Cryptography Based on (Idempotent) Semirings: Abandoning Tropicality?

Subjects: Computer Science, Cybernetics

Contributor: Mariana Durcheva

This review explores the current state of public key cryptography based on idempotent semirings, with an emphasis on tropical semirings. It examines key hard problems, such as the tropical discrete logarithm problem, semidirect tropical product problem, the factorization of tropical polynomials, and the matrix power function, that underpin the security of these protocols. Given the significant number of compromised protocols based on tropical semirings, most of which are variations of the Stickel protocol, we present three algorithms and classify schemes of this type. The analysis is further illustrated with a figure that maps the relationships between tropical Stickel's-like protocols and the attacks targeting them. Additionally, the review provides an in-depth exploration of the vulnerabilities that have led to many tropical semiring-based cryptosystems being compromised. To address these challenges, the review highlights promising alternative approaches, including non-tropical idempotent platforms and non-idempotent options, such as supertropical semirings, which offer potential solutions to overcome known limitations. Furthermore, a discussion on the interplay between tropical cryptography and post-quantum cryptography is presented, raising the following question: what is the future of tropical cryptography?

semiring idempotent semiring tropical cryptography Stickel's-like protocol

Semirings were first introduced implicitly in [1] and later appeared in other works related to the study of ideals in rings. They were further discussed in [2] in connection with the formalization of non-negative integers and rational numbers. The concept of semirings was first explicitly defined in [3], specifically in the context of the axiomatization of natural number arithmetic. Throughout time, numerous researchers have conducted extensive studies of semirings, both as a natural extension of methods from semigroup and ring theory and in connection with practical applications. These applications cover a wide range of fields, including computer science and automata theory. For example, weighted automata, which assign weights to transitions, often utilize semirings, such as the tropical semiring, to model and analyze language properties [4]. In dynamic programming, numerous algorithms, including Dijkstra's algorithm and the Viterbi algorithm, are built upon semiring structures [5]. Furthermore, specific semiring operations enable the addressing of certain NP-hard problems such as Connected Dominating Set problems and finite-domain Constraint Satisfaction Problems [6]. Tropical semirings (max, +) play a pivotal role in algorithms related to the shortest paths, minimal spanning trees, and network flows [7]. Optimization problems with particular algebraic constraints can be effectively formulated using semirings to find efficient solutions. Semirings are widely applied in control theory and discrete event systems. For instance, tropical semirings are instrumental in modeling and analyzing discrete event systems, including automated manufacturing systems and traffic control [8]. In systems theory, semirings provide a framework for representing systems where operations like "max" and "min" replace traditional addition and multiplication, enabling the handling of nonlinearities in models [9]. They are also employed in certain signal processing tasks, such as wavelet transforms and max-plus transforms, which are used

for signal filtering and compression [10]. Semirings have diverse applications in artificial intelligence (AI) and machine learning. For example, neural networks can be trained to learn semiring operations, enabling more effective reasoning in symbolic AI tasks [11]. Semiring programming offers a unified framework for integrating various AI disciplines, such as SAT solving, Bayesian inference, and convex optimization [12]. In ontology learning, semirings help structure data for machine understanding in the Semantic Web, aiding in the construction and refinement of ontologies [13]. In economics and game theory, semirings are used to model scenarios like mean payoff games, where algebraic operations over semirings describe decision-making processes involving costs and rewards [14]. In phylogenetics and biological modeling, tropical semirings are employed to model evolutionary distances and relationships between species, enabling researchers to construct accurate evolutionary trees. Additionally, semirings address optimization problems in biological systems, such as protein production pathways and cellular processes [15]. In railway scheduling and logistics, semirings provide a framework for modeling scheduling and resource allocation challenges, ensuring tasks are completed efficiently while adhering to time or resource constraints [16].

A compelling motivation for this research is the field of semiring-based cryptography, which traces its origins to the seminal work in [17], introducing one of the first cryptosystems leveraging semigroups and semirings. Since then, numerous cryptosystems have been developed using semirings, with a particular focus on tropical and idempotent semirings. These algebraic structures are being actively explored as promising alternatives to classical cryptographic frameworks, especially for constructing secure key exchange protocols. However, despite their potential, many of these systems have been compromised over time, underscoring the critical need for further research and advancements in this area.

Most of our attention will be focused on tropical cryptography due to its versatile applications in real-world scenarios that require cryptographic mechanisms, such as SSL, SSH, and IPSec. Various tropical semiring-based protocols offer exceptional robustness and efficiency, making them particularly well suited for contemporary IoT ecosystems. In these settings, devices frequently function with limited resources and demand rapid and at the same time secure communication. Furthermore, such schemes seamlessly embed into blockchains to boost the safety of trade operations and digital contracts while providing additional defenses to resist typical flaws in distributed networks. Their inherent resilience to targeted algebraic attacks also makes them perfect for protecting information in cloud-based systems, where data integrity and privacy are critical. Namely, this adaptability positions tropical algebra as a solid foundation for applying cutting-edge security protocols throughout a wide range of web-based platforms and applications.

In this work, we present the current situation in the field of cryptography based on idempotent semirings and revisit the most prominent tropical-based protocols from the literature, with a particular focus on Stickel's-like protocols, which constitute the majority of the proposed schemes. Our main contributions include analyzing the underlying problems upon which the security of these protocols relies, examining existing attacks against them, and discussing solutions and strategies for developing more secure protocols in light of the post-quantum cryptography landscape. Recognizing concerns about the future of tropical cryptography, we have also extended our discussion

to cryptographic approaches that utilize various types of semirings, including non-idempotent ones, as possible platforms.

This paper is structured as follows: Section 2 presents an overview of idempotent semirings. Section 3 discusses the current state of tropical cryptography, including existing attacks and several promising approaches to address these challenges. Section 4 explores cryptography based on idempotent but non-tropical semirings as a possible platform. Section 5 examines the potential of abandoning idempotency as a strategy for constructing more secure cryptographic schemes. Finally, Section 6 offers a discussion and concludes the paper.

Semirings were first introduced implicitly in [1] and later appeared in other works related to the study of ideals in rings. They were further discussed in [2] in connection with the formalization of non-negative integers and rational numbers. The concept of semirings was first explicitly defined in [3], specifically in the context of the axiomatization of natural number arithmetic. Throughout time, numerous researchers have conducted extensive studies of semirings, both as a natural extension of methods from semigroup and ring theory and in connection with practical applications. These applications cover a wide range of fields, including computer science and automata theory. For example, weighted automata, which assign weights to transitions, often utilize semirings, such as the tropical semiring, to model and analyze language properties [4]. In dynamic programming, numerous algorithms, including Dijkstra's algorithm and the Viterbi algorithm, are built upon semiring structures [5]. Furthermore, specific semiring operations enable the addressing of certain NP-hard problems such as Connected Dominating Set problems and finite-domain Constraint Satisfaction Problems [6]. Tropical semirings (max, +) play a pivotal role in algorithms related to the shortest paths, minimal spanning trees, and network flows [7]. Optimization problems with particular algebraic constraints can be effectively formulated using semirings to find efficient solutions. Semirings are widely applied in control theory and discrete event systems. For instance, tropical semirings are instrumental in modeling and analyzing discrete event systems, including automated manufacturing systems and traffic control [8]. In systems theory, semirings provide a framework for representing systems where operations like "max" and "min" replace traditional addition and multiplication, enabling the handling of nonlinearities in models [9]. They are also employed in certain signal processing tasks, such as wavelet transforms and max-plus transforms, which are used for signal filtering and compression [10]. Semirings have diverse applications in artificial intelligence (AI) and machine learning. For example, neural networks can be trained to learn semiring operations, enabling more effective reasoning in symbolic AI tasks [11]. Semiring programming offers a unified framework for integrating various AI disciplines, such as SAT solving, Bayesian inference, and convex optimization [12]. In ontology learning, semirings help structure data for machine understanding in the Semantic Web, aiding in the construction and refinement of ontologies [13]. In economics and game theory, semirings are used to model scenarios like mean payoff games, where algebraic operations over semirings describe decision-making processes involving costs and rewards [14]. In phylogenetics and biological modeling, tropical semirings are employed to model evolutionary distances and relationships between species, enabling researchers to construct accurate evolutionary trees. Additionally, semirings address optimization problems in biological systems, such as protein production pathways and cellular processes [15]. In railway scheduling and logistics, semirings provide a framework for modeling scheduling and resource allocation challenges, ensuring tasks are completed efficiently while adhering to time or resource constraints [16].

A compelling motivation for this research is the field of semiring-based cryptography, which traces its origins to the seminal work in [17], introducing one of the first cryptosystems leveraging semigroups and semirings. Since then, numerous cryptosystems have been developed using semirings, with a particular focus on tropical and idempotent semirings. These algebraic structures are being actively explored as promising alternatives to classical cryptographic frameworks, especially for constructing secure key exchange protocols. However, despite their potential, many of these systems have been compromised over time, underscoring the critical need for further research and advancements in this area.

Most of our attention will be focused on tropical cryptography due to its versatile applications in real-world scenarios that require cryptographic mechanisms, such as SSL, SSH, and IPSec. Various tropical semiring-based protocols offer exceptional robustness and efficiency, making them particularly well suited for contemporary IoT ecosystems. In these settings, devices frequently function with limited resources and demand rapid and at the same time secure communication. Furthermore, such schemes seamlessly embed into blockchains to boost the safety of trade operations and digital contracts while providing additional defenses to resist typical flaws in distributed networks. Their inherent resilience to targeted algebraic attacks also makes them perfect for protecting information in cloud-based systems, where data integrity and privacy are critical. Namely, this adaptability positions tropical algebra as a solid foundation for applying cutting-edge security protocols throughout a wide range of web-based platforms and applications.

In this work, we present the current situation in the field of cryptography based on idempotent semirings and revisit the most prominent tropical-based protocols from the literature, with a particular focus on Stickel's-like protocols, which constitute the majority of the proposed schemes. Our main contributions include analyzing the underlying problems upon which the security of these protocols relies, examining existing attacks against them, and discussing solutions and strategies for developing more secure protocols in light of the post-quantum cryptography landscape. Recognizing concerns about the future of tropical cryptography, we have also extended our discussion to cryptographic approaches that utilize various types of semirings, including non-idempotent ones, as possible platforms.

This paper is structured as follows: Section 2 presents an overview of idempotent semirings. Section 3 discusses the current state of tropical cryptography, including existing attacks and several promising approaches to address these challenges. Section 4 explores cryptography based on idempotent but non-tropical semirings as a possible platform. Section 5 examines the potential of abandoning idempotency as a strategy for constructing more secure cryptographic schemes. Finally, Section 6 offers a discussion and concludes the paper.

Semirings were first introduced implicitly in [1] and later appeared in other works related to the study of ideals in rings. They were further discussed in [2] in connection with the formalization of non-negative integers and rational numbers. The concept of semirings was first explicitly defined in [3], specifically in the context of the axiomatization of natural number arithmetic. Throughout time, numerous researchers have conducted extensive studies of semirings, both as a natural extension of methods from semigroup and ring theory and in connection with practical applications. These applications cover a wide range of fields, including computer science and automata theory. For example, weighted automata, which assign weights to transitions, often utilize semirings, such as the tropical

semiring, to model and analyze language properties [4]. In dynamic programming, numerous algorithms, including Dijkstra's algorithm and the Viterbi algorithm, are built upon semiring structures [5]. Furthermore, specific semiring operations enable the addressing of certain NP-hard problems such as Connected Dominating Set problems and finite-domain Constraint Satisfaction Problems [6]. Tropical semirings (max, +) play a pivotal role in algorithms related to the shortest paths, minimal spanning trees, and network flows [7]. Optimization problems with particular algebraic constraints can be effectively formulated using semirings to find efficient solutions. Semirings are widely applied in control theory and discrete event systems. For instance, tropical semirings are instrumental in modeling and analyzing discrete event systems, including automated manufacturing systems and traffic control [8]. In systems theory, semirings provide a framework for representing systems where operations like "max" and "min" replace traditional addition and multiplication, enabling the handling of nonlinearities in models [9]. They are also employed in certain signal processing tasks, such as wavelet transforms and max-plus transforms, which are used for signal filtering and compression [10]. Semirings have diverse applications in artificial intelligence (AI) and machine learning. For example, neural networks can be trained to learn semiring operations, enabling more effective reasoning in symbolic AI tasks [11]. Semiring programming offers a unified framework for integrating various AI disciplines, such as SAT solving, Bayesian inference, and convex optimization [12]. In ontology learning, semirings help structure data for machine understanding in the Semantic Web, aiding in the construction and refinement of ontologies [13]. In economics and game theory, semirings are used to model scenarios like mean payoff games, where algebraic operations over semirings describe decision-making processes involving costs and rewards [14]. In phylogenetics and biological modeling, tropical semirings are employed to model evolutionary distances and relationships between species, enabling researchers to construct accurate evolutionary trees. Additionally, semirings address optimization problems in biological systems, such as protein production pathways and cellular processes [15]. In railway scheduling and logistics, semirings provide a framework for modeling scheduling and resource allocation challenges, ensuring tasks are completed efficiently while adhering to time or resource constraints [16].

A compelling motivation for this research is the field of semiring-based cryptography, which traces its origins to the seminal work in [17], introducing one of the first cryptosystems leveraging semigroups and semirings. Since then, numerous cryptosystems have been developed using semirings, with a particular focus on tropical and idempotent semirings. These algebraic structures are being actively explored as promising alternatives to classical cryptographic frameworks, especially for constructing secure key exchange protocols. However, despite their potential, many of these systems have been compromised over time, underscoring the critical need for further research and advancements in this area.

Most of our attention will be focused on tropical cryptography due to its versatile applications in real-world scenarios that require cryptographic mechanisms, such as SSL, SSH, and IPSec. Various tropical semiring-based protocols offer exceptional robustness and efficiency, making them particularly well suited for contemporary IoT ecosystems. In these settings, devices frequently function with limited resources and demand rapid and at the same time secure communication. Furthermore, such schemes seamlessly embed into blockchains to boost the safety of trade operations and digital contracts while providing additional defenses to resist typical flaws in distributed networks. Their inherent resilience to targeted algebraic attacks also makes them perfect for protecting

information in cloud-based systems, where data integrity and privacy are critical. Namely, this adaptability positions tropical algebra as a solid foundation for applying cutting-edge security protocols throughout a wide range of web-based platforms and applications.

In this work, we present the current situation in the field of cryptography based on idempotent semirings and revisit the most prominent tropical-based protocols from the literature, with a particular focus on Stickel's-like protocols, which constitute the majority of the proposed schemes. Our main contributions include analyzing the underlying problems upon which the security of these protocols relies, examining existing attacks against them, and discussing solutions and strategies for developing more secure protocols in light of the post-quantum cryptography landscape. Recognizing concerns about the future of tropical cryptography, we have also extended our discussion to cryptographic approaches that utilize various types of semirings, including non-idempotent ones, as possible platforms.

This paper is structured as follows: Section 2 presents an overview of idempotent semirings. Section 3 discusses the current state of tropical cryptography, including existing attacks and several promising approaches to address these challenges. Section 4 explores cryptography based on idempotent but non-tropical semirings as a possible platform. Section 5 examines the potential of abandoning idempotency as a strategy for constructing more secure cryptographic schemes. Finally, Section 6 offers a discussion and concludes the paper.

Semirings were first introduced implicitly in [1] and later appeared in other works related to the study of ideals in rings. They were further discussed in [2] in connection with the formalization of non-negative integers and rational numbers. The concept of semirings was first explicitly defined in [3], specifically in the context of the axiomatization of natural number arithmetic. Throughout time, numerous researchers have conducted extensive studies of semirings, both as a natural extension of methods from semigroup and ring theory and in connection with practical applications. These applications cover a wide range of fields, including computer science and automata theory. For example, weighted automata, which assign weights to transitions, often utilize semirings, such as the tropical semiring, to model and analyze language properties [4]. In dynamic programming, numerous algorithms, including Dijkstra's algorithm and the Viterbi algorithm, are built upon semiring structures [5]. Furthermore, specific semiring operations enable the addressing of certain NP-hard problems such as Connected Dominating Set problems and finite-domain Constraint Satisfaction Problems [6]. Tropical semirings (max, +) play a pivotal role in algorithms related to the shortest paths, minimal spanning trees, and network flows [7]. Optimization problems with particular algebraic constraints can be effectively formulated using semirings to find efficient solutions. Semirings are widely applied in control theory and discrete event systems. For instance, tropical semirings are instrumental in modeling and analyzing discrete event systems, including automated manufacturing systems and traffic control [8]. In systems theory, semirings provide a framework for representing systems where operations like "max" and "min" replace traditional addition and multiplication, enabling the handling of nonlinearities in models [9]. They are also employed in certain signal processing tasks, such as wavelet transforms and max-plus transforms, which are used for signal filtering and compression [10]. Semirings have diverse applications in artificial intelligence (AI) and machine learning. For example, neural networks can be trained to learn semiring operations, enabling more effective reasoning in symbolic AI tasks [11]. Semiring programming offers a unified framework for integrating various AI disciplines, such as SAT solving, Bayesian inference, and convex optimization [12]. In ontology learning,

semirings help structure data for machine understanding in the Semantic Web, aiding in the construction and refinement of ontologies [13]. In economics and game theory, semirings are used to model scenarios like mean payoff games, where algebraic operations over semirings describe decision-making processes involving costs and rewards [14]. In phylogenetics and biological modeling, tropical semirings are employed to model evolutionary distances and relationships between species, enabling researchers to construct accurate evolutionary trees. Additionally, semirings address optimization problems in biological systems, such as protein production pathways and cellular processes [15]. In railway scheduling and logistics, semirings provide a framework for modeling scheduling and resource allocation challenges, ensuring tasks are completed efficiently while adhering to time or resource constraints [16].

A compelling motivation for this research is the field of semiring-based cryptography, which traces its origins to the seminal work in [17], introducing one of the first cryptosystems leveraging semigroups and semirings. Since then, numerous cryptosystems have been developed using semirings, with a particular focus on tropical and idempotent semirings. These algebraic structures are being actively explored as promising alternatives to classical cryptographic frameworks, especially for constructing secure key exchange protocols. However, despite their potential, many of these systems have been compromised over time, underscoring the critical need for further research and advancements in this area.

Most of our attention will be focused on tropical cryptography due to its versatile applications in real-world scenarios that require cryptographic mechanisms, such as SSL, SSH, and IPSec. Various tropical semiring-based protocols offer exceptional robustness and efficiency, making them particularly well suited for contemporary IoT ecosystems. In these settings, devices frequently function with limited resources and demand rapid and at the same time secure communication. Furthermore, such schemes seamlessly embed into blockchains to boost the safety of trade operations and digital contracts while providing additional defenses to resist typical flaws in distributed networks. Their inherent resilience to targeted algebraic attacks also makes them perfect for protecting information in cloud-based systems, where data integrity and privacy are critical. Namely, this adaptability positions tropical algebra as a solid foundation for applying cutting-edge security protocols throughout a wide range of web-based platforms and applications.

In this work, we present the current situation in the field of cryptography based on idempotent semirings and revisit the most prominent tropical-based protocols from the literature, with a particular focus on Stickel's-like protocols, which constitute the majority of the proposed schemes. Our main contributions include analyzing the underlying problems upon which the security of these protocols relies, examining existing attacks against them, and discussing solutions and strategies for developing more secure protocols in light of the post-quantum cryptography landscape. Recognizing concerns about the future of tropical cryptography, we have also extended our discussion to cryptographic approaches that utilize various types of semirings, including non-idempotent ones, as possible platforms.

This paper is structured as follows: Section 2 presents an overview of idempotent semirings. Section 3 discusses the current state of tropical cryptography, including existing attacks and several promising approaches to address

these challenges. Section 4 explores cryptography based on idempotent but non-tropical semirings as a possible platform. Section 5 examines the potential of abandoning idempotency as a strategy for constructing more secure cryptographic schemes. Finally, Section 6 offers a discussion and concludes the paper.

Semirings were first introduced implicitly in [1] and later appeared in other works related to the study of ideals in rings. They were further discussed in [2] in connection with the formalization of non-negative integers and rational numbers. The concept of semirings was first explicitly defined in [3], specifically in the context of the axiomatization of natural number arithmetic. Throughout time, numerous researchers have conducted extensive studies of semirings, both as a natural extension of methods from semigroup and ring theory and in connection with practical applications. These applications cover a wide range of fields, including computer science and automata theory. For example, weighted automata, which assign weights to transitions, often utilize semirings, such as the tropical semiring, to model and analyze language properties [4]. In dynamic programming, numerous algorithms, including Dijkstra's algorithm and the Viterbi algorithm, are built upon semiring structures [5]. Furthermore, specific semiring operations enable the addressing of certain NP-hard problems such as Connected Dominating Set problems and finite-domain Constraint Satisfaction Problems [6]. Tropical semirings (max, +) play a pivotal role in algorithms related to the shortest paths, minimal spanning trees, and network flows [7]. Optimization problems with particular algebraic constraints can be effectively formulated using semirings to find efficient solutions. Semirings are widely applied in control theory and discrete event systems. For instance, tropical semirings are instrumental in modeling and analyzing discrete event systems, including automated manufacturing systems and traffic control [8]. In systems theory, semirings provide a framework for representing systems where operations like "max" and "min" replace traditional addition and multiplication, enabling the handling of nonlinearities in models [9]. They are also employed in certain signal processing tasks, such as wavelet transforms and max-plus transforms, which are used for signal filtering and compression [10]. Semirings have diverse applications in artificial intelligence (AI) and machine learning. For example, neural networks can be trained to learn semiring operations, enabling more effective reasoning in symbolic AI tasks [11]. Semiring programming offers a unified framework for integrating various AI disciplines, such as SAT solving, Bayesian inference, and convex optimization [12]. In ontology learning, semirings help structure data for machine understanding in the Semantic Web, aiding in the construction and refinement of ontologies [13]. In economics and game theory, semirings are used to model scenarios like mean payoff games, where algebraic operations over semirings describe decision-making processes involving costs and rewards [14]. In phylogenetics and biological modeling, tropical semirings are employed to model evolutionary distances and relationships between species, enabling researchers to construct accurate evolutionary trees. Additionally, semirings address optimization problems in biological systems, such as protein production pathways and cellular processes [15]. In railway scheduling and logistics, semirings provide a framework for modeling scheduling and resource allocation challenges, ensuring tasks are completed efficiently while adhering to time or resource constraints [16].

A compelling motivation for this research is the field of semiring-based cryptography, which traces its origins to the seminal work in [17], introducing one of the first cryptosystems leveraging semigroups and semirings. Since then, numerous cryptosystems have been developed using semirings, with a particular focus on tropical and idempotent semirings. These algebraic structures are being actively explored as promising alternatives to classical

cryptographic frameworks, especially for constructing secure key exchange protocols. However, despite their potential, many of these systems have been compromised over time, underscoring the critical need for further research and advancements in this area.

Most of our attention will be focused on tropical cryptography due to its versatile applications in real-world scenarios that require cryptographic mechanisms, such as SSL, SSH, and IPSec. Various tropical semiring-based protocols offer exceptional robustness and efficiency, making them particularly well suited for contemporary IoT ecosystems. In these settings, devices frequently function with limited resources and demand rapid and at the same time secure communication. Furthermore, such schemes seamlessly embed into blockchains to boost the safety of trade operations and digital contracts while providing additional defenses to resist typical flaws in distributed networks. Their inherent resilience to targeted algebraic attacks also makes them perfect for protecting information in cloud-based systems, where data integrity and privacy are critical. Namely, this adaptability positions tropical algebra as a solid foundation for applying cutting-edge security protocols throughout a wide range of web-based platforms and applications.

In this work, we present the current situation in the field of cryptography based on idempotent semirings and revisit the most prominent tropical-based protocols from the literature, with a particular focus on Stickel's-like protocols, which constitute the majority of the proposed schemes. Our main contributions include analyzing the underlying problems upon which the security of these protocols relies, examining existing attacks against them, and discussing solutions and strategies for developing more secure protocols in light of the post-quantum cryptography landscape. Recognizing concerns about the future of tropical cryptography, we have also extended our discussion to cryptographic approaches that utilize various types of semirings, including non-idempotent ones, as possible platforms.

This paper is structured as follows: Section 2 presents an overview of idempotent semirings. Section 3 discusses the current state of tropical cryptography, including existing attacks and several promising approaches to address these challenges. Section 4 explores cryptography based on idempotent but non-tropical semirings as a possible platform. Section 5 examines the potential of abandoning idempotency as a strategy for constructing more secure cryptographic schemes. Finally, Section 6 offers a discussion and concludes the paper.

References

1. Dedekind, R. Uber die Theorie der ganzen algebraischen Zahlen. In Supplement XI to P. G. Lejeune Dirichlet: Vorlesungen Iiber Zahlentheorie, 4th ed.; Druck und Verlag: Braunschweig, Germany, 1894.
2. Hilbert, D. Über den Zahlbegriff. Jahresber. Der Dtsch. Math.-Ver. 1899, 8, 180–184, ISSN: 0012-0456; 1869-7135.

3. Vandiver, H.S. Note on a simple type of algebra in which cancellation law of addition does not hold. Bull. Am. Math. Soc. 1934, 40, 914–920.
4. Hebisch, U.; Weinert, H.J. Semirings: Algebraic Theory and Applications in Computer Science; Series in Algebra; World Scientific Publishing Co., Ltd. Inc.: River Edge, NJ, USA, 1998; Volume 5.
5. Droste, M.; Kuich, W.; Vogler, H. (Eds.) Handbook of Weighted Automata; Springer: Berlin/Heidelberg, Germany, 2009; ISSN 1431-2654.
6. Baril, A.; Couceiro, M.; Lagerkvist, V. New Perspectives on Semiring Applications to Dynamic Programming; 2024. HAL Open Science, hal-04434071, Version 1 (02-02-2024). Available online: https://hal.science/hal-04434071v1 (accessed on 4 September 2024).
7. Butkovic, P. Max-Linear Systems: Theory and Algorithms; Springer: Berlin/Heidelberg, Germany, 2010.
8. Cohen, G.; Gaubert, S.; Quadrat, J.P. Max-plus algebra and system theory: Where we are and where to go now. Annu. Rev. Control 1999, 23, 207–219.
9. Baccelli, F.; Cohen, G.; Olsder, G.J.; Quadrat, J.P. Synchronization and Linearity: An Algebra for Discrete Event Systems; Wiley: Hoboken, NJ, USA, 1992.
10. Debnath, L.; Shah, F.A. Wavelet Transforms and Their Applications; Springer, Birkhäuser: Boston, MA, USA, 2014.
11. Martires, P.Z. Neural Semirings. International Workshop on Neural-Symbolic Learning and Reasoning. 2021. CEUR Workshop Proceedings (CEUR-WS.org). Available online: https://ceur-ws.org/Vol-2986/paper7.pdf (accessed on 3 October 2022).
12. Belle, V.; Raedt, L.D. Semiring Programming: A Framework for Search, Inference and Learning. arXiv 2016, arXiv:1609.06954.
13. Maedche, A.; Staab, S. Ontology Learning for the Semantic Web. IEEE Intell. Syst. 2002, 16, 72–79.
14. Akian, M.; Gaubert, S.; Guterman, A. Tropical Polyhedra Are Equivalent to Mean Payoff Games. Int. J. Algebra Comput. 2010, 22, 1250014.
15. Pachter, L.; Sturmfels, B. Algebraic Statistics for Computational Biology; Cambridge University Press: Cambridge, UK, 2004.
16. Heidergott, B.; Olsder, G.J.; van der Woude, J. Max Plus at Work: Modeling and Analysis of Synchronized Systems: A Course on Max-Plus Algebra and Its Applications; Princeton University Press: Princeton, NJ, USA, 2006.

17. Maze, G.; Monico, C.; Rosenthal, J. Public key cryptography based on semigroup actions. Adv. Math. Commun. 2007, 1, 489–507.