $A\backslash_* w = (A_w^s, A_w^\epsilon, A_w^t)$, by taking*

$$A_w^s = \begin{cases} A_w^i & \text{if } s_A \in V[G_i^*] \\ \mathring{0} & \text{if } w = s_A \end{cases}$$

$$A_w^t = \begin{cases} A_w^i & \text{if } t_A \in V[G_i^*] \\ \mathring{0} & \text{if } w = t_A \end{cases}$$

$$A_w^\epsilon = \bigoplus_{1 \in \epsilon_w} A_w^i$$

Note that $A = A_w^s \oplus A_w^\epsilon \oplus A_w^t$. Figure 3 (pp. 137) provides an example of a w-splitting.

Remark 2.6. *In Definition 2.5, each A_w^i ($i = 1, \ldots, k(w)$) is non-trivial, since in steps $1 - 4$ of the construction of $G\backslash_* w$ (see Definition 2.1) no component G_i can have fewer than 1 edge, and G_i^* is obtained by identifying vertices in G_i.*

Remark 2.7. *In Definition 2.5, each A_w^i ($i \in \epsilon_w$) is infinitesimal and contains no splitting vertex. To see the latter assertion, suppose, towards contradiction, that some A_w^i contains a splitting vertex w. Then $w = s_{A_w^i} = t_{A_w^i}$ by Remark 2.3. But w_i (in G_i^*) is the identification of a set of vertices in the connected graph G_i (see step 6 of Definition 2.1). Hence, w_i is not a cut vertex in G_i^*, and so by Remark 2.4 cannot be a splitting vertex of A.*

If w is a splitting vertex of A then was deleted in the construction of $G\backslash_* w$ (see step 4 of Definition 2.1), so $w \notin V[A_u^s]$ and $w \notin V[A_u^t]$. There are natural injections of the vertices of A_w^s, A_w^t and A_w^ϵ into the vertices of A. The splitting vertices of A_w^s and A_w^t are also splitting vertices of A. The splitting vertices of A which lie in A_w^s (resp. A_w^t) are

splitting vertices of A^s_w (resp. A^t_w). Since A^ϵ_w is infinitesimal, its has at most one splitting vertex, that being its source/target. The implications of these facts are collected in the next observation.

Observation 2.8. *For any flow graph $A = (G, s_A, t_A)$*

a. For all $u \in \chi(A)$, $u \notin \chi(A^s_u)$ and $u \notin \chi(A^t_u)$.

b. $\chi(A) \cap A^s_u = \chi(A^s_u)$ and $\chi(A) \cap A^t_u = \chi(A^t_u)$.

c. For all $w \in \chi(A)$, if $u \in \chi(A^s_w)$ and $v \in \chi(A^s_u)$, then $v \in \chi(A^s_w)$.

d. For all $w \in \chi(A)$, if $u \in \chi(A^t_w)$ and $v \in \chi(A^t_u)$, then $v \in \chi(A^t_w)$

e. Let u, v be distinct vertices in $\chi(A)$ then $u \notin A^\epsilon_v$ and $v \notin A^\epsilon_u$.

Lemma 2.9. *Let A be a flow graph with splitting vertex w. Then*

(i) A^ϵ_w is infinitesimal.

(ii) A^s_w and A^t_w are each either trivial, or non-infinitesimal.

(iii) No two adjacent elements in the triple $(A^s_w, A^\epsilon_w, A^t_w)$ are trivial flow graphs.

Proof. (i) By Definition 2.5, if $\epsilon = \emptyset$ then $A^\epsilon_w = \mathring{0}$; otherwise, A^ϵ_w is the sum of flow graphs which are each (by Remark 2.7) infinitesimal, and since the sum of infinitesimals is infinitesimal, the result follows.

(ii) If A^s_w is non-trivial, then $A^s_w = A^i_w$ for some i in $\{1, \ldots, k(w)\}$, with $s_A \in V[G^*_i]$. Since $s_A \neq w_i$ in $V[G^*_i]$, by Definition 2.5 we know A^s_w is not infinitesimal. The proof for A^t_w is analogous.

(iii) If w satisfies condition (1) of Definition 2.2, then s_A and t_A lie in distinct components of $G\backslash_* w$, but then by Remark 2.6, A^s_w and A^t_w are both non-trivial. On the other hand, if w satisfies condition (2) of Definition 2.2, then either $w = s_A$, or $w = t_A$, or both—hence either $A^t_w = \mathring{0}$, or $A^s_w = \mathring{0}$, or both—and since $G\backslash_* w$ contains at least two non-trivial components, Definition 2.5 implies $|\epsilon_w| \geqslant 1$, and hence $A^\epsilon_w \neq \mathring{0}$. □

The next Proposition provides a graph-theoretic characterization of $\oplus$-reducibility.

Proposition 2.10 ($\oplus$-Irreducibility Lemma)**.** *A flow graph $A = (G, s_A, t_A)$ is $\oplus$-reducible if A has a splitting vertex.*

Proof. ($\Rightarrow$) Suppose $A = B \oplus C$. Take $w = t_B = s_C$ to be the vertex in $V[A]$ which is the identification of t_B with s_C. If B is not infinitesimal, $t_B \neq s_B$; but $s_A = s_B$, so $w \neq s_A$; thus even after w is deleted s_A will be found in some component A^i_w, so $A^s_w \neq \mathring{0}$. By a similar argument, if C is not infinitesimal $t_A = t_C$ is in some component A^j_w, and $A^t_w \neq \mathring{0}$. If B is infinitesimal, then $t_B = s_B$; but $s_B = s_A$, so $w = s_A$; thus after w is deleted s_A will not be found in any component A^i_w (for $i = 1, \ldots, k(w)$), hence $A^s_w = \mathring{0}$. By a similar argument, if C is infinitesimal, $A^t_w = \mathring{0}$

- If B and C are both not infinitesimal then s_A and t_A are in different components, i.e. $i \neq j$, since s_B and t_C came from different summands. Thus w is a splitting vertex by case (1) of Definition 2.2.
- If exactly one of the flow graphs, say B, is infinitesimal (and C is not). then $A^s_w = \mathring{0}$, then part (iii) of Lemma 2.9 indicates that $A^\epsilon_w \neq \mathring{0}$. Since C is not infinitesimal, $A^t_w \neq \mathring{0}$. Thus, there are at least two non-trivial flow graphs in $\{A^1_w, \ldots, A^{k(w)}_w\}$, so w is a splitting vertex by case (2) of Definition 2.2. A similar argument holds when C is infinitesimal and B is not.
- If B, C are both infinitesimal, then so is A and by Remark 2.3, the set $\{A^i_w \mid i \in \epsilon_w\}$ contains at least two non-trivial flow graphs, so w is a splitting vertex by case (2) of Definition 2.2.

($\Leftarrow$) Let w be a splitting vertex of A. If w satisfies case (1) of Definition 2.2, then A^s_w and A^t_w are both non-trivial, and we can take $B = A^s_w$ and $C = A^\epsilon_w \oplus A^t_w$, which expresses A as the sum of two flow graphs that are both non-trivial (by part (iii) of Lemma 2.9). If w satisfies case (2) of Definition 2.2, then either A^s_w is trivial or A^t_w or both.

- If *only* A^s_w is trivial, then taking $B = A^\epsilon_w$ and $C = A^t_w$, we can express A as the sum of two flow graphs which are each non-trivial by part (iii) of Lemma 2.9. An analogous approach applies in the case when only A^t_w is trivial.
- If *both* A^s_w and A^t_w are trivial, then A is infinitesimal and so $k(w) \geqslant 2$ by Remark 2.3. We can therefore partition $\epsilon_w = \epsilon^1_w \sqcup \epsilon^2_w$, taking $B = \oplus_{i \in \epsilon^1_w} A^i_w$ and $C = \oplus_{i \in \epsilon^1_w} A^i_w$, thus expressing A as the sum of two flow graphs which are each non-trivial.

In all cases, A is $\oplus$*reducible*. □

A splitting of the form $(\mathring{0}, A, \mathring{0})$ is called a *trivial splitting*; an example is illustrated in Figure Figure 2 (pp. 136).

Proposition 2.11. *All the w-splittings of an infinitesimal flow graph are trivial splittings.*

Proof. If A is infinitesimal, and w a splitting vertex of A, then $w = s_A = t_A$ by Remark 2.3. Since step 4 in the construction of $G\backslash_* w$ (see Definition 2.1) requires deleting w, it follows that $s_A = t_A$ are not in any of the components G^*_i. By Definition 2.5, we have $A^s_w = A^t_w = \mathring{0}$, and $A^\epsilon_w = A$; thus $A\backslash_* w = (\mathring{0}, A, \mathring{0})$. □

Definition 2.12 (Splitting vertex ranking)**.** *Given flow graph $A = (G, s_A, t_A)$, define the* s-ranking *and* t-ranking *functions $r_s, r_t : \chi(A) \to \mathbb{N}$ as follows:*

$$\begin{aligned} r_s(w) &= |V[A^s_w] \cap \chi(A)|, \\ r_t(w) &= |V[A^t_w] \cap \chi(A)|. \end{aligned}$$

Lemma 2.13. *Let $w \in \chi(A)$ be a splitting vertex for flow graph $A = (G, s_A, t_A)$. Then for all $u \in V[A^s_w] \cap \chi(A)$:*

$$\begin{aligned} r_s(u) &< r_s(w), \\ r_t(u) &> r_t(w); \end{aligned}$$

and for all $u \in V[A^t_w] \cap \chi(A)$:

$$\begin{aligned} r_s(u) &> r_s(w), \\ r_t(u) &< r_t(w). \end{aligned}$$

Proof. Take $u \in V[A^s_w] \cap \chi(A)$. To show $r_s(u) < r_s(w)$, it suffices to demonstrate that $V[A^s_u] \cap \chi(A)$ is a proper subset of $V[A^s_w] \cap \chi(A)$. Let $v \in V[A^s_u] \cap \chi(A)$. Then by Observation 2.8b, $v \in \chi(A^s_w)$. Since $u \in V[A^s_w]$ and $u \in \chi(A)$, it follows by Observation 2.8b, that $u \in \chi(A^s_w)$. Now $v \in \chi(A^s_u)$ and $u \in \chi(A^s_w)$, so by Observation 2.8c, it follows that $v \in \chi(A^s_w)$. To see that the set inclusion is proper, note that $u \notin \chi(A^s_u)$ by Observation 2.8a, but $u \in \chi(A^s_w)$. Analogous arguments prove the other three assertions. □

Lemma 2.14. *Let u, v be distinct vertices in $\chi(A)$ then $r_s(u) \neq r_s(v)$ and $r_t(u) \neq r_t(v)$.*

Proof. Since $u \neq v$, by Observation 2.8e, either $u \in A^s_v$ or $u \in A^t_v$. If $u \in A^t_v$, then $v \in A^s_u$, and by Lemma 2.13, $r_s(v) < r_s(u)$. If $u \in A^s_v$, then $v \in A^t_u$, and by Lemma 2.13, $r_t(v) < r_t(u)$. □

Lemma 2.15. *Given a flow graph $A = (G, s_A, t_A)$, for each $i = 0, 1, \ldots, |\chi(A)| - 1$ there is a unique vertex v_i in $\chi(A)$ with the property that $r_s(v_i) = i$.*

Proof. Given two distinct vertices v, v' in $\chi(A)$, either $v \in V[A^s_{v'}]$ or $v \in V[A^t_{v'}]$. In the latter circumstance, $v' \in V[A^s_v]$ so it follows from Lemma 2.13 that $r_s(v') < r_s(v)$.

Base case, $i = 0$. Let w_0 be any vertex in $\chi(A)$. If $r_s(w_0) > 0$, then $V[A^s_{w_0}] \cap \chi(A)$ is not empty. So let w_1 be any vertex in $V[A^s_{w_0}] \cap \chi(A)$. By Lemma 2.13, $r_s(w_1) < r_s(w_0)$. Repeating in this fashion, after finitely many steps $w_0 \rightsquigarrow w_1 \rightsquigarrow \ldots$ we find some vertex v_0 for which $r_s(v_0) = 0$.

Inductive step $i + 1$: Let v_i be the unique vertex in $\chi(A)$ having $r_s(v_i) = i$. Define v_{i+1} to be the vertex in $V[A^t_{v_i}] \cap \chi(A)$ for whose s-rank is minimum (which exists because the s-rank of all cut vertices are distinct, by Lemma 2.14). It now follows that $r_s(v_{i+1}) = r_s(v_i) + 1 = i + 1$, hence the result. □

Definition 2.16 (Canonical $\oplus$-decomposition)**.** *Let $A = (G, s_A, t_A)$ be a flow graph. If $\chi(A) = \emptyset$ and A is infinitesimal, then the canonical $\oplus$-decomposition of A is defined to be the formal sum $\mathring{0} \oplus A \oplus \mathring{0}$. If $\chi(A) = \emptyset$ and A is non-infinitesimal, the canonical $\oplus$-decomposition of A is defined to be A.*

Otherwise, let $\chi(A) = \{v_0, v_1, \ldots, v_{|\chi(A)|-1}\}$ *be the non-empty set of splitting vertices of* A*, ordered according to the indexing scheme postulated in Lemma 2.15. Define* $A^{(0)} = A^s_{v_0}$, $A^{\epsilon(0)} = A^\epsilon_{v_0}$, $\bar{A}^{(0)} = A^t_{v_0}$, *and then for each* $i = 1, 2, \ldots, |\chi(A)| - 1$, *put*

$$\begin{aligned} A^{(i)} &= (\bar{A}^{(i-1)})^s_{v_i}, \\ A^{\epsilon(i)} &= (\bar{A}^{(i-1)})^\epsilon_{v_i}, \\ \bar{A}^{(i)} &= (\bar{A}^{(i-1)})^t_{v_i}. \end{aligned}$$

We shall denote $\bar{A}^{(|\chi(A)|-1)}$ *as* $A^{(|\chi(A)|)}$. *The* canonical $\oplus$-decomposition of A *is defined to be the* formal *summation:*

$$\langle A \rangle \stackrel{\text{def}}{=} A^{(0)} \oplus A^{\epsilon(0)} \oplus A^{(1)} \oplus A^{\epsilon(1)} \ldots \oplus A^{(|\chi(A)|-1)} \oplus A^{\epsilon(|\chi(A)|-1)} \oplus A^{(|\chi(A)|)}.$$

Note that Lemma 2.15 and effectiveness of the definition above together guarantee the uniqueness of the decomposition.

Definition 2.17 (Alternating sum)**.** *A sum* $A_0 \oplus A_1 \oplus \cdots \oplus A_{2k}$ *(*$k \in \mathbb{N}$*) is called an* alternating sum *of weight* k *if*

$$A_i \quad \textit{is} \quad \begin{cases} \textit{either trivial or infinitesimal} & i \textit{ is odd,} \\ \textit{non-trivial, non-infinitesimal, and } \oplus\textit{-irreducible} & 0 < i < 2k, \textit{ i is even,} \\ \textit{non-infinitesimal and } \oplus\textit{-irreducible} & i = 0 \textit{ or } i = 2k. \end{cases}$$

no two adjacent elements A_i, A_{i+1} *(*$i = 0, \ldots, 2k-1$*) are trivial.*

Remark 2.18. *It is easy to see that given a flow graph* A *expressed as an alternating sum:*

$$A = A_0 \oplus A_1 \oplus \cdots \oplus A_{2m}$$

the set of its splitting vertices $\chi(A) = \chi(A_0 \oplus A_1 \oplus \cdots \oplus A_{2m})$ *is precisely* $\{s_{A_i} \mid i \textit{ odd}\}$ *under the suitable embeddings of* $A_i \hookrightarrow A_0 \oplus A_1 \oplus \cdots \oplus A_{2m}$.

Proposition 2.19 (Correctness of the $\oplus$-decomposition)**.** *Let* $A = (G, s_A, t_A)$ *be a flow graph. Then* $\langle A \rangle$ *is an alternating sum of weight* $|\chi(A)|$ *which satisfies* $\langle A \rangle = A$.

Proof. We prove by induction on $|\chi(A)|$. If $|\chi(A)| = 0$, then $\langle A \rangle = A$ trivially. Suppose $|\chi(A)| = n > 1$. Let w be the unique vertex for which $r_s(w) = 0$. As a formal summation, $\langle A \rangle = A^s_w \oplus A^\epsilon_w \oplus \langle A^t_w \rangle$. Since $|\chi(A^t_w)| = n - 1$, by inductive hypothesis, $\langle A^t_w \rangle = A^t_w$ has weight $n-1$. This implies that $\langle A \rangle = A^s_w \oplus A^\epsilon_w \oplus A^t_w$ has weight n, and so $A^s_w \oplus A^\epsilon_w \oplus A^t_w = A$. □

Given a flow graph A, we see that $\langle A \rangle$ is an alternating sum. The next proposition shows that it is canonical, and that up to isomorphism, there is only one alternating sum which evaluates to A, namely $\langle A \rangle$.

Proposition 2.20 (Component-wise decomposition of isomorphisms under $\oplus$)**.** *Suppose A and B are two isomorphic flow graphs, expressed as alternating sums:*

$$\begin{aligned} A &= A_0 \oplus A_1 \oplus \cdots \oplus A_{2m}, \\ B &= B_0 \oplus B_1 \oplus \cdots \oplus B_{2n} \end{aligned}$$

Then $m = n$ and every isomorphism $\phi : A \to B$ satisfies $\phi(A_i) = B_i$ (for $i = 1, \ldots m$).

Proof. Clearly, $\phi|_{\chi(A)}$ a bijection from $\chi(A)$ to $\chi(B)$. By Remark 2.18, for each i in $\{0, \ldots, |\chi(A)| - 1\}$, there exists some j in $\mathbb{N}$, such that $\phi(s_{A_{2i+1}}) = s_{B_{2j+1}}$. Take u_i to be the image of $s_{A_{2i+1}}$ in A under the natural embedding $A_{2i+1} \hookrightarrow A$, and v_j to be the image of $s_{B_{2j+1}}$ in B under the natural embedding $B_{2j+1} \hookrightarrow B$. Then $\phi(u_i) = v_j$ implies ϕ maps $\chi(A^s_{u_i})$, having size i, bijectively onto $\chi(B^s_{v_j})$, having size j. It follows that $i = j$. Since $\phi(u_i) = v_i$, the u_i splitting of A equals the v_i splitting of B, i.e.

$$\begin{aligned} \phi(A^s_{u_i}) &= B^s_{v_i} \\ \phi(A^\epsilon_{u_i}) &= B^\epsilon_{v_i} \\ \phi(A^t_{u_i}) &= B^t_{v_i}. \end{aligned}$$

In the case when $i = m - 1$, $u_{m-1} = s_{A_{2(m-1)+1}}$ and $v_{m-1} = s_{B_{2(m-1)+1}}$. Since $\chi(A^t_{u_{m-1}})$ is empty, $\chi(B^t_{v_{m-1}})$ must also be empty. Hence $2(m-1)+1 = 2n-1$, and therefore $m = n$.

Now if $|\chi(A)| = 0$ the theorem is trivially true. Suppose $|\chi(A)| = m > 0$. Then $\phi(u_{m-1}) = v_{m-1}$ and so $\phi(A^s_{u_{m-1}}) = B^s_{v_{m-1}}$. Since $|\chi(A^s_{u_{m-1}})| = m - 1$ the inductive hypothesis applies and ϕ maps $A_0 \oplus A_1 \oplus \cdots \oplus A_{2(m-1)}$ component-wise onto $B_0 \oplus B_1 \oplus \cdots \oplus B_{2(m-1)}$. Since A_{m-1}, B_{m-1} are infinitesimal or trivial, and A_m, B_m are non-infinitesimal or trivial (but not both can be trivial, it follows that ϕ maps A_{m-1} onto B_{m-1} and A_m onto B_m. □

We might hope that the proposition above would enable us to convert an isomorphism $\phi : A \oplus B \to A \oplus C$ into an isomorphism $B \to C$. However, the obvious candidate based on the natural embeddings

$$\begin{aligned} \sigma_{A,B} &: A \hookrightarrow A \oplus B \\ \tau_{A,B} &: B \hookrightarrow A \oplus B \\ \sigma_{A,C} &: A \hookrightarrow A \oplus C \\ \tau_{A,C} &: C \hookrightarrow A \oplus C \end{aligned}$$

is $\tau^{-1}_{A,C} \circ \phi|_B \circ \tau_{A,B}$, but this is well-defined only when $\phi(Im(\tau_{A,B})) = Im(\tau_{t_A,C})$. Unfortunately, this may not be the case—a counterexample is given in Figure 4, where ϕ is the isomorphism of rigid translation to the right, and the canonical embeddings σ and τ are vertical translations. The next Lemma shows that one can make a surgical alteration to ϕ to correct this difficulty.

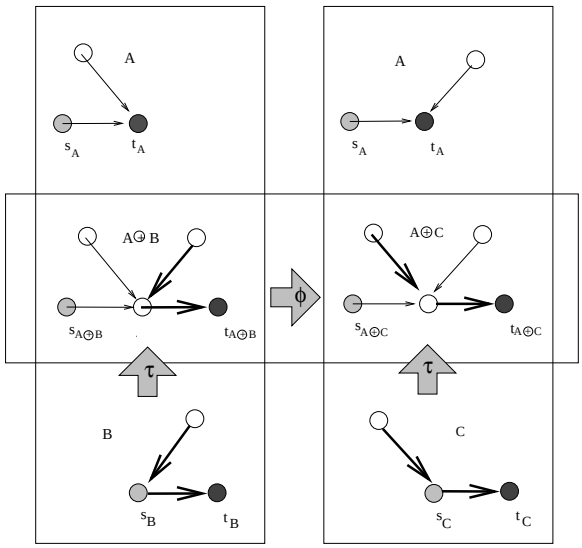

Figure 4: An example: component-wise decomposition of isomorphisms do not imply a cancellation law.

Lemma 2.21 (Surgery Lemma)**.** *Let A, B, C be flow graphs satisfying $A \oplus B = A \oplus C$ via isomorhism $\phi : A \oplus B \to A \oplus C$. Then there exists an isomorphism $\psi : A \oplus B \to A \oplus C$ such that*

$$\psi(Im(\sigma_{A,B})) = Im(\sigma_{A,C}),$$
$$\psi(Im(\tau_{A,B})) = Im(\tau_{A,C}).$$

Proof. If *at most one* of the two summands $A^{(2|\chi(A)|)}$ and $B^{(0)}$ are $\mathring{0}$ then $\langle A \oplus B \rangle$ is formally equal to $\langle A \rangle \oplus \langle C \rangle$. By Proposition 2.20 the result follows by taking $\psi = \phi$.

If both $A^{(2|\chi(A)|)} = B^{(0)} = \mathring{0}$ and $(A \oplus B)^{(2|\chi(A)|-1)} = A^{(2|\chi(A)|-1)} \oplus B^{(1)}$. Let ψ_0 be the identity function on $A^{(2|\chi(A)|-1)} \oplus B^{(1)}$, which each summand identically onto itself. Note that the corresponding restriction of ϕ need not have this property. We define ψ as follows:

$$\begin{aligned}
\psi|_{\sigma(A_i)} &\equiv \phi|_{\sigma(A_i)} && \text{if } i < 2|\chi(A)| - 1,\\
\psi|_{\tau(B_j)} &\equiv \phi|_{\tau(B_j)} && \text{if } j > 1,\\
\psi|_{\sigma(A^{(2|\chi(A)|-1)})} &\equiv \phi_0|_{\sigma^{-1}(A^{(2|\chi(A)|-1)})},\\
\psi|_{\tau(B^{(1)})} &\equiv \phi_0|_{\tau^{-1}(B^{(1)})}.
\end{aligned}$$

By construction, the isomorphism ψ has the desired property. □

Corollary 2.22 (Cancellation laws)**.** *Let A, B, C be flow graphs; $A \oplus B = A \oplus C \Rightarrow B = C$, and $B \oplus A = C \oplus A \Rightarrow B = C$.*

Proof. Suppose $A \oplus B = A \oplus C$. By Lemma 2.21, there is an isomorphism $\psi : A \oplus B \to A \oplus C$ satisfying $\psi(Im(\tau_{A,B})) = Im(\tau_{A,C})$. Then $\tau_{A,C}^{-1} \circ \phi|_B \circ \tau_{A,B} : B \to C$ is an isomorphism of flow graphs, and so $B = C$. □

Theorem 2.23 (Commutativity condition for $\oplus$)**.** *Two non-trivial flow graphs $A = (G, s_A, t_A)$ and $B = (H, s_B, t_B)$, commute with respect to addition iff there is a flow graph C and k_1, k_2 in $\mathbb{N}$ such that $A = k_1 C$ and $B = k_2 C$.*

Proof. [$\Leftarrow$] If $A = k_1 C$ and $B = k_2 C$, then $A \oplus B = (k_1 + k_2)C = B \oplus A$.

[$\Rightarrow$] Consider the canonical decompositions of A and B, viewed as alternating sums:

$$\begin{aligned} A &= A_0 \oplus A_1 \oplus A_2 \oplus \cdots \oplus A_{2m-1} \oplus A_{2m}, \\ B &= B_0 \oplus B_1 \oplus B_2 \oplus \cdots \oplus B_{2n-1} \oplus B_{2n}. \end{aligned}$$

The proof is carried by induction on $\max(2m, 2n)$.

If $m = n$ then Proposition 2.20 tells us that an isomorphism $\phi : A \oplus B \to B \oplus A$ can be surgically adjusted (see Lemma 2.21) to yield an isomorphism from A to B. So in this case, we can take $C = A = B$ and $k_1 = k_2 = 1$. This proves the case $m = 2n$ which forms the basis of the induction.

Suppose that $\max(m, n) > 0$, and $m \neq n$. Without loss of generality, suppose $m < n$. Then $A_i = B_i$ for $i = 0, \ldots, 2m$. It follows that

$$B_{i+(2m+1)} = B_i \text{ for } i = 0, \ldots, 2n - (2m+1), \quad (1)$$
$$B_{i-(2m+1)} = B_i \text{ for } i = (2m+1), \ldots, 2n. \quad (2)$$

If $(2n+1)$ is divisible by $(2m+1)$, then expressions (1) and (2) above are in fact equivalent, and in this setting, we take $C = A$, $k_1 = 1$ and $k_2 = \frac{(2n+1)}{(2m+1)}$ in order to satisfy the proposition. Suppose now that $(2n+1)$ is *not* divisible by $(2m+1)$. Put

$$\begin{aligned} d &= \left\lfloor \frac{(2n+1)}{(2m+1)} \right\rfloor, \text{ and} \\ r &= (2n+1) \mod (2m+1). \end{aligned}$$

and define

$$\begin{aligned} X &= B_0 \oplus B_1 \cdots \oplus B_{r-1}, \\ Y &= B_r \oplus B_{r+1} \cdots \oplus B_{2m}. \end{aligned}$$

Note that $B = dA \oplus X$ and

$$\begin{aligned} A &= A_0 \oplus A_1 \oplus A_2 \oplus \cdots \oplus A_{2m-1} \oplus A_{2m} \\ &= B_0 \oplus B_1 \oplus \cdots B_{r-1} \oplus B_r \oplus B_{r+1} \cdots \oplus B_{2m-1} \oplus B_{2m} \\ &= X \oplus Y. \end{aligned}$$

It follows that $B = d(X \oplus Y) \oplus X$. On the other hand, $X \oplus Y = A = Y \oplus X$ (see Figure 5), since

$$\begin{aligned} X \oplus Y &= A \\ &= A_0 \oplus A_1 \oplus \cdots \oplus A_{2m} \\ &= B_0 \oplus B_1 \oplus \cdots \oplus B_r \oplus \cdots \oplus B_{2m-1} \oplus B_{2m} \\ &= B_r \oplus \cdots \oplus B_{2n-1} \oplus B_{2n} \oplus B_0 \oplus \cdots \oplus B_{r-1} \\ &= Y \oplus X. \end{aligned}$$

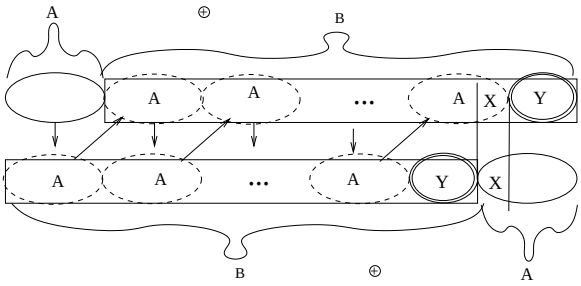

Figure 5: Inductive step showing $X \oplus Y = A = Y \oplus X$.

Since $r \neq 0$ the inductive hypothesis applies to the flow graphs X, Y, i.e. there exists some flow graph Z and suitable integers l_1, l_2 so that $X = l_1 Z$, $Y = l_2 Z$. It follows that

$$\begin{aligned} A &= X \oplus Y = l_1 Z \oplus l_2 Z = (l_1 + l_2)Z \text{ and} \\ B &= dA \oplus X = d(X \oplus Y) \oplus X = d(l_1 + l_2)Z \oplus l_1 Z = ((d+1)l_1 + l_2)Z. \end{aligned}$$

So taking $C = Z$, $k_1 = l_1 + l_2$ and $k_2 = (d+1)l_1 + l_2$, the theorem is proved. □

If A be a flow graph, then $C_{\mathcal{F}}(\{A\}) = \{B \in F \mid A \oplus B = B \oplus A\}$ is called the *additive centralizer* of A in $\mathcal{F}$.

Definition 2.24 (k-additive root)**.** *If A and B be flow graph, then the B is called the* k-additive root *of A if B is $\oplus$-irreducible and there exists a positive integer k such that $A = kB$.*

Lemma 2.25 (Additive roots)**.** *Additive roots are unique in $\mathcal{F}$.*

Proof. If A trivial, or if A is non-trivial and $\oplus$-irreducible then $A = 1A$ and A is its own unique additive root. Suppose A is non-trivial and $\oplus$-reducible but $A = k_1 B_1$ and $A = k_2 B_2$. Then the isomorphism from $k_1 B_1$ to $k_2 B_2$, factors through their canonical decompositions to yield an isomorphism from B_1 to B_2 □

In light of the above lemma, we denote the additive root of A as $\sqrt[\oplus]{A}$. Theorem 2.23 and Lemma 2.25 now yield a characterization of additive centralizers.

Corollary 2.26 (Additive centralizers)**.** *Let A be a flow graph. If $A \neq \mathring{0}$ then $C_{\mathcal{F}}(\{A\}) = \{\mathring{0}\} \cup \{k \sqrt[\oplus]{A} \mid k \in \mathbb{N}, k > 0\}$;*
If A is trivial, $C_{\mathcal{F}}(\{A\}) = F$, where F is the set of all flow graphs.

3 Conclusions

Building on a graph-theoretic characterization of flow graph $\oplus$-reducibility, we developed canonical (additive) decompositions for flow graph. Such decompositions enable us to restrict flow graph isomorphisms to irreducible summands, and carry out inductive arguments. This, in turn, permits us to verify cancellation laws, and explore the implications of additive commutation between flow graphs. On the latter question, we determine that if two flow graphs A and B commute with respect to $\oplus$ then they must both necessarily be scalar multiples of some flow graph C. This, in turn allows us to show that the centralizer of any non-trivial flow graph A in $\mathcal{F}$ "looks like" $\mathbb{N}$, in the sense that it consists of left scalar multiples of the additive root of A. The question of multiplicative centralizers remains open, and is to be the subject of subsequent inquiry.

While the results presented here advance our understanding of the additive semigroup, any future practical applications of this work to the development of cryptographic schemes will likely require parallel progress to be made on the properties of multiplication in $\mathcal{F}$. In particular, the structure of ideals and the difficulty of factorization remain areas of ongoing inquiry. It is our hope that once the theory of both addition and multiplication in $\mathcal{F}$ have been more fully developed (and their interplay is better understood), new practical applications involving flow graph based cryptography will become accessible.

Acknowledgments

The authors would like to thank the referees for many helpful comments and suggestions. Also, we wish to thank The Catholic University of America for travel grants in support of this research.

References

[1] N. Alon, *Graph powers*, In Contemporary Combinatorics, (B. Bollobas, ed), Bolyai Society Mathematical Studies, Springer, (2002), 11–28.

[2] K. Bhutani, B. Khan and D. Kahrobaei, A graphic generalization of arithmetic, *INTEGERS*, **7** (2007), #A12.

[3] G. Cantor, *Uber unendliche, lineare Punktmannigfaltigkeiten, Arbeiten zur Mengenlehre aus dem Jahren 1872-1884*, Teubner-Archiv zur Mathematik, Leipzig, Germany, 1884.

[4] K. Ciesielski, *Set Theory for the Working Mathematician*, Cambridge University Press, 1997.

[5] C. Godsil and B. McKay, A new graph product and its spectrum, *Bull. Aust. Math. Soc.*, **18** (1978), 21–28.

[6] W. Imrich and S. Klavzar, *Product Graphs, Structure and Recognition*, John Wiley & Sons Inc., 2000.

[7] A. Kaveh and K. Laknejadi, Factorization of product graphs for partitioning and domain decomposition, *Finite Elem. Anal. Des.*, **45**(6-7) (2009), 476–483.

[8] L. Kirby, Ordinal operations on graph representations of sets, *Mathematical Logic Quarterly*, **59**(1) (2013), 19–26.

[9] J. Li, Prime graphs and exponential composition of species, *J. Combin. Theory Ser. A*, **115** (8) (2008), 1374–1401.

[10] D. M. Monarres and M. E. O'Sullivan, *A generalization of the zig-zag graph product by means of the sandwich product*, In Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-18 '09, Berlin, Heidelberg, Springer-Verlag, (2009), 231–234.

[11] J. E. Rubin, *Theory for the Mathematician*, Holden-Day, New York, 1967.

[12] G. Sabidussi, Graph multiplication, *Mathematische Zeitschrift*, **72** (1959), 446–457.

[13] P. Suppes, *Axiomatic Set Theory*, Dover, New York, 1972.

[14] P. M. Weichsel, The Kronecker Product of Graphs, *Proc. Amer. Math. Soc.*, **13** (1) (1962), 47–52.

[15] D. B. West, *Introduction to Graph Theory*, Prentice Hall, 2nd edition, 2001.