DISSERTATION

From Logic to Discrete Geometry via Lattices

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der Naturwissenschaften unter der Leitung von

Ao.Univ.Prof. Dr.phil. Matthias Baaz

E104 - Institut für Diskrete Mathematik und Geometrie

eingereicht an der Technischen Universität Wien

Fakultät für Mathematik und Geoinformation

von

MSc. Lorenzo Sauras-Altuzarra

Matr. Nr.: 01563234

E104 - Institut für Diskrete Mathematik und Geometrie

Wien, am eigenhändige Unterschrift

To the memory of my brother Ignacio

Contents

Affidavit

- I declare, in lieu of oath, that I wrote this thesis and performed the associated research myself, using only literature cited in this volume. If text passages from sources are used literally, they are marked as such.
- I confirm that this work is original and has not been submitted elsewhere for any examination, nor is it currently under consideration for a thesis elsewhere.
- I acknowledge that the submitted work will be checked electronically and technically using suitable and state-of-the-art means (plagiarism detection software). On the one hand, this ensures that the submitted work was prepared according to the high-quality standards within the applicable rules to ensure good scientific practice "Code of Conduct" at the TU Wien. On the other hand, a comparison with other student theses avoids violations of my personal copyright.

Lorenzo Sauras-Altuzarra

Acknowledgements

- I thank **Vasile Brînzănescu** for his contribution to Subsection 3.3.2.
- I thank **Cecilia Cimadamore**, **Laura Rueda** and **Néstor Thomé** for their joint work in Section 2.1.
- I thank **Gergely Harcos** for his joint work in Subsection 3.3.2 and for his instructive notions on number theory, which substantially improved the presentation of Chapter 3.
- I thank **José-Antonio Hervás-Contreras** for his contribution to Subsubsection 3.3.5.1.
- I thank **Daniele Parisse**, **Mabud Sarkar** and **René Schoof** for their contributions to Subsubsection 3.3.1.1.
- I thank **Mihai Prunescu** for his corrections in Subsection 2.2.2.
- I thank **Grigorii Stepanov** for his joint work in Subsection 2.2.1.
- I thank **Jinyuan Wang** for his contributions to Section 3.2, Subsubsection 3.3.1.2 and Subsubsection 3.3.1.3; and for his joint work in Section 3.1 and Subsection 3.3.3.
- A special word of appreciation goes to **Matthias Baaz**, my doctoral supervisor, for his faith, trust and generosity; and for having found such profitable topics for me.
- Finally, I convey my gratitude to my family, and specially to my mother, **María-Esperanza Altuzarra-Sierra**, for their love.

Lorenzo Sauras-Altuzarra

Chapter 1

Introduction

This doctoral dissertation consists of a selection of mathematical texts, which are divided into two parts: Chapter 2, whose title is "*Order-theoretic lattices*"; and Chapter 3, whose title is "*Number-theoretic lattices*".

The author's journal article "*Lattice properties of partial orders for complex matrices via orthogonal projectors*" (hereinafter called Article A) utilized lattice theory, the core of algebraic logic, in order to prove several results on the geometry of matrices. More specifically, it contains a study of the different geometric structures that the intervals of complex square matrices get when sorted by three important partial orders in matrix theory (viz., the left-star order, the star order and the core order).

Chapter 2 contains Article A in Section 2.1, as well as a complete and finitely axiomatizable foundation of ultrafinitist mathematics in Subsection 2.2.1 and a connection between the arithmetical hierarchy and the irrationality measure in Subsection 2.2.2.

The author's journal articles "*Some properties of the factors of Fermat numbers*" (hereinafter called Article B) and "*Some applications of Baaz's generalization method to the study of the factors of Fermat numbers*" (hereinafter called Article C) are part of an ongoing research project on the geometry of numbers, which had its origin in Baaz's article "*Note on the generalization of calculations*" (see Baaz [1]).

The common procedure in these three articles is the application of a new technique of extractive proof theory, called Baaz's generalization method, to different proofs of compositeness of some concrete Fermat numbers. The information that was extracted from these proofs led to several new results, among which stands out

Theorem 3.0.0.1, which is a geometric characterization of the factors of Fermat numbers in terms of point-lattices and of a new concept called cover.

Chapter 3 contains Article B in Section 3.1 and Article C in Section 3.2, as well as further investigation on the theory of covers in Subsection 3.3.1, related results on the factorization of near-square numbers and of Mersenne numbers in Subsection 3.3.2 and Subsection 3.3.3 respectively, an iterative expression of the products of the first consecutive generalized Fermat numbers in Subsection 3.3.4 and a detailed study of a new object, called Hervás-Contreras chain, in Subsection 3.3.5.

Chapter 2

Order-theoretic lattices

Algebraic logic is the mathematical field which translates logic into algebra by transforming logical systems into Lindenbaum–Tarski algebras.

These algebras are often expressed as partially ordered sets in which the existence of infima and suprema of finite non-empty subsets is ensured, called **order-theoretic lattices** or simply **lattices** (see Section 1 of Article A in Section 2.1).

The most paradigmatic lattices are probably the **Boolean algebras** (see Section 1 of Article A in Section 2.1), since they are the algebraic counterpart of classic propositional logic (by identifying conjunctions with infima, disjunctions with suprema and negations with complements). In addition, they appear in many other mathematical contexts of central importance, such as finite set theory (by identifying the intersections of the elements of a power set with infima, the unions with suprema and the absolute complements with complements) or number theory (because the number of ordered partitions of a positive integer n is 2^{n-1} or, equivalently, the cardinality of the power set of a set of $n-1$ elements; see OEIS A000079).

Article A makes use of lattice theory to provide a structural description of the intervals of complex square matrices when sorted by some important partial orders, namely the **left star order**, the **core order** and the **star order** (see Section 1 of Article A in Section 2.1).

Remarkably, we have Theorem 2.0.0.1 for the left star order (i.e. Theorem 3.4 of Article A in Section 2.1).

Theorem 2.0.0.1. *If n is any positive integer and B is any complex square matrix of order n, then the interval $[O, B]$ with respect to the left-star order is an*

orthomodular lattice of finite height; which in addition is non-distributive if the rank of B exceeds two.

For the core order, we have Theorem 2.0.0.2 (i.e. Theorem 3.14 of Article A in 2.1).

Theorem 2.0.0.2. *If n is any positive integer and B is any non-zero complex square matrix of order n, then the interval $[O, B]$ with respect to the core order is a sublattice of the interval $[O, B]$ with respect to the left-star order.*

And for the star order, we have Theorem 2.0.0.3 (i.e. Corollary 3.11 of Article A in Section 2.1).

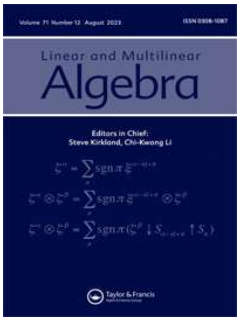
Theorem 2.0.0.3. *If n and r are any two positive integers such that $r \leq n$, and B is any non-zero complex square matrix of order n and rank r, then the following statements are equivalent.*

1. *The interval $[O, B]$ with respect to the star order is a finite lattice.*
2. *The interval $[O, B]$ with respect to the star order is a Boolean algebra of 2^r elements.*
3. *The positive singular values of B are pairwise distinct.*

We now reproduce Article A, and then continue by showing some related work in logic.

2.1 Article A

This is an Accepted Manuscript of an article published by Taylor & Francis in Linear and Multilinear Algebra on 26/Dec/2022, available online: https://www.tandfonline.com/doi/full/10.1080/03081087.2022.2160948.



Linear and Multilinear Algebra

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/glma20

Lattice properties of partial orders for complex matrices via orthogonal projectors

C. R. Cimadamore, L. A. Rueda, L. Sauras-Altuzarra & N. Thome

To cite this article: C. R. Cimadamore, L. A. Rueda, L. Sauras-Altuzarra & N. Thome (2022): Lattice properties of partial orders for complex matrices via orthogonal projectors, Linear and Multilinear Algebra, DOI: 10.1080/03081087.2022.2160948

To link to this article: https://doi.org/10.1080/03081087.2022.2160948

Published online: 26 Dec 2022.

LINEAR AND MULTILINEAR ALGEBRA
https://doi.org/10.1080/03081087.2022.2160948

Taylor & Francis
Taylor & Francis Group

Lattice properties of partial orders for complex matrices via orthogonal projectors

C. R. Cimadamore[a,b], L. A. Rueda[a,b], L. Sauras-Altuzarra[c] and N. Thome[d]

[a]Departamento de Matemática, Universidad Nacional del Sur (UNS), Bahía Blanca, Argentina; [b]Instituto de Matemática (INMABB), Universidad Nacional del Sur (UNS)-CONICET, Bahía Blanca, Argentina; [c]Institut für Diskrete Mathematik und Geometrie, TU Wien, Vienna, Austria; [d]Instituto Universitario de Matemática Multidisciplinar, Universitat Politècnica de València, Valencia, Spain

ABSTRACT

This paper deals with left star, star, and core partial orders for complex matrices. For each partial order, we present an order-isomorphism between the down-set of a fixed matrix B and a certain set (depending on the partial order) of orthogonal projectors whose matrix sizes can be considerably smaller than that of the matrix B. We study the lattice structure and we give properties of the down-sets. We prove that the down-set of B ordered by the core partial order and by the star partial order are sublattices of the down-set ordered by the left star partial order. We analize the existence of supremum and infimum of two given matrices and we give characterizations of these operations (whenever they exist). Some of the results given in the paper are already known in the literature but we present a different proof based on the previously established order-isomorphism.

ARTICLE HISTORY
Received 8 June 2022
Accepted 6 October 2022

COMMUNICATED BY
J. F. Queiró

KEYWORDS
Hartwig–Spindelböck factorization; left star partial order; star partial order; core partial order; lattice structure

AMS SUBJECT CLASSIFICATIONS
15A09 (primary); 06A06 (secondary)

1. Introduction and preliminaries

The set of complex $m \times n$ matrices is denoted by $\mathbb{C}^{m\times n}$. The conjugate transpose, range, and rank of $A \in \mathbb{C}^{m\times n}$ are denoted by A^*, $\mathcal{R}(A)$, and $\mathrm{rk}(A)$, respectively. The identity matrix of order $n \times n$ is denoted by I_n and zero matrices are denoted simply by O.

For each $A \in \mathbb{C}^{m\times n}$, there exists a unique matrix $X \in \mathbb{C}^{n\times m}$ such that AX and XA are Hermitian, $AXA = A$, and $XAX = X$, which is called the Moore-Penrose inverse of A and it is denoted by $A^\dagger$. We denote by $\mathbb{C}^n_1$ the set of all $n \times n$ complex matrices that have index at most 1, that is, $\mathrm{rk}(A^2) = \mathrm{rk}(A)$. If $A \in \mathbb{C}^n_1$ then there exists a unique matrix $X \in \mathbb{C}^{n\times n}$ that satisfies $AX = AA^\dagger$ and $\mathcal{R}(X) \subseteq \mathcal{R}(A)$, which is called the core inverse of A and it is denoted by $X = A^{\textcircled{\#}}$. For further properties and applications of these inverses we refer the reader to [1–9].

This paper deals with some matrix partial orders. Specifically, with the star and the left star partial orders defined on the set $\mathbb{C}^{n\times n}$ of square complex matrices, and with the core partial order defined on the set $\mathbb{C}^n_1$. The star partial order was introduced by Drazin in [10] and it has been studied since then by numerous authors. The left star partial order was

CONTACT N. Thome njthome@mat.upv.es Instituto Universitario de Matemática Multidisciplinar, Universitat Politècnica de València, Valencia 46022, Spain

introduced by Baksalary and Mitra in [11]. Finally, the core partial order was introduced more recently by Baksalary and Trenkler in [1]. For any $A, B \in \mathbb{C}^{n\times n}$, let us recall that (see, for example, [12–14]):

- the left star partial order is defined by: $A \overset{l*}{\leq} B$ if and only if $A^*A = A^*B$ and $\mathcal{R}(A) \subseteq \mathcal{R}(B)$ (or equivalently, $A^*A = A^*B$ and $A = BB^\dagger A$);
- the star partial order is defined by: $A \overset{*}{\leq} B$ if and only if $A^*A = A^*B$ and $AA^* = BA^*$ (or equivalently, $A^\dagger A = A^\dagger B$ and $AA^\dagger = BA^\dagger$);

and, for any $A, B \in \mathbb{C}^n_1$:

- the core partial order is defined by: $A \overset{\textcircled{\#}}{\leq} B$ if and only if $A^{\textcircled{\#}}A = A^{\textcircled{\#}}B$ and $AA^{\textcircled{\#}} = BA^{\textcircled{\#}}$ (or equivalently, $A^*A = A^*B$ and $BA = A^2$).

For the sake of completeness we recall some basic definitions of structures defined over a partially ordered set that are used throughout the article. Recall that a partially ordered set (poset) $(Q, \leq)$ is a lattice if for every $x, y \in Q$ both the least upper bound (or supremum) $x \vee y$ and the greatest lower bound (or infimum) $x \wedge y$ of $\{x, y\}$ exist. A lattice is said to be bounded if it has a first element 0 and a greatest element 1. Two elements a, b of a bounded lattice are complementary if $a \vee b = 1$ and $a \wedge b = 0$. A complemented lattice is a bounded lattice in which every element has a complement. An orthogonal lattice Q is a bounded lattice with a unary operation $'$ that satisfies that $x \wedge x' = 0$, $x \vee x' = 1$, $(x \vee y)' = x' \wedge y'$, $(x \wedge y)' = x' \vee y'$, $x'' = x$, for all $x, y \in Q$. An orthomodular lattice is an orthogonal lattice that satisfies the law 'if $x \leq y$, then $y = x \vee (y \wedge x')$'. A distributive lattice is a lattice which satisfies either (and hence, as it is easy to see, both) of the distributive laws $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. Finally, a Boolean algebra is a complemented distributive lattice. Every Boolean algebra is an orthogonal lattice but, in general, the converse is not true. We refer the reader to [15] for more information about the different structures defined above.

Let Q and R be two posets. It is said that a map $\phi\colon Q \to R$ is order-preserving if $\phi(x) \leq \phi(y)$ holds in R whenever $x \leq y$ holds in Q. We say that Q and R are (order-)isomorphic if there exists a bijection ϕ from Q to R such that both ϕ and ϕ^{-1} are order-preserving. In that case, ϕ is called an order-isomorphism.

The aim of this paper is to study the down-sets $[O, B]^x = \{A \mid O \overset{x}{\leq} A \overset{x}{\leq} B\}$ for each $x \in \{l*, *, \textcircled{\#}\}$ and a fixed matrix B. If $x = \textcircled{\#}$ then it is required that B and all the matrices in $[O, B]^{\textcircled{\#}}$ have index at most 1 accordingly. The structure and properties of these down-sets were studied by other authors for rectangular matrices and for the wider case of bounded linear Hilbert space operators. For the case of the left star partial order, $[O, B]^{l*}$ was studied by Cırulis in [16] where it was proved that $[O, B]^{l*}$ is a complete orthomodular lattice. Antezana et al. studied in [17] the star partial order on bounded operators on a Hilbert space. In particular, from their results, it can be deduced that $[O, B]^*$ is a lattice. Finally, in [18], Djikić proved that $[O, B]^{\textcircled{\#}}$ is also a lattice.

Our approach to the study of $[O, B]^x$ is different from the authors abovementioned. In this paper, we prove that $[O, B]^x$ is order-isomorphic to a certain ordered set (depending on the partial order we are dealing with) of orthogonal projectors. Our starting point is

the characterization given in [19] of matrices which are below a given matrix B by using a Hartwig-Spindelböck decomposition of B. More precisally, given $B \in \mathbb{C}^{n\times n}$ (or in $\mathbb{C}^n_1$ for $x = \circledast$), where $0 < r = \mathrm{rk}(B)$ and the r positive singular values $\sigma_1, \ldots, \sigma_r$ of B are ordered in decreasing order, we consider a Hartwig-Spindelböck decomposition of B (see [20]) given by

$$B = U \begin{bmatrix} \Sigma K & \Sigma L \\ O & O \end{bmatrix} U^*, \tag{1}$$

where $U \in \mathbb{C}^{n\times n}$ is unitary, $\Sigma = \mathrm{diag}\ (\sigma_1, \ldots, \sigma_r) \in \mathbb{C}^{r\times r}$, and $K \in \mathbb{C}^{r\times r}$ and $L \in \mathbb{C}^{r\times(n-r)}$ satisfy $KK^* + LL^* = I_r$ (note that L is absent when $r = n$). It is worth mentioning that this decomposition always exists but it is not necessarily unique, and that $B \in \mathbb{C}^n_1$ if and only if K is nonsingular. The predecessors of B are characterized as follows.

Theorem 1.1 ([19, Theorems 4, 8, 16]): *Let $B \in \mathbb{C}^{n\times n}$ (or $B \in \mathbb{C}^n_1$ for $x = \circledast$) be a nonzero matrix written as in* (1)*. The following conditions are equivalent.*

(1) *There exists a matrix $A \in \mathbb{C}^{n\times n}$ (where $A \in \mathbb{C}^n_1$ for $x = \circledast$) such that $A \overset{x}{\leq} B$.*
(2) *There exists a unique matrix $T \in \mathbb{C}^{r\times r}$ such that*

$$A = U \begin{bmatrix} T\Sigma K & T\Sigma L \\ O & O \end{bmatrix} U^*, \tag{2}$$

where $T^2 = T = T^*$ and the following conditions hold depending on the partial order:
(a) *no extra condition for the left star partial order,*
(b) *$T\Sigma = \Sigma T$ for the star partial order, and*
(c) *$T\Sigma KT = \Sigma KT$ for the core partial order.*

According to Theorem 1.1, we define the following posets that play a crucial role in this paper.

Definition 1.2: Let $B \in \mathbb{C}^{n\times n}$ (or $B \in \mathbb{C}^n_1$ for $x = \circledast$) be a nonzero matrix written as in (1), let

(a) $\tau^{l*}_{\Sigma,K} = \{T \in \mathbb{C}^{r\times r} \mid T^2 = T = T^*\}$,
(b) $\tau^{*}_{\Sigma,K} = \{T \in \mathbb{C}^{r\times r} \mid T^2 = T = T^* \text{ and } T\,\Sigma = \Sigma\,T\}$, and
(c) $\tau^{\circledast}_{\Sigma,K} = \{T \in \mathbb{C}^{r\times r} \mid T^2 = T = T^* \text{ and } T\,\Sigma\,K\,T = \Sigma\,K\,T\}$,

endowed each one with the natural partial order given by

$$T_1 \leq T_2 \quad \text{if and only if} \quad T_1 = T_1T_2.$$

This last relation will be used indistinctly over any of the aformentioned sets.

It is easy to see that $T_1T_2 = T_1$ implies $T_2T_1 = T_1$ for any $T_1, T_2 \in \tau^x_{\Sigma,K}$. Note that the set $\tau^{l*}_{\Sigma,K}$ is the set of all orthogonal projectors in $\mathbb{C}^{r\times r}$. It is well-known that if T_1 and T_2 are orthogonal projectors in $\mathbb{C}^{r\times r}$ and we consider the partial order $\leq$ defined above then

$(\tau^{l*}_{\Sigma,K}, \leq)$ is an orthomodular lattice (see [21, Propositions 1, 2] and [16]) where, for any $T, T_1, T_2 \in \tau^{l*}_{\Sigma,K}$, we have that

$$T_1 \vee T_2 = (T_1 + T_2)(T_1 + T_2)^\dagger = (T_1 + T_2)^\dagger(T_1 + T_2),$$
$$T_1 \wedge T_2 = 2T_1(T_1 + T_2)^\dagger T_2 = 2T_2(T_1 + T_2)^\dagger T_1,$$

and the complement of T is

$$T' = I_r - T.$$

By Theorem 1.1, for any $x \in \{l*, *, ⓐ\}$, we clearly have a bijection

$$\phi\colon [O, B]^x \to \tau^x_{\Sigma,K}$$

defined by $\phi(A) = T$, for every $A \in [O, B]^x$ and T given as in Theorem 1.1. Furthermore, we prove in Section 2 that ϕ is an order-isomorphism. Taking advantage of this order-isomorphism, we study the ordered structure of $[O, B]^x$ by means of the poset $\tau^x_{\Sigma,K}$. Matrices $T \in \tau^x_{\Sigma,K}$ are orthogonal projectors and, in addition, it can be proved that the Moore-Penrose inverse $T^\dagger$ and the core inverse $T^{ⓒ}$ of T are both equal to T. Moreover, all of them belong to $\mathbb{C}^{r\times r}$ (instead of $\mathbb{C}^{n\times n}$), with $0 < r \leq n$, where r can be considerably smaller than n. So, working with the matrices $T \in \tau^x_{\Sigma,K}$ is easier than using the matrices A and this fact brings significant advantages.

In Section 3 we investigate the lattice properties of $[O, B]^x$. One of our main goals is to show that there exists a relation between $[O, B]^*$, $[O, B]^{l*}$, and $[O, B]^{ⓒ}$. More precisely, based on the order-isomorphism proved in Section 2, we show that $[O, B]^x$, for each x, is a lattice; and that $[O, B]^*$ and $[O, B]^{ⓒ}$ are sublattices of $[O, B]^{l*}$. In addition, we find properties of $[O, B]^x$, for each partial order. We show that $[O, B]^{l*}$ and $[O, B]^*$ are orthomodular lattices whose subchains (that is, a subset for which every pair of elements are comparable) are all finite. We give a necessary and sufficient condition for $[O, B]^{l*}$ to be distributive. We show that if $[O, B]^*$ is distributive then it is a Boolean algebra. Eagambaram et al. showed in [22] that $[O, B]^*$ is a finite lattice if and only if all the positive singular values of B are pairwise distinct. We improve this result by showing that, in that case, not only $[O, B]^*$ is a finite lattice but also a Boolean algebra. Additionally, we derive its cardinality. For the left star and the star partial orders, we prove that if $A_1 \overset{x}{\leq} A_2 \overset{x}{\leq} B$ then $[A_1, A_2]^x$ and $[O, A_2 - A_1]^x$ are order-isomorphic. Assuming that $A_2 - A_1 \overset{ⓒ}{\leq} B$, an analogous result is obtained for the core partial order.

As a last application of the order-isomorphism ϕ, we study the supremum and the infimum of two given matrices in $\mathbb{C}^{n\times n}$ (or in $\mathbb{C}^n_1$ for the core partial order). Xu et al. proved in [23] that there exists the star supremum of A_1 and A_2 if and only if A_1 and A_2 have a common upper bound. Moreover, an explicit representation of the supremum was established (whenever it exists). In [24], Hartwig gave necessary and sufficient conditions for the existence of the star supremum in rings with involution and found an expression for that supremum. Later, Djikić gave in [25] a simple necessary and sufficient condition for the existence of the star supremum for two operators on a Hilbert space. Recently, Djikić proved in [18] a similar result to that by Xu et al., for the core partial order by giving necessary and sufficient conditions for the existence of the core supremum in a Hilbert space. In

Section 4, we use the order-isomorphism ϕ to present a different proof from those given by Hartwig, Xu et al. and Djikić. Our proof is also valid for the left star partial order. In addition, we compute the supremum (whenever it exists) by means of the same expression for the three orders. Finally, we analyse the infimum of two arbitrary matrices. Hartwig and Drazin proved in [21] that the set of matrices endowed with the star partial order is a lower semilattice, i.e. for every pair of matrices A_1 and A_2, there exists $A_1 \wedge A_2$. The set of matrices that have index at most 1 endowed with the core partial order is also a lower semilattice (see [18]). In Section 4, we compute the infimum of two matrices that have a common upper bound by means of the same expression for the three orders. We would like to highlight that the expressions for the infimum and supremum of two matrices in $[O, B]^{l*}$ that we provide are different from those given in [16].

If two matrices B (written as in (1)) and C do not have a common upper bound, we find an expression of the type (2) for the infimum and the conditions that the associated orthogonal projectors must satisfy.

2. Isomorphic representation of down-sets

From now on, x will refer to any of the three partial orders we are dealing with, that is, $x \in \{l*, *, \#\}$. In the case that $x = \#$, without mentioning it explicitly, we will regard the matrices to be in $\mathbb{C}_1^n$.

In this section we state the order-isomorphism between $[O, B]^x$ and $\tau^x_{\Sigma,K}$. In order to do that, for a fixed a Hartwig-Spindelböck decomposition of B, we consider the posets $\tau^x_{\Sigma,K}$ and the bijection

$$\phi\colon [O, B]^x \to \tau^x_{\Sigma,K}$$

defined by $\phi(A) = T$ given in Section 1. Note that if $T \in \tau^x_{\Sigma,K}$ then $T \in \mathbb{C}_1^r$; O is the least element and I_r is the greatest element of $\tau^x_{\Sigma,K}$. More precisely, we should denote ϕ by $\phi_{\Sigma,K}$ because this map depends on matrices Σ and K of the decomposition used to factorize the matrix B. However, to simplify the notation, from now on, we simply denote it by ϕ.

Theorem 2.1: *The posets $[O, B]^x$ and $\tau^x_{\Sigma,K}$ are order-isomorphic. Moreover, the function rank is preserved under the order-isomorphism ϕ.*

Proof: Let us first prove that ϕ is order-preserving. For that, let $A_1 \overset{x}{\leq} A_2 \in [O, B]^x$ both written as in (2), $T_1 = \phi(A_1)$ and $T_2 = \phi(A_2)$. From $A_1^* A_1 = A_1^* A_2$ and taking into account that $T_1^2 = T_1 = T_1^*$, we have that

$$\begin{bmatrix} K^*\Sigma T_1 \Sigma K & K^*\Sigma T_1 \Sigma L \\ L^*\Sigma T_1 \Sigma K & L^*\Sigma T_1 \Sigma L \end{bmatrix} = \begin{bmatrix} K^*\Sigma T_1 T_2 \Sigma K & K^*\Sigma T_1 T_2 \Sigma L \\ L^*\Sigma T_1 T_2 \Sigma K & L^*\Sigma T_1 T_2 \Sigma L \end{bmatrix}.$$

Hence we obtain the following system

$$K^*\Sigma T_1 \Sigma K = K^*\Sigma T_1 T_2 \Sigma K, \tag{3}$$

$$K^*\Sigma T_1 \Sigma L = K^*\Sigma T_1 T_2 \Sigma L, \tag{4}$$

$$L^*\Sigma T_1 \Sigma K = L^*\Sigma T_1 T_2 \Sigma K, \tag{5}$$

$$L^*\Sigma T_1 \Sigma L = L^*\Sigma T_1 T_2 \Sigma L. \tag{6}$$

Post-multiplicating (3) and (4) by K^* and L^*, respectively, and then adding both equations we obtain $K^*\Sigma T_1\Sigma = K^*\Sigma T_1 T_2\Sigma$, since $KK^* + LL^* = I_r$. Consequently,

$$K^*\Sigma T_1 = K^*\Sigma T_1 T_2. \tag{7}$$

Similarly, from (5) and (6) we obtain

$$L^*\Sigma T_1 = L^*\Sigma T_1 T_2. \tag{8}$$

Pre-multiplying (7) and (8) by K and L respectively, and then adding we have $T_1 = T_1T_2$ and this means that $T_1 \leq T_2$.

Let us suppose now that $T_1 \leq T_2$ with $T_1, T_2 \in \tau^x_{\Sigma,K}$. By $T_1 = T_1T_2$ and $T_1^2 = T_1 = T_1^*$, it is straightforward to see that $A_1^*A_1 = A_1^*A_2$. To prove that $A_1 \overset{x}{\leq} A_2$, we consider each partial order separately.

Consider first the star partial order. Then,

$$A_2A_1^* = U\begin{bmatrix} T_2\Sigma K & T_2\Sigma L \\ O & O \end{bmatrix}\begin{bmatrix} K^*\Sigma T_1 & O \\ L^*\Sigma T_1 & O \end{bmatrix}U^* = U\begin{bmatrix} T_2\Sigma^2 T_1 & O \\ O & O \end{bmatrix}U^*.$$

Since both T_1 and T_2 commute with Σ, we have that $T_2\Sigma^2T_1 = \Sigma^2T_2T_1 = \Sigma^2T_1 = \Sigma^2T_1T_1 = T_1\Sigma^2T_1$. Thus, $A_2A_1^* = A_1A_1^*$. Hence, $A_1 \overset{*}{\leq} A_2$.

Consider now $x = l*$. From [19, Lemma 14], we know that $T_2 = T_2\Sigma(T_2\Sigma)^\dagger$ since Σ is nonsingular. Then, $T_1 = T_2T_1 = T_2\Sigma(T_2\Sigma)^\dagger T_1$. From [19, Lemma 3], we also know that $A_2^\dagger = U\begin{bmatrix} K^*(T_2\Sigma)^\dagger & O \\ L^*(T_2\Sigma)^\dagger & O \end{bmatrix}U^*$. Now, taking into account this fact, it is easy to see that $A_2A_2^\dagger A_1 = A_1$. So, $A_1 \overset{l^*}{\leq} A_2$.

Finally, we consider the core partial order. From $\Sigma KT_1 = T_1\Sigma KT_1$ and $T_2T_1 = T_1$ we have

$$T_1\Sigma KT_1\Sigma K = T_2T_1\Sigma KT_1\Sigma K = T_2\Sigma KT_1\Sigma K$$

and

$$T_1\Sigma KT_1\Sigma L = T_2T_1\Sigma KT_1\Sigma L = T_2\Sigma KT_1\Sigma L.$$

Then $A_2A_1 = A_1^2$ follows. So, $A_1 \overset{\#}{\leq} A_2$.

We have proved that $[O, B]^x$ is order-isomorphic to $\tau^x_{\Sigma,K}$, for every x.

In order to see that ϕ preserves the rank function, we observe that if $A \in [O, B]^x$ and $T = \phi(A)$, then

$$\begin{aligned}\operatorname{rk}(A) = \operatorname{rk}(AA^*) &= \operatorname{rk}\left(\begin{bmatrix} T\Sigma K & T\Sigma L \\ O & O \end{bmatrix}\begin{bmatrix} K^*\Sigma T^* & O \\ L^*\Sigma T^* & O \end{bmatrix}\right) = \operatorname{rk}\left(\begin{bmatrix} T\Sigma^2 T^* & O \\ O & O \end{bmatrix}\right) \\ &= \operatorname{rk}\left(\begin{bmatrix} (T\Sigma)(T\Sigma)^* & O \\ O & O \end{bmatrix}\right) = \operatorname{rk}(T\Sigma) = \operatorname{rk}(T) = \operatorname{rk}(\phi(A)).\end{aligned}$$

■

Remark 2.1: By using a Schur's factorization of the matrix ΣK, we have that there exists a unitary matrix V and an upper triangular matrix S such that $\Sigma K = VSV^*$. It can be proved that the sets $\tau^{\#}_{\Sigma,K}$ and $\rho^{\#}_B := \{T \in \mathbb{C}^{r\times r} \mid T = T^2 = T^* \text{ and } TST = ST\}$, ordered by $\leq$, are

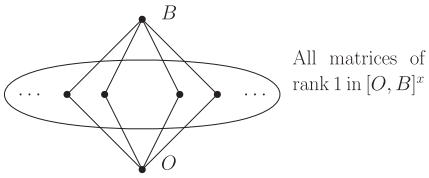


Figure 1. The lattice $[O, B]^x$ with $\mathrm{rk}(B) = 2$.

order-isomorphic by using the map $\varphi : \rho_B^{\circledast} \to \tau_{\Sigma,K}^{\circledast}$ defined by $\varphi(T) = VTV^*$. In practice, examples can be constructed more easily with a such matrix S instead of using ΣK.

Remark 2.2: Assume $A \overset{x}{\leq} B$ and $A \neq B$. It is easy to see that $\mathrm{rk}(A) < \mathrm{rk}(B)$ and so the maximum length of any subchain in $[O, B]^x$ is $\mathrm{rk}(B) + 1$. Moreover, if $\mathrm{rk}(B) = r$ and we consider the projectors $T_s = [t_{ij}] \in \mathbb{C}^{r\times r}$ where

$$t_{ij} = \begin{cases} 1 & \text{if } i = j \text{ and } i \leq s \\ 0 & \text{otherwise} \end{cases},$$

for each $s \in \{1, \ldots, r\}$, it is straightforward to see that $T_s \in \tau_{\Sigma,K}^{l*}$, $T_s \in \tau_{\Sigma,K}^{*}$, and $T_s \in \rho_B^{\circledast}$. Then, we obtain a chain

$$O < T_1 < \ldots < T_r = I_r.$$

with $r + 1$ elements of maximum length.

Lemma 2.2: *Let $B_1, B_2 \in \mathbb{C}^{n\times n}$. If $[O, B_1]^x$ is order-isomorphic to $[O, B_2]^x$ then* $\mathrm{rk}(B_1) = \mathrm{rk}(B_2)$. *Moreover, if* $\mathrm{rk}(B_1) = \mathrm{rk}(B_2)$ *then $[O, B_1]^{l*}$ is order-isomorphic to $[O, B_2]^{l*}$.*

Proof: Let us suppose that $\mathrm{rk}(B_1) < \mathrm{rk}(B_2)$. Then, by using Remark 2.2, we can construct a chain in $[O, B_1]^x$ of length $\mathrm{rk}(B_2) + 1$ and this contradicts the maximum length of a chain in $[O, B_1]^x$. The second statement is immediate from Theorem 2.1. ■

Remark 2.3: For each $x \in \{l*, *, \circledast\}$:

(a) if $\mathrm{rk}(B) = 1$, then $\tau_{\Sigma,K}^x = \{O, I_1\}$. Hence, $[O, B]^x$ is a chain with two elements.
(b) if $\mathrm{rk}(B) = 2$, then $\mathrm{rk}(T) = 1$ for each $T \in \tau_{\Sigma,K}^x \setminus \{O, I_2\}$; so every distinct $T_1, T_2 \in \tau_{\Sigma,K}^x \setminus \{O, I_2\}$ are incomparable and thus $[O, B]^x$ has the aspect presented in Figure 1.

3. Lattice structure of $[O, B]^x$

In this section we investigate the lattice structure of $[O, B]^x$ for each x by using the order-isomorphism ϕ. We prove that $[O, B]^*$ and $[O, B]^{\circledast}$ are sublattices of $[O, B]^{l*}$. For each x, we analyse the structure of $[O, B]^x$. We show that $[O, B]^{l*}$ and $[O, B]^*$ are orthomodular lattices whose subchains are all finite. In addition, we give a necessary and sufficient condition for $[O, B]^{l*}$ to be distributive. We also state that if $[O, B]^*$ is distributive then it is a Boolean

algebra. Finally, we give necessary and sufficient conditions for $[O, B]^*$ to be a finite Boolean algebra.

For the left star and the star partial order, we prove that if $A_1 \overset{x}{\leq} A_2 \overset{x}{\leq} B$ then $[A_1, A_2]^x$ and $[O, A_2 - A_1]^x$ are order-isomorphic. An analogous result is obtained for the core partial order, provided that $A_2 - A_1 \overset{\#}{\leq} B$ holds.

We start giving the infimum and the supremum of two matrices in the segment $[O, B]^x$ for the case in which their associated orthogonal projectors commute.

Proposition 3.1: *Let $T_1, T_2 \in \tau^x_{\Sigma,K}$ such that $T_1T_2 = T_2T_1$. Then $T_1 \wedge T_2 = T_1T_2$ and $T_1 \vee T_2 = T_1 + T_2 - T_1T_2$.*

Proof: It is clear that $(T_1T_2)^2 = T_1T_2 = (T_1T_2)^*$ and it is well-known that T_1T_2 is the infimum of T_1 and T_2 in $\tau^{l*}_{\Sigma,K}$ (see [16]). In addition, if $x = *$, then $(T_1T_2)\Sigma = T_1\Sigma T_2 = \Sigma(T_1T_2)$; and if $x = \#$, then $(T_1T_2)\Sigma K(T_1T_2) = T_1(T_2\Sigma KT_2)T_1 = T_1(\Sigma KT_2)T_1 = (T_1\Sigma KT_1)T_2 = \Sigma K(T_1T_2)$. So, $T_1 \wedge T_2 = T_1T_2$ in $\tau^x_{\Sigma,K}$ for all x.

It is also known that if T_1 and T_2 commute then $T_1 \vee T_2 = T_1 + T_2 - T_1T_2 \in \tau^{l*}_{\Sigma,K}$ (see [16]). In addition, if $x = *$, then $(T_1 + T_2 - T_1T_2)\Sigma = \Sigma(T_1 + T_2 - T_1T_2)$; and if $x = \#$, then $(T_1 + T_2 - T_1T_2)\Sigma K(T_1 + T_2 - T_1T_2) = T_1\Sigma KT_1 + T_1\Sigma KT_2 - T_1\Sigma KT_1T_2 + T_2\Sigma KT_1 + T_2\Sigma KT_2 - T_2\Sigma KT_1T_2 - T_1T_2\Sigma KT_1 - T_1T_2\Sigma KT_2 + T_1T_2\Sigma KT_1T_2 = \Sigma KT_1 + T_1\Sigma KT_2 - \Sigma KT_1T_2 + T_2\Sigma KT_1 + \Sigma KT_2 - \Sigma KT_2T_1 - T_2\Sigma KT_1 - T_1\Sigma KT_2 + \Sigma KT_1T_2 = \Sigma KT_1 + \Sigma KT_2 - \Sigma KT_1T_2 = \Sigma K(T_1 + T_2 - T_1T_2)$. Therefore, $T_1 + T_2 - T_1T_2 \in \tau^x_{\Sigma,K}$ for every x. ■

As an immediate consequence of the above result and the fact that ϕ is an order-isomorphism we have the following result.

Corollary 3.2: *Let $A_1, A_2 \in [O, B]^x$ be written as in* (2) *such that $T_1T_2 = T_2T_1$, where $T_i = \phi(A_i)$ for every $i \in \{1, 2\}$. Then:*

(a) $A_1 \wedge A_2 = U \begin{bmatrix} T_1T_2\Sigma K & T_1T_2\Sigma L \\ O & O \end{bmatrix} U^*$ *and*
(b) $A_1 \vee A_2 = A_1 + A_2 - A_1 \wedge A_2$.

We now investigate $[O, B]^x$ separately for each order.

3.1. Left star partial order

In this section we show that $[O, B]^{l*}$ is an orthomodular lattice of finite height and nondistributive provided that $\mathrm{rk}(B) \geq 2$. It is worth mentioning that the fact that $[O, B]^{l*}$ is an orthomodular lattice was proved by Cırulis in [16] for the more general case of a bounded operator X over a complex Hilbert space H, by setting an isomorphism between every down-set $[O, X]^{l*}$ of the set of all bounded linear operators over H and the down-set $[O, P_X]^{l*}$ of projectors where P_X is the projector onto the closure of the range $\mathcal{R}(X)$ ($P_X = XX^\dagger$ for $X, P_X \in \mathbb{C}^{n\times n}$). Our proof is based on the order-isomorphism ϕ and the advantage of this technique is that allows us to work with orthogonal projectors whose sizes can be considerably smaller than those of matrix B itself.

Our first objective is to show that $[O,B]^{l*}$ is a nondistributive lattice if $\mathrm{rk}(B) \geq 2$. In order to do that, we have to observe that $\tau^{l*}_{\Sigma,K}$ is exactly the set of all $r \times r$ orthogonal projectors. So, we only need to find an example where the distributive property does not hold and this example will serve in general.

Example 3.3: Let B be any matrix in $\mathbb{C}^{n\times n}$ such that $\mathrm{rk}(B) \geq 2$ and $A_1, A_2, A_3 \in [O,B]^{l*}$ such that $T_i = \phi(A_i) = \left[\begin{smallmatrix} X_i & O \\ O & O \end{smallmatrix}\right] \in \tau^{l*}_{\Sigma,K}$ for every $i \in \{1,2,3\}$, where $X_1 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, $X_2 = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, and $X_3 = \left[\begin{smallmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{smallmatrix}\right]$. Let us see that $A_3 \wedge (A_1 \vee A_2) \neq (A_3 \wedge A_1) \vee (A_3 \wedge A_2)$. Indeed, by Proposition 3.1, $T_3 \wedge (T_1 \vee T_2) = T_3(T_1 + T_2 - T_1T_2) = T_3$. On the other hand, by Remark 2.3, $(T_3 \wedge T_1) \vee (T_3 \wedge T_2) = O \vee O = O$, since $\mathrm{rk}(T_i) = 1$, for each $i \in \{1,2,3\}$.

Since $\tau^{l*}_{\Sigma,K}$ is an orthomodular lattice (see [16]), by Theorem 2.1, $[O,B]^{l*}$ is an orthomodular lattice too and, by considering a rank argument, it is clear that all its subchains are finite. In this case, it is said that the lattice has finite height. We summarize these reasonings in the following theorem.

Theorem 3.4: *If $B \in \mathbb{C}^{n\times n}$ then $[O,B]^{l*}$ is an orthomodular lattice of finite height. In addition, if $\mathrm{rk}(B) \geq 2$ then $[O,B]^{l*}$ is nondistributive.*

Remark 3.1: Let $A_1, A_2 \in [O,B]^{l*}$ be written as in (2), where $T_i = \phi(A_i)$ for each $i \in \{1,2\}$. Then:

(a) $A_1 \wedge A_2 = U \left[\begin{smallmatrix} (T_1\wedge T_2)\Sigma K & (T_1\wedge T_2)\Sigma L \\ O & O \end{smallmatrix}\right] U^*$ and
(b) $A_1 \vee A_2 = U \left[\begin{smallmatrix} (T_1\vee T_2)\Sigma K & (T_1\vee T_2)\Sigma L \\ O & O \end{smallmatrix}\right] U^*$.

Remark 3.2: If $\mathrm{rk}(B) \geq 2$ then $[O,B]^{l*}$ is an infinite lattice. For example, if $X = \left[\begin{smallmatrix} a & b \\ \bar{b} & 1-a \end{smallmatrix}\right]$, with a in the real interval $[0,1]$, $b \in \mathbb{C}$, and $|b|^2 = a - a^2$, then $T = \left[\begin{smallmatrix} X & O \\ O & O \end{smallmatrix}\right] \in \tau^{l*}_{\Sigma,K}$.

Note also that if A is any matrix such that $A \overset{l*}{\leq} B$ and $\mathrm{rk}(A) = 2$ then, in general, $[O,A]^{l*}$ is an infinite lattice order-isomorphic to the one given in Figure 1.

Remark 3.3: Let $P, T, Q \in \mathbb{C}^{r\times r}$ be orthogonal projectors such that $P \leq T$ and $TQ = O$. It is easy to see that $PQ = O$.

Lemma 3.5: *Let $A, A_1, A_2, B \in \mathbb{C}^{n\times n}$. If $A_1 \overset{l*}{\leq} A_2 \overset{l*}{\leq} B$ then $[O, A_2 - A_1]^{l*}$ and $[A_1, A_2]^{l*}$ are order-isomorphic. In particular, if $A \overset{l*}{\leq} B$ then $[O, B - A]^{l*}$ and $[A, B]^{l*}$ are order-isomorphic.*

Proof: Assume that $A_1 \overset{l*}{\leq} A_2 \overset{l*}{\leq} B$ and set T_1, T_2 such that $\phi(A_i) = T_i$, for each $i \in \{1,2\}$. If P satisfies $P^2 = P^* = P \leq T_2 - T_1$, by $(T_2 - T_1)T_1 = O$ and Remark 3.3, we have that $PT_1 = O$. Moreover, $T_1P = (P^*T_1^*)^* = (PT_1)^* = O$. It is easy to see that $P + T_1$ is idempotent, Hermitian, and $T_1 \leq P + T_1$. Now, again from $P \leq T_2 - T_1$, we have that $P = P(T_2 - T_1) = PT_2$ and then $(P + T_1)T_2 = PT_2 + T_1T_2 = P + T_1$; i.e.

$P + T_1 \leq T_2$. Thus, the map $\varphi\colon [O, T_2 - T_1] \to [T_1, T_2]$ given by $\varphi(P) = P + T_1$ is well-defined. Let us prove that φ is an order-isomorphism. Indeed, let $Q \in [T_1, T_2]$ and $P = Q - T_1$. Since $P(T_2 - T_1) = (Q - T_1)(T_2 - T_1) = QT_2 - T_1T_2 - QT_1 + T_1^2 = Q - T_1 - T_1 + T_1 = Q - T_1 = P$, we get $P \in [O, T_2 - T_1]$ and $\varphi(P) = Q$. Thus, φ is surjective. Let $P_1, P_2 \in [O, T_2 - T_1]$. Since $T_1P_2 = O$ and $P_1T_1 = O$, we have $\varphi(P_1) \leq \varphi(P_2)$ if and only if $(P_1 + T_1)(P_2 + T_1) = P_1 + T_1$, that is equivalent to $P_1P_2 + T_1P_2 + P_1T_1 + T_1^2 = P_1 + T_1$, which simplifies to $P_1P_2 = P_1$, that is, $P_1 \leq P_2$. Then, φ is an order-isomorphism.

The second statement follows by setting $A_1 = A$ and $A_2 = B$. ■

Lemma 3.5 allows us to realize the complexity of the down-set $[O, B]^{l*}$ when $\mathrm{rk}(B) \geq 2$. For instance, if we choose a matrix A such that $\mathrm{rk}(B - A) = 2$ then the Figure 1 will appear repeated at the top (down-set $[A, B]^{l*}$) and at the bottom (down-set $[O, B - A]^{l*}$) of the Hasse diagram of the whole down-set $[O, B]^{l*}$.

3.2. Star partial order

We now need the following technical result.

Lemma 3.6 ([3, Theorem 1.4.2]): *Let $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times p}$. Then $(AB)^\dagger = B^\dagger A^\dagger$ if and only if $A^\dagger ABB^*A^* = BB^*A^*$ and $BB^\dagger A^*AB = A^*AB$.*

Theorem 3.7: *If $B \in \mathbb{C}^{n\times n}$ then $[O, B]^*$ is a sublattice of $[O, B]^{l*}$.*

Proof: It is immediate that $\tau^*_{\Sigma,K} \subseteq \tau^{l*}_{\Sigma,K}$. Then $[O, B]^* \subseteq [O, B]^{l*}$.

Let $A_1, A_2 \in [O, B]^*$. We know that $A_1 \vee A_2$ and $A_1 \wedge A_2$ exist in $[O, B]^{l*}$. Now we prove that $A_1 \vee A_2, A_1 \wedge A_2 \in [O, B]^*$. By Theorem 3.4, $\phi(A_1) \vee \phi(A_2)$ and $\phi(A_1) \wedge \phi(A_2)$ exist in $\tau^{l*}_{\Sigma,K}$. So, we only need to see that $(\phi(A_1) \vee \phi(A_2))\Sigma = \Sigma(\phi(A_1) \vee \phi(A_2))$ and $(\phi(A_1) \wedge \phi(A_2))\Sigma = \Sigma(\phi(A_1) \wedge \phi(A_2))$.

Let $T_1 = \phi(A_1)$ and $T_2 = \phi(A_2)$. Taking into account that $\Sigma^\dagger = \Sigma^{-1}$ and $\Sigma^* = \Sigma$, the equalities $\Sigma^\dagger\Sigma(T_1 + T_2)(T_1 + T_2)^*\Sigma^* = (T_1 + T_2)(T_1 + T_2)^*\Sigma^*$, and $(T_1 + T_2)(T_1 + T_2)^\dagger\Sigma^*\Sigma(T_1 + T_2) = (T_1 + T_2)(T_1 + T_2)^\dagger(T_1 + T_2)\Sigma\Sigma = (T_1 + T_2)\Sigma\Sigma = \Sigma^*\Sigma(T_1 + T_2)$ imply, by Lemma 3.6, that

$$(\Sigma(T_1 + T_2))^\dagger = (T_1 + T_2)^\dagger\Sigma^{-1}. \tag{9}$$

Now, the equalities

$$\begin{aligned}
&(\Sigma(T_1 + T_2))^\dagger\Sigma(T_1 + T_2)\Sigma^{-1}(\Sigma^{-1})^*(\Sigma(T_1 + T_2))^* \\
&\quad = (T_1 + T_2)^\dagger\Sigma^{-1}\Sigma(T_1 + T_2)\Sigma^{-1}(T_1 + T_2)^* \\
&\quad = ((T_1 + T_2)^\dagger(T_1 + T_2))^*(T_1 + T_2)^*\Sigma^{-1} \\
&\quad = ((T_1 + T_2)(T_1 + T_2)^\dagger(T_1 + T_2))^*\Sigma^{-1} = (T_1 + T_2)\Sigma^{-1} \\
&\quad = \Sigma^{-1}(\Sigma^{-1})^*(\Sigma(T_1 + T_2))^*
\end{aligned}$$

and

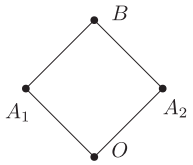


Figure 2. The Boolean algebra $[O, B]^*$.

$$\Sigma^{-1}(\Sigma^{-1})^\dagger(\Sigma(T_1+T_2))^*\Sigma(T_1+T_2)\Sigma^{-1} = \Sigma^{-1}\Sigma(\Sigma(T_1+T_2))^*\Sigma(T_1+T_2)\Sigma^{-1}$$
$$= (\Sigma(T_1+T_2))^*\Sigma(T_1+T_2)\Sigma^{-1},$$

again by Lemma 3.6 and (9), imply that

$$((\Sigma(T_1+T_2))\Sigma^{-1})^\dagger = \Sigma(T_1+T_2)^\dagger\Sigma^{-1}.$$

Finally, from $(T_1+T_2)^\dagger = (T_1\Sigma\Sigma^{-1}+T_2\Sigma\Sigma^{-1})^\dagger = (\Sigma T_1\Sigma^{-1}+\Sigma T_2\Sigma^{-1})^\dagger = (\Sigma(T_1+T_2)\Sigma^{-1})^\dagger = \Sigma(T_1+T_2)^\dagger\Sigma^{-1}$, we get that

$$(T_1\wedge T_2)\Sigma = 2T_1(T_1+T_2)^\dagger T_2\Sigma = 2T_1\Sigma(T_1+T_2)^\dagger\Sigma^{-1}T_2\Sigma$$
$$= 2\Sigma T_1(T_1+T_2)^\dagger\Sigma^{-1}\Sigma T_2 = \Sigma 2T_1(T_1+T_2)^\dagger T_2 = \Sigma(T_1\wedge T_2)$$

and

$$(T_1\vee T_2)\Sigma = (T_1+T_2)(T_1+T_2)^\dagger\Sigma = (T_1+T_2)\Sigma(T_1+T_2)^\dagger\Sigma^{-1}\Sigma$$
$$= \Sigma(T_1+T_2)(T_1+T_2)^\dagger = \Sigma(T_1\vee T_2).$$

Hence, $[O, B]^*$ is a sublattice of $[O, B]^{l*}$. ■

Proposition 3.8: *The lattice $[O, B]^*$ is an orthomodular lattice of finite height. Moreover, if $[O, B]^*$ is distributive then $[O, B]^*$ is a Boolean algebra.*

Proof: Let $T \in \tau^*_{\Sigma,K}$. Let us see that $I_r - T \in \tau^*_{\Sigma,K}$. Indeed, it is clear that $(I_r - T)^2 = I_r - T = (I_r - T)^*$. Since $T\Sigma = \Sigma T$, then $(I_r - T)\Sigma = \Sigma(I_r - T)$. So $I_r - T \in \tau^*_{\Sigma,K}$. Thus, $\tau^*_{\Sigma,K}$ is closed under the unary operation of complementation of $\tau^{l*}_{\Sigma,K}$. Taking into account Theorems 3.4 and 3.7, we have that $\tau^*_{\Sigma,K}$ is an orthomodular lattice.

If $\tau^*_{\Sigma,K}$ is a distributive lattice then $\tau^*_{\Sigma,K}$ is a Boolean algebra. So, $[O, B]^*$ is a Boolean algebra. ■

The next example illustrates the existence of matrices B such that $[O, B]^*$ are distributive lattices.

Example 3.9: Let us consider the matrix $B = \left[\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right]$. Some computations give $\tau^*_{\Sigma,K} = \{O, \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right], I_2\}$. The Hasse diagram associated to $[O, B]^*$ is given in Figure 2.

Eagambaram et al. showed in [22] that $[O, B]^*$ is a finite lattice if and only if all the positive singular values of B are pairwise distinct. The next theorem improves this result

by showing that, in that case, $[O, B]^*$ is not only a finite lattice but also a Boolean algebra. Additionally, we find its cardinality.

Theorem 3.10: *Let $B \in \mathbb{C}^{n\times n}\backslash\{O\}$. The lattice $[O, B]^*$ is a Boolean algebra if and only if all the positive singular values of B are pairwise distinct.*

Proof: Let $\sigma_1, \sigma_2, \ldots, \sigma_r \in \mathbb{R}^+$ be pairwise distinct and $\Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_r)$. If $T \in \tau^*_{\Sigma,K}$ then $T = T^2 = T^*$ and $T\Sigma = \Sigma T$. Thus, $T = \operatorname{diag}(a_1, \ldots, a_r)$, where $a_j \in \{0, 1\}$. Let $A_1, A_2, A_3 \in [O, B]^*$ and $T_i = \phi(A_i)$, for each $i \in \{1, 2, 3\}$. Then $T_i = \operatorname{diag}(a_{i1}, \ldots, a_{ir})$, where $a_{ij} \in \{0, 1\}$ for all i. Note that $T_iT_j = T_jT_i$, for any i, j, and all the supremum and infimum obtained from these projectors also commute with T_i, for all i. Then, by Proposition 3.1, we have that $T_1 \wedge (T_2 \vee T_3) = T_1(T_2 + T_3 - T_2T_3) = T_1T_2 + T_1T_3 - T_1T_2T_3 = (T_1 \wedge T_2) \vee (T_1 \wedge T_3)$. Thus, $[O, B]^*$ is a distributive lattice and, by Proposition 3.8, it is Boolean algebra.

Conversely, suppose that $\Sigma = \operatorname{diag}(\sigma_1 I_{r_1}, \ldots, \sigma_t I_{r_t})$ with $r_i > 1$ for some $i \in \{1, \ldots, t\}$. Let us consider the matrices X_1, X_2, X_3 constructed in Example 3.3 and $Y_j = \begin{bmatrix} X_j & O \\ O & O \end{bmatrix} \in \mathbb{C}^{r_i\times r_i}$, for every $j \in \{1, 2, 3\}$. Now, take $T_j \in \mathbb{C}^{r\times r}$ partitioned in blocks like the matrix Σ where the block (i, i) is the matrix Y_j and the rest is completed with null matrices of the corresponding order. Now, we can choose $A_1, A_2, A_3 \in [O, B]^*$ such that $T_j = \phi(A_j)$. Then $A_3 \wedge (A_1 \vee A_2) \neq (A_3 \wedge A_1) \vee (A_3 \wedge A_2)$. Hence, $[O, B]^*$ is nondistributive. ■

Corollary 3.11: *Let $B \in \mathbb{C}^{n\times n}$ be a nonzero matrix of rank r. The following conditions are equivalent.*

(a) $[O, B]^*$ *is a finite lattice.*
(b) *All positive singular values of B are pairwise distinct.*
(c) $[O, B]^*$ *is a Boolean algebra with 2^r elements.*

Corollary 3.12: *If $A, B \in \mathbb{C}^{n\times n}$ are nonzero matrices such that all positive singular values of B are pairwise distinct and $A \in [O, B]^*\backslash\{O\}$, then all the positive singular values of A are pairwise distinct as well.*

Proof: It follows from Theorem 3.10, because every down-set of a Boolean algebra is a Boolean algebra too. ■

Remark 3.4: (a) If $\Sigma = \sigma I_r$ for some $\sigma \in \mathbb{R}^+$ then $\tau^*_{\Sigma,K} = \tau^{l*}_{\Sigma,K}$. If, in addition, $r \geq 2$, then $[O, B]^*$ is an infinite nondistributive lattice by Theorem 3.4 and Remark 3.2.

(b) If $\Sigma = \operatorname{diag}(\sigma_1 I_{r_1}, \ldots, \sigma_t I_{r_t})$, for some $\sigma_1, \ldots, \sigma_t \in \mathbb{R}^+$, then the condition $T \in \tau^*_{\Sigma,K}$ is equivalent to $T = \operatorname{diag}(X_1, \ldots, X_t)$ where $X_i \in \mathbb{C}^{r_i\times r_i}$ and $X_i^2 = X_i = X_i^*$ for every $i \in \{1, \ldots, t\}$.

If $A \overset{*}{\leq} B$, $A_1 \overset{*}{\leq} A_2 \overset{*}{\leq} B$, and we consider the map φ defined in the proof of Lemma 3.5, then we have the following result since $\varphi(P)$ commutes with Σ.

Lemma 3.13: *Let $A, A_1, A_2, B \in \mathbb{C}^{n\times n}$. If $A_1 \overset{*}{\leq} A_2 \overset{*}{\leq} B$ then $[O, A_2 - A_1]^*$ and $[A_1, A_2]^*$ are order-isomorphic. In particular, if $A \overset{*}{\leq} B$ then $[O, B - A]^*$ and $[A, B]^*$ are order-isomorphic.*

3.3. Core partial order

We now investigate the lattice structure of $[O, B]^{\textcircled{\#}}$ for any $B \in \mathbb{C}_1^n$. Once again, we take advantadge of the order-isomorphism ϕ to prove that $[O, B]^{\textcircled{\#}}$ is a sublattice of $[O, B]^{l*}$. Inspired by some examples, we highlight that the behaviour of the core partial order is rather different from the others. For instance, $[O, B]^{\textcircled{\#}}$ is not necessarily an orthogonal lattice (see Example (c)). Moreover, under the natural assumptions $A_1 \overset{\textcircled{\#}}{\leq} A_2 \overset{\textcircled{\#}}{\leq} B$ and $A_2 - A_1 \overset{\textcircled{\#}}{\leq} B$, we demonstrate that $[A_1, A_2]^{\textcircled{\#}}$ and $[O, A_2 - A_1]^{\textcircled{\#}}$ are order-isomorphic.

Theorem 3.14: *If $B \in \mathbb{C}_1^n \backslash \{O\}$ then $[O, B]^{\textcircled{\#}}$ is a sublattice of $[O, B]^{l*}$.*

Proof: It is immediate that $\tau_{\Sigma,K}^{\textcircled{\#}} \subseteq \tau_{\Sigma,K}^{l*}$. Then $[O, B]^{\textcircled{\#}} \subseteq [O, B]^{l*}$.

Let $A_1, A_2 \in [O, B]^{\textcircled{\#}}$. We know that $A_1 \vee A_2$ and $A_1 \wedge A_2$ exist in $[O, B]^{l*}$. Now we prove that $A_1 \vee A_2, A_1 \wedge A_2 \in [O, B]^{\textcircled{\#}}$. By Theorem 3.4, $\phi(A_1) \vee \phi(A_2)$ and $\phi(A_1) \wedge \phi(A_2)$ exist in $\tau_{\Sigma,K}^{l*}$. So, it remains to prove:

(a) $(\phi(A_1) \vee \phi(A_2))\Sigma K(\phi(A_1) \vee \phi(A_2)) = \Sigma K(\phi(A_1) \vee \phi(A_2))$ and
(b) $(\phi(A_1) \wedge \phi(A_2))\Sigma K(\phi(A_1) \wedge \phi(A_2)) = \Sigma K(\phi(A_1) \wedge \phi(A_2))$.

Indeed, let $T_1 = \phi(A_1)$ and $T_2 = \phi(A_2)$.

Replacing the supremum expressions in (a), we have

$$\begin{aligned}
&(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma K (T_1 + T_2)(T_1 + T_2)^\dagger \\
&\quad = ((T_1 + T_2)(T_1 + T_2)^\dagger T_1 \Sigma K T_1 + (T_1 + T_2)(T_1 + T_2)^\dagger T_2 \Sigma K T_2)(T_1 + T_2)^\dagger \\
&\quad = (T_1 \Sigma K T_1 + T_2 \Sigma K T_2)(T_1 + T_2)^\dagger = \Sigma K (T_1 + T_2)(T_1 + T_2)^\dagger.
\end{aligned}$$

So, $(T_1 \vee T_2)\Sigma K(T_1 \vee T_2) = \Sigma K(T_1 \vee T_2)$. Therefore, (a) is proved.

To show (b), notice first that:

$$\begin{aligned}
T_1(T_1 + T_2)^\dagger T_2 \Sigma K T_1 (T_1 + T_2)^\dagger T_2 &= T_1(T_1 + T_2)^\dagger (T_2 \Sigma K T_2)(T_1 + T_2)^\dagger T_1 \\
&= T_1(T_1 + T_2)^\dagger \Sigma K T_1 (T_1 + T_2)^\dagger T_2 \qquad (10)
\end{aligned}$$

and

$$\begin{aligned}
T_1(T_1 + T_2)^\dagger T_2 \Sigma K T_1 (T_1 + T_2)^\dagger T_2 &= T_2(T_1 + T_2)^\dagger (T_1 \Sigma K T_1)(T_1 + T_2)^\dagger T_2 \\
&= T_2(T_1 + T_2)^\dagger \Sigma K T_1 (T_1 + T_2)^\dagger T_2. \qquad (11)
\end{aligned}$$

By adding (10) and (11),

$$2T_1(T_1 + T_2)^\dagger T_2 \Sigma K T_1 (T_1 + T_2)^\dagger T_2 = (T_1 + T_2)(T_1 + T_2)^\dagger \Sigma K T_1 (T_1 + T_2)^\dagger T_2$$

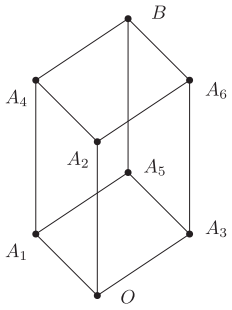


Figure 3. The Boolean algebra $[O, B]^{\circledast}$.

$$= (T_1 + T_2)(T_1 + T_2)^{\dagger} T_1 \Sigma K T_1 (T_1 + T_2)^{\dagger} T_2 = T_1 \Sigma K T_1 (T_1 + T_2)^{\dagger} T_2$$
$$= \Sigma K T_1 (T_1 + T_2)^{\dagger} T_2.$$

Then, $(T_1 \wedge T_2)\Sigma K(T_1 \wedge T_2) = \Sigma K(T_1 \wedge T_2)$. Thus, (b) is proved. ■

Remark 3.5: (a) $[O, B]^{\circledast}$ may be a nondistributive lattice. For example, if $\Sigma K = \sigma I_r$, for some $\sigma \in \mathbb{C}$, then $\tau^{\circledast}_{\Sigma,K} = \tau^{l*}_{\Sigma,K}$.

(b) The next example is constructed by using the set $\rho^{\circledast}_B$ defined in Remark 2.1 and it shows that $[O, B]^{\circledast}$ may be a Boolean algebra. Indeed, consider the matrix

$$B = \begin{bmatrix} \Sigma K & \Sigma L \\ O & O \end{bmatrix} = \begin{bmatrix} 3/2 & -1/2 & 0 & \sqrt{6}/2 \\ -1/2 & 3/2 & 0 & \sqrt{6}/2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

where

$$\Sigma K = \begin{bmatrix} 3/2 & -1/2 & 0 \\ -1/2 & 3/2 & 0 \\ 0 & 0 & -1 \end{bmatrix} = VSV^*, \quad V = \begin{bmatrix} \sqrt{2}/2 & \sqrt{2}/2 & 0 \\ -\sqrt{2}/2 & \sqrt{2}/2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and}$$
$$S = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Some computations lead to $\rho^{\circledast}_B = \{\mathrm{diag}(a_1, a_2, a_3) \mid a_i \in \{0, 1\}\}$ and

$$\tau^{\circledast}_{\Sigma,K} = \{VTV^* \mid T \in \rho^{\circledast}_B\} = \{O, \underbrace{V\mathrm{diag}(1,0,0)V^*}_{\phi(A_1)}, \underbrace{V\mathrm{diag}(0,1,0)V^*}_{\phi(A_2)},$$
$$\underbrace{V\mathrm{diag}(0,0,1)V^*}_{\phi(A_3)}, \underbrace{I_3 - \phi(A_3)}_{\phi(A_4)}, \underbrace{I_3 - \phi(A_2)}_{\phi(A_5)}, \underbrace{I_3 - \phi(A_1)}_{\phi(A_6)}, I_3\}.$$

The associated Hasse diagram of $[O, B]^{\circledast}$ is given in Figure 3.

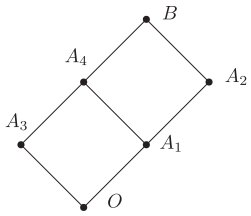


Figure 4. The lattice $[O, B]^{\overset{\#}{}}$.

(1) $[O, B]^{\overset{\#}{}}$ may be a non-Boolean distributive lattice as the following example shows. Consider $B = \begin{bmatrix} \Sigma K & \Sigma L \\ O & O \end{bmatrix}$ where $\Sigma = 2I_3$,

$$K = \begin{bmatrix} 1/2 & -1/2 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad L = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & \sqrt{2}/2 \\ 0 & 0 & 0 \end{bmatrix}.$$

Some computations lead to

$$\tau^{\overset{\#}{}}_{\Sigma,K} = \left\{ O, \underbrace{\mathrm{diag}(1,0,0)}_{\phi(A_1)}, \underbrace{\mathrm{diag}(1,1,0)}_{\phi(A_2)}, \underbrace{\mathrm{diag}(0,0,1)}_{\phi(A_3)}, \underbrace{\mathrm{diag}(1,0,1)}_{\phi(A_4)}, I_3 \right\},$$

and the associated Hasse diagram of $[O, B]^{\overset{\#}{}}$ is given in Figure 4.

As we can observe in the last example, not always $B - A \overset{\#}{\leq} B$ holds whenever $A \overset{\#}{\leq} B$. When $B - A \overset{\#}{\leq} B$, the following result is valid.

Lemma 3.15: *Let $A, A_1, A_2, B \in \mathbb{C}^n_1$. If $A_1 \overset{\#}{\leq} A_2 \overset{\#}{\leq} B$ and $A_2 - A_1 \overset{\#}{\leq} B$ then $[A_1, A_2]^{\overset{\#}{}}$ and $[O, A_2 - A_1]^{\overset{\#}{}}$ are order-isomorphic. In particular, if $A, B - A \overset{\#}{\leq} B$ then $[O, B - A]^{\overset{\#}{}}$ and $[A, B]^{\overset{\#}{}}$ are order-isomorphic.*

Proof: Take φ as in Lemma 3.5. Let us see that φ is surjective. Since $T_1 \leq T_2$ where $T_1, T_2 \in \tau^{\overset{\#}{}}_{\Sigma,K}$, from $(T_2 - T_1)\Sigma K(T_2 - T_1) = \Sigma K(T_2 - T_1)$, we obtain that $\Sigma K T_1 = T_1 \Sigma K T_2$. Now, consider $T_1 \leq Q \leq T_2$. Then $(Q - T_1)\Sigma K(Q - T_1) = Q\Sigma KQ - Q\Sigma KT_1 - T_1\Sigma KQ + T_1\Sigma KT_1$. But $Q\Sigma KT_1 = QT_1\Sigma KT_1 = T_1\Sigma KT_1 = \Sigma KT_1$ and $T_1\Sigma KQ = T_1\Sigma KT_2Q = \Sigma KT_1Q = \Sigma KT_1$. So, $Q\Sigma KQ - Q\Sigma KT_1 - T_1\Sigma KQ + T_1\Sigma KT_1 = \Sigma KQ - \Sigma KT_1 - \Sigma KT_1 + \Sigma KT_1 = \Sigma KQ - \Sigma KT_1 = \Sigma K(Q - T_1)$. The rest of conditions for φ to be an order-isomorphism can be proved as in Lemma 3.5. ■

4. Supremum and infimum of two arbitrary matrices

In this section we first demonstrate that there exists the supremum (for all three partial orders) of two given matrices A_1 and A_2 if and only if A_1 and A_2 have a common upper bound. Our main tools are Theorems 3.4, 3.7, and 3.14. In addition, we find an expression

for this supremum. Secondly, we analyse the infimum of two given matrices. In the case where the matrices have a common upper bound, we obtain an expression for their infimum. If two matrices B and C do not have a common upper bound, we already know that $B \wedge C$ exists for the three partial orders (see [16, 18, 21]). If B is written as in (1) then the infimum can be written as in (2) and we find the conditions that the associated orthogonal projector must satisfy.

Theorem 4.1: *Let $B \in \mathbb{C}^{n\times n}$ be a nonsingular matrix, and $A_1, A_2 \in [O, B]^x$ such that $S = A_1 \vee A_2 \in [O, B]^x$. If $A_1, A_2 \overset{x}{\leq} \widetilde{B}$, for some $\widetilde{B} \in \mathbb{C}^{n\times n}$, then $S \overset{x}{\leq} \widetilde{B}$.*

Proof: Let $T_1 = \phi(A_1)$ and $T_2 = \phi(A_2)$. The fact that B is nonsingular yields that $B = U\Sigma KU^*$ and $A_i = UT_i\Sigma KU^*$, for every $i \in \{1, 2\}$, with $L = O$ and $KK^* = I_n$. By Theorems 3.4, 3.7, or 3.14, depending on the corresponding partial order x, and by Remark 3.1 we know that $S = U(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma KU^*$.

Since $A_i \overset{x}{\leq} \widetilde{B}$, we have that $A_i^* A_i = A_i^* \widetilde{B}$. Then $UK^*\Sigma T_i \Sigma KU^* = UK^*\Sigma T_i U^* \widetilde{B}$ and consequently

$$T_i \Sigma KU^* = T_i U^* \widetilde{B}.$$

Taking into account this last fact,

$$\begin{aligned} S^*S &= UK^*\Sigma(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma KU^* = UK^*\Sigma(T_1 + T_2)^\dagger (T_1 + T_2)\Sigma KU^* \\ &= UK^*\Sigma(T_1 + T_2)^\dagger (T_1 + T_2)U^*\widetilde{B} = S^*\widetilde{B}. \end{aligned} \tag{12}$$

Now we need to study each order separately.

- From $A_i \overset{*}{\leq} \widetilde{B}$ we know that $A_iA_i^* = \widetilde{B}A_i^*$. Then $UT_i\Sigma\Sigma T_iU^* = \widetilde{B}UK^*\Sigma T_iU^*$ and consequently $U\Sigma^2 T_i = \widetilde{B}UK^*\Sigma T_i$. Since $\Sigma T = T\Sigma$, for every $T \in \tau^*_{\Sigma K}$, and $(T_1 + T_2)(T_1 + T_2)^\dagger(T_1 + T_2) = T_1 + T_2$, we have

$$\begin{aligned} SS^* &= U(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma\Sigma(T_1 + T_2)(T_1 + T_2)^\dagger U^* \\ &= U\Sigma^2(T_1 + T_2)(T_1 + T_2)^\dagger U^* = \widetilde{B}UK^*\Sigma(T_1 + T_2)(T_1 + T_2)^\dagger U^* = \widetilde{B}S^* \end{aligned}$$

  and by (12), we get $S \overset{*}{\leq} \widetilde{B}$.
- If $A_i \overset{l*}{\leq} \widetilde{B}$ then $A_i = \widetilde{B}\widetilde{B}^\dagger A_i$. So, $UT_i\Sigma KU^* = \widetilde{B}\widetilde{B}^\dagger UT_i\Sigma KU^*$. Thus, $UT_i = \widetilde{B}\widetilde{B}^\dagger UT_i$. Then

$$S = U(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma KU^* = \widetilde{B}\widetilde{B}^\dagger U(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma KU^* = \widetilde{B}\widetilde{B}^\dagger S$$

  and from (12) we obtain that $S \overset{l*}{\leq} \widetilde{B}$.
- Finally, if $A_i \overset{\oplus}{\leq} \widetilde{B}$ then $A_i^2 = \widetilde{B}A_i$. Thus, $U(T_i\Sigma KT_i)\Sigma KU^* = \widetilde{B}UT_i\Sigma KU^*$ or equivalently $U\Sigma KT_i = \widetilde{B}UT_i$. Taking into account that $T_1 \vee T_2 \in \tau^{\oplus}_{\Sigma,K}$, we have

$$\begin{aligned} S^2 &= U((T_1 + T_2)(T_1 + T_2)^\dagger \Sigma K(T_1 + T_2)(T_1 + T_2)^\dagger)\Sigma KU^* \\ &= U\Sigma K(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma KU^* = \widetilde{B}U(T_1 + T_2)(T_1 + T_2)^\dagger \Sigma KU^* = \widetilde{B}S. \end{aligned}$$

Therefore, by (12), we have that $S \overset{\circledcirc}{\leq} \widetilde{B}$. ■

Let us observe that if $\widetilde{B} \in \mathbb{C}^{n\times n}$ (or $\widetilde{B} \in \mathbb{C}^n_1$ for the core partial order) then there exists a nonsingular matrix B such that $\widetilde{B} \overset{x}{\leq} B$. Indeed:

- If $x = l^*$ and $\widetilde{B} = U \left[\begin{smallmatrix} \Sigma K & \Sigma L \\ O & O \end{smallmatrix}\right] U^*$, then it is enough to consider $B = U \left[\begin{smallmatrix} \Sigma K & \Sigma L \\ O & I_{n-r} \end{smallmatrix}\right] U^*$.
- If $x = *$ then consider a singular value decomposition of $\widetilde{B}$ given by $\widetilde{B} = U \left[\begin{smallmatrix} \Sigma & O \\ O & O \end{smallmatrix}\right] V^*$ and we can choose $B = U \left[\begin{smallmatrix} \Sigma & O \\ O & I_{n-r} \end{smallmatrix}\right] V^*$.
- If $x = \circledcirc$ and we consider again $\widetilde{B} = U \left[\begin{smallmatrix} \Sigma K & \Sigma L \\ O & O \end{smallmatrix}\right] U^*$ then, by Baksalary and Trenkler [1, Lemma 3], we can take $B = U \left[\begin{smallmatrix} \Sigma K & \Sigma L \\ O & I_{n-r} \end{smallmatrix}\right] U^*$.

Proposition 4.2: *Let $A_1, A_2 \in \mathbb{C}^{n\times n}$ (or $A_1, A_2 \in \mathbb{C}^n_1$ for the core partial order). Then, $A_1 \vee A_2$ exists if and only if A_1 and A_2 have a common upper bound. In that case, $A_1 \vee A_2 = (A_1A_1^\dagger + A_2A_2^\dagger)^\dagger(A_1 + A_2)$.*

Proof: The first statement is immediate from Theorem 4.1 taking into account that if A_1 and A_2 have a common upper bound $\widetilde{B}$ then there exists a nonsingular matrix B such that $\widetilde{B} \overset{x}{\leq} B$, for all partial order x. For the second statement, assume that A_1, A_2 have a common upper bound and take B a nonsingular matrix such that $A_1, A_2 \leq B$. Consider a Hartwig-Spindelböck decomposition of B given by $B = U\Sigma KU^*$, where $U, K \in \mathbb{C}^{n\times n}$ are unitary and $\Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_n) \in \mathbb{C}^{n\times n}$. Let T_1 and T_2 be the orthogonal projectors such that $\phi(A_i) = T_i$, for each i, that is $A_i = UT_i\Sigma KU^*$. Then,

$$\begin{aligned} A_1 \vee A_2 &= U(T_1 \vee T_2)\Sigma KU^* = U(T_1 + T_2)^\dagger(T_1 + T_2)\Sigma KU^* \\ &= U(T_1 + T_2)^\dagger U^*U(T_1 + T_2)\Sigma KU^* = (U(T_1 + T_2)U^*)^\dagger U(T_1 + T_2)\Sigma KU^* \\ &= (UT_1U^* + UT_2U^*)^\dagger(A_1 + A_2). \end{aligned}$$

From $KK^* = I_n$, by using the facts that Σ is nonsingular and $T_i\Sigma(T_i\Sigma)^\dagger = T_i$ for each i (see [19, Lemma 14]), we have that

$$UT_iU^* = UT_i\Sigma KU^*UK^*(T_i\Sigma)^\dagger U^* = A_iA_i^\dagger.$$

Hence, $A_1 \vee A_2 = (A_1A_1^\dagger + A_2A_2^\dagger)^\dagger(A_1 + A_2)$. ■

Proposition 4.3: *Let $A_1, A_2 \in \mathbb{C}^{n\times n}$ (or $A_1, A_2 \in \mathbb{C}^n_1$ for the core partial order). If A_1 and A_2 have a common upper bound then $A_1 \wedge A_2 = 2A_1A_1^\dagger(A_1A_1^\dagger + A_2A_2^\dagger)^\dagger A_2$.*

Proof: Proceeding as in the proof of the Proposition 4.2, consider a nonsingular matrix B and a Hartwig-Spindelböck decomposition $B = U\Sigma KU^*$ such that $A_i \overset{x}{\leq} B$ and T_i the orthogonal projectors such that $\phi(A_i) = T_i$. Then, $A_i = UT_i\Sigma KU^*$, $A_iA_i^\dagger = UT_iU^*$, and $(A_1A_1^\dagger + A_2A_2^\dagger)^\dagger = U(T_1 + T_2)^\dagger U^*$. By Theorems 3.4, 3.7 or 3.14, depending on the corresponding partial order x, we have that $A_1 \wedge A_2 = U(T_1 \wedge T_2)\Sigma KU^* = U2T_1(T_1 + T_2)^\dagger T_2\Sigma KU^* = 2UT_1U^*U(T_1 + T_2)^\dagger U^*UT_2\Sigma KU^* = 2A_1A_1^\dagger(A_1A_1^\dagger + A_2A_2^\dagger)^\dagger A_2$. ■

In general, if B and C do not have a common upper bound, we know that there exists $B \wedge C$ for the three partial orders. If B is written as in (1) and we write $C = U \left[\begin{smallmatrix} C_1 & C_2 \\ C_3 & C_4 \end{smallmatrix}\right] U^*$, where $C_1 \in \mathbb{C}^{r\times r}$, then for the infimum $J = B \wedge C$ there exists $T \in \tau^x_{\Sigma,K}$ such that $J = U \left[\begin{smallmatrix} T\Sigma K & T\Sigma L \\ O & O \end{smallmatrix}\right] U^*$. It is straightforward to see that $J^*J = J^*C$ if and only if $T\Sigma K = TC_1$ and $T\Sigma L = TC_2$. Moreover, $\mathcal{R}(J) \subseteq \mathcal{R}(C)$ if and only if $\mathcal{R}(T) \subseteq \mathcal{R}([C_1 \;\; C_2])$. Indeed, $\mathcal{R}(J) = \mathcal{R}(JJ^\dagger) = U\mathcal{R}(\left[\begin{smallmatrix} T\Sigma(T\Sigma)^\dagger \\ O \end{smallmatrix}\right])$. Thus, $\mathcal{R}(J) \subseteq \mathcal{R}(C)$ if and only if $\mathcal{R}\left(\left[\begin{smallmatrix} T\Sigma(T\Sigma)^\dagger \\ O \end{smallmatrix}\right]\right) \subseteq \mathcal{R}\left(\left[\begin{smallmatrix} C_1 & C_2 \\ C_3 & C_4 \end{smallmatrix}\right]\right)$, and this is equivalent to $\mathcal{R}(T) \subseteq \mathcal{R}([C_1 \;\; C_2])$ because Σ is nonsingular and so $\mathcal{R}(T\Sigma(T\Sigma)^\dagger) = \mathcal{R}(T\Sigma) = \mathcal{R}(T)$.

For the star partial order we have that $JJ^* = CJ^*$ if and only if $T\Sigma = (C_1K^* + C_2L^*)T$ and $(C_3K^* + C_4L^*)T = O$.

Finally, for the core partial order we obtain that $CJ = J^2$ if and only if $C_1T = \Sigma KT$ and $C_3T = O$.

We summarize the last reasoning in the following proposition.

Proposition 4.4: *Let $B, C \in \mathbb{C}^{n\times n}$ (or $B, C \in \mathbb{C}^n_1$ for the core partial order) where B is written as in* (1) *and C as above. Then the infimum is given by $B \wedge C = U \left[\begin{smallmatrix} T_m\Sigma K & T_m\Sigma L \\ O & O \end{smallmatrix}\right] U^*$, where T_m is the maximum of the following set.*

(a) *For the left star partial order,*

$$\{T \in \tau^{l*}_{\Sigma,K} | T\Sigma K = TC_1, T\Sigma L = TC_2, \mathcal{R}(T) \subseteq \mathcal{R}([C_1 \;\; C_2])\}.$$

(b) *For the star partial order,*

$$\{T \in \tau^{*}_{\Sigma,K} | T\Sigma K = TC_1, T\Sigma L = TC_2, \\ T\Sigma = (C_1K^* + C_2L^*)T, (C_3K^* + C_4L^*)T = O\}.$$

(c) *For the core partial order,*

$$\{T \in \tau^{\#}_{\Sigma,K} | T\Sigma K = TC_1, T\Sigma L = TC_2, C_1T = \Sigma KT, C_3T = O\}.$$

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The first, the second, and the fourth author were partially supported by Departamento de Matemática, Universidad Nacional del Sur (UNS), Argentina [project number PGI 24/L108]. The third author was partially supported by FWF Austria [project numbers I 4427 and P 31955]. The fourth author was partially supported by Ministerio de Economía y Competitividad of Spain [grant Red de Excelencia, MTM2017-90682-REDT], by Universidad Nacional de Río Cuarto [grant number PPI 083/2020], and by Universidad Nacional de La Pampa, Facultad de Ingeniería, Argentina [grant number Resol. Nro. 135/19].

References

[1] Baksalary OM, Trenkler G. Core inverse of matrices. Linear Multilinear Algebra. 2010;58(5–6): 681–697. DOI:10.1080/03081080902778222

[2] Ben-Israel A, Greville TNE. Generalized inverses: theory and applications. 2nd ed. New York: Springer-Verlag; 2003. (CMS books in mathematics/ouvrages de mathématiques de la SMC; vol. 15).
[3] Campbell SL, Meyer Jr CD, Generalized inverses of linear transformations. New York: Dover Publications Inc.; 1991. Corrected reprint of the 1979 original.
[4] Chen J, Zhu H, Patricio P, et al. Characterizations and representations of core and dual core inverses. Canad Math Bull. 2017;60(2):269–282. DOI:10.4153/CMB-2016-045-7
[5] Kyrchei I. Determinantal representations of the W-weighted Drazin inverse over the quaternion skew field. Appl Math Comput. 2015;264:453–465. DOI:10.1016/j.amc.2015.04.125
[6] Pablos Romo F. On Drazin–Moore–Penrose inverses of finite potent endomorphisms. Linear Multilinear Algebra. 2021;69(4):627–647. DOI:10.1080/03081087.2019.1612834
[7] Wang H, Liu X. Characterizations of the core inverse and the core partial ordering. Linear Multilinear Algebra. 2015;63(9):1829–1836. DOI:10.1080/03081087.2014.975702
[8] Zhou M, Chen J, Stanimirovic PS, et al. Complex varying-parameter Zhang neural networks for computing core and core-EP inverse. Neural Process Lett. 2020;51(2):1299–1329. DOI:10.1007/s11063-019-10141-6
[9] Zhu H, Patrício P. Several types of one-sided partial orders in rings. Rev R Acad Cienc Exactas Fís Nat Ser A Mat RACSAM. 2019;113(4):3177–3184. DOI:10.1007/s13398-019-00685-6
[10] Drazin MP. Natural structures on semigroups with involution. Bull Amer Math Soc. 1978;84(1):139–141. DOI:10.1090/S0002-9904-1978-14442-5
[11] Baksalary JK, Mitra SK. Left-star and right-star partial orderings. Linear Algebra Appl. 1991;149:73–89. DOI:10.1016/0024-3795(91)90326-R
[12] Cvetković-Ilić DS, Mosić D, Wei Y. Partial orders on $\mathcal{B}(\mathcal{H})$. Linear Algebra Appl. 2015;481:115–130. DOI:10.1016/j.laa.2015.04.025
[13] Manjunatha Prasad K, Mohana KS, Sheela YS. Matrix partial orders associated with space preorder. In: Combinatorial matrix theory and generalized inverses of matrices. New Delhi: Springer; 2013. p. 195–226.
[14] Mitra SK, Bhimasankaram P, Malik SB. Matrix partial orders, shorted operators and applications. Hackensack (NJ): World Scientific Publishing Co. Pte. Ltd.; 2010. (Series in algebra; vol. 10).
[15] Burris S, Sankappanavar HP. A course in universal algebra. New York-Berlin: Springer-Verlag; 1981. (Graduate texts in mathematics; vol. 78).
[16] C̄irulis J. One-sided star partial orders for bounded linear operators. Oper Matrices. 2015;9(4):891–905. DOI:10.7153/oam-09-52
[17] Antezana J, Cano C, Mosconi I, et al. A note on the star order in Hilbert spaces. Linear Multilinear Algebra. 2010;58(7–8):1037–1051. DOI:10.1080/03081080903227104
[18] Djikić MS. Lattice properties of the core-partial order. Banach J Math Anal. 2017;11(2):398–415. DOI:10.1215/17358787-0000010X
[19] Malik SB, Rueda L, Thome N. Further properties on the core partial order and other matrix partial orders. Linear Multilinear Algebra. 2014;62(12):1629–1648. DOI:10.1080/03081087.2013.839676
[20] Hartwig RE, Spindelböck K. Matrices for which A^* and $A^\dagger$ commute. Linear Multilinear Algebra. 1983;14(3):241–256. DOI:10.1080/03081088308817561
[21] Hartwig RE, Drazin MP. Lattice properties of the $*$-order for complex matrices. J Math Anal Appl. 1982;86(2):359–378. DOI:10.1016/0022-247X(82)90228-1
[22] Eagambaram N, Manjunatha Prasad K, Mohana KS. Column space decomposition and partial order on matrices. Electron J Linear Algebra. 2013;26:795–815. DOI:10.13001/1081-3810.1688
[23] Xu XM, Du HK, Fang X, et al. The supremum of linear operators for the $*$-order. Linear Algebra Appl. 2010;433(11–12):2198–2207. DOI:10.1016/j.laa.2010.07.026
[24] Hartwig RE. Pseudolattice properties of the star-orthogonal partial ordering for star-regular rings. Proc Amer Math Soc. 1979;77(3):299–303. DOI:10.2307/2042174
[25] Djikić MS. Properties of the star supremum for arbitrary Hilbert space operators. J Math Anal Appl. 2016;441(1):446–461. DOI:10.1016/j.jmaa.2016.04.020

2.2 Related work

We now show some work which goes in the opposition direction, by bringing algebraic notions (or, more specifically, number-theoretic notions) to logic.

2.2.1 An ultrafinitist version of Peano arithmetic

Let k be any integer exceeding one. The following joint work with Grigorii Stepanov presents an ultrafinitist version of Peano arithmetic which is obtained by modifying its proper axioms: the k-th **modular arithmetic**, which is denoted by PA_k and defined in Table 2.1 (note that $S^i(0)$ denotes the i-th iteration of the function letter S to the constant 0 and the notation $\psi(z)$, where ψ is any formula and z any variable, indicates that z occurs free in ψ) (the propositional logical axioms, the equality axioms and the proper axioms of Peano arithmetic can be found in Hamilton [7, Section 4.1, Section 5.2 and Section 5.4]; and the first-order logical axioms can be found in Mendelson [13, Subsection 2.3.1]).

Note that the theories PA and PA_k share the same **language** (viz., relation letters, function letters and constants).

Lemma 2.2.1.1. *Given any formula $\phi(x)$, PA_k proves $\forall x\ \phi(x)$ if and only if PA_k proves $[\phi(0) \wedge \phi(S(0)) \wedge \ldots \wedge \phi(S^{k-1}(0))]$.*

Proof. The direct implication is immediate. For the converse implication, note that the logical axioms, Axiom M2 and the rule $\forall x\ \forall y\ [x = y \Rightarrow [\phi(x) \Leftrightarrow \phi(y)]]$ yield that PA_k proves $\forall x\ [[\phi(x) \Leftrightarrow \phi(0)] \vee [\phi(x) \Leftrightarrow \phi(S(0))] \vee \ldots \vee [\phi(x) \Leftrightarrow \phi(S^{k-1}(0))]]$, so it also proves $\forall x\ [[\phi(0) \wedge \phi(S(0)) \wedge \ldots \wedge \phi(S^{k-1}(0))] \Rightarrow \phi(x)]$ and therefore it proves $\forall x\ \phi(x)$ too (by applying modus ponens with the hypothesis). □

A consequence of Lemma 2.2.1.1 is Corollary 2.2.1.2, which ensures total quantifier elimination for every formula.

Corollary 2.2.1.2. *For every formula ϕ, there exists a formula ψ without variables (neither free nor bounded; so, in particular, ψ is quantifier-free) such that PA_k proves $[\phi \Leftrightarrow \psi]$.*

Proof. The result follows by first transforming any eventual occurrence of an existential quantifier in ϕ into an occurrence of an universal quantifier, by means of the rule $[\exists x\ \alpha(x) \Leftrightarrow \neg\forall x\ \neg\alpha(x)]$ (where $\alpha(x)$ is any formula); and then replacing any eventual subformula of the form $\forall x\ \beta(x)$ (where $\beta(x)$ is any formula) with the corresponding formula $[\beta(0) \wedge \beta(S(0)) \wedge \ldots \wedge \beta(S^{k-1}(0))]$, by means of Lemma 2.2.1.1. □

	Peano arithmetic	k-th modular arithmetic
Inference rules	Generalization (i.e. universal quantification) and modus ponens	
Relation letters	$=$ (equality, binary)	
Function letters	$+$ (sum, binary), $\cdot$ (product, binary), S (successor, unary)	
Constants	0 (zero)	
Logical axioms (let α, β, γ, $\delta(x)$ and ε be formulas such that ε contains no free occurrences of x, and let t be a term which is free for x in $\delta(x)$)	$[\alpha \Rightarrow [\beta \Rightarrow \alpha]]$	
	$[[\alpha \Rightarrow [\beta \Rightarrow \gamma]] \Rightarrow [[\alpha \Rightarrow \beta] \Rightarrow [\alpha \Rightarrow \gamma]]]$	
	$[[\neg\alpha \Rightarrow \neg\beta] \Rightarrow [\beta \Rightarrow \alpha]]$	
	$[\forall x\ \delta(x) \Rightarrow \delta(t)]$	
	$[\forall x\ [\varepsilon \Rightarrow \alpha] \Rightarrow [\varepsilon \Rightarrow \forall x\ \alpha]]$	
Equality axioms (let t, u and v be terms)	$t = t$	
	$[u = v \Rightarrow v = u]$	
	$[[t = u \wedge u = v] \Rightarrow t = v]$	
	$[u = v \Rightarrow t + u = t + v]$	
	$[u = v \Rightarrow u + t = v + t]$	
	$[u = v \Rightarrow t \cdot u = t \cdot v]$	
	$[u = v \Rightarrow u \cdot t = v \cdot t]$	
	$[u = v \Rightarrow S(u) = S(v)]$	
Proper axioms (let $\phi(x)$ be a formula)	$\forall x\ \forall y\ [S(x) = S(y) \Rightarrow x = y]$	
	$\forall x\ x + 0 = x$	
	$\forall x\ \forall y\ x + S(y) = S(x + y)$	
	$\forall x\ x \cdot 0 = 0$	
	$\forall x\ \forall y\ x \cdot S(y) = (x \cdot y) + x$	
	$\forall x\ \neg S(x) = 0$	$\forall x\ [S(x) = 0 \Leftrightarrow x = S^{k-1}(0)]$ (**Axiom M1**)
	$[[\phi(0) \wedge \forall x\ [\phi(x) \Rightarrow \phi(S(x))]] \Rightarrow \forall x\ \phi(x)]$ (induction principle)	$\forall x\ [x = 0 \vee x = S(0) \vee \ldots \vee x = S^{k-1}(0)]$ (**Axiom M2**)

Table 2.1: A comparison between PA and PA_k.

Theorem 2.2.1.3 shows that Axiom M2 and the induction principle are interchangeable in PA_k, but Axiom M2 was preferred in order to evidence that PA_k is **finitely axiomatizable** (i.e. its set of proper axioms is finite), while PA is **recursively axiomatizable** (i.e. its set of proper axioms is recursively enumerable).

Theorem 2.2.1.3. *Axiom M2 and the induction principle are interchangeable in* PA_k.

Proof. Let T be the theory obtained by replacing Axiom M2 with the induction principle in PA_k, and let $\alpha(x)$ be the formula

$$\bigvee_{i=0}^{k-1} [x = S^i(0)].$$

Obviously T proves $\alpha(0)$. The formula $[\alpha(x) \Rightarrow \alpha(S(x))]$ is equivalent to

$$\left[\neg\alpha(x) \vee \bigvee_{i=0}^{k-1} [S(x) = S^i(0)]\right]$$

or, in other words, to

$$\left[\neg\alpha(x) \vee \bigvee_{i=1}^{k} [S(x) = S^i(0)]\right]$$

(by Axiom M1). And this last formula is equivalent to $[\neg\alpha(x) \vee \alpha(x)]$ (by successor cancellation), which is a tautology that T proves. Thus T proves $\forall x\ \alpha(x)$ (by applying the induction principle), i.e. Axiom M2. Now, let $\phi(x)$ be any formula. It is clear that PA_k proves the tautology

$$\left[\left[\phi(0) \wedge \bigwedge_{i=0}^{k-1} [\phi(0) \Leftrightarrow \phi(S^i(0))]\right] \Rightarrow \bigwedge_{i=0}^{k-1} [\phi(S^i(0))]\right];$$

which can be written as

$$\left[\left[\phi(0) \wedge \bigwedge_{i=0}^{k-1} [\phi(S^i(0)) \Rightarrow \phi(S^{i+1}(0))]\right] \Rightarrow \bigwedge_{i=0}^{k-1} [\phi(S^i(0))]\right]$$

(by Axiom M1). Therefore, PA_k proves $[[\phi(0) \wedge \forall x\ [\phi(x) \Rightarrow \phi(S(x))]] \Rightarrow \forall x\ \phi(x)]$ (by Lemma 2.2.1.1), i.e. the induction principle. □

Theorem 2.2.1.4 shows that the k-th modular arithmetic possess completeness.

Theorem 2.2.1.4. *The theory* PA_k *is complete.*

Proof. The proof goes by induction on the number of quantifiers. The base case consists of quantifier-free formulas without free variables; which PA_k clearly decides. Now, let n be any non-negative integer. In addition, suppose that, for every non-negative integer i and every formula $\psi(x)$ with exactly n quantifiers and whose only free variable is x, PA_k decides $\psi(S^i(0))$; and let $\phi(x)$ be any formula with exactly n quantifiers and whose only free variable is x.

Case 1: $\forall x\ \phi(x)$ is true Then PA_k proves $[\phi(0) \wedge \phi(S(0)) \wedge \ldots \wedge \phi(S^{k-1}(0))]$ (by induction hypothesis) and therefore it also proves $\forall x\ \phi(x)$ (by Lemma 2.2.1.1).

Case 2: $\forall x\ \phi(x)$ is false Then there is some non-negative integer r such that PA_k proves $\neg\phi(S^r(0))$ (by induction hypothesis), so it also proves $\exists x\ \neg\phi(x)$ or, equivalently, $\neg\forall x\ \phi(x)$.

Case 3: $\exists x\ \phi(x)$ is true Then there is some non-negative integer r such that PA_k proves $\phi(S^r(0))$ (by induction hypothesis) and therefore it also proves $\exists x\ \phi(x)$.

Case 4: $\exists x\ \phi(x)$ is false Then PA_k proves $[\neg\phi(0) \wedge \neg\phi(S(0)) \wedge \ldots \wedge \neg\phi(S^{k-1}(0))]$ (by induction hypothesis), so it also proves $\forall x\ \neg\phi(x)$ (by Lemma 2.2.1.1) or, in equivalently, $\neg\exists x\ \phi(x)$. □

2.2.2 A Diophantine measure of complexity

This work connects two complexity measures, one from logic (viz., the arithmetical hierarchy) and another from number theory (viz., the irrationality measure).

The **generating function** in variable z of a sequence s of non-negative integers, which is denoted by $\mathrm{GF}(s(n);z)$, is the expression $\sum_{n=0}^{\infty}(s(n)z^n)$ (see Weisstein [23]).

For example, $\mathrm{GF}(n^2;z)$ is equal to $z(z+1)/(1-z)^3$.

And the **characteristic function** of a set S of non-negative integers, which is denoted by χ_S, is the unary operation on the set of non-negative integers which maps every non-negative integer n into one, if n belongs to S; and into zero otherwise (cf. Weisstein [19]).

For example, if S is the set of even non-negative integers and n is a non-negative integer, then $\chi_S(n)$ equals $(1+(-1)^n)/2$.

Now, let Φ denote the function from the set of sets of non-negative integers to the interval $[0,1]$ which maps every set S of non-negative integers into the number $\mathrm{GF}(\chi_S(n);1/2)/2$.

For example, the number $\mathrm{GF}(\chi_{\varnothing}(n);1/2)/2$ (resp., $\mathrm{GF}(\chi_{\mathbb{Z}_{\geq 0}}(n);1/2)/2$) is equal to $\sum_{n=0}^{\infty}(0/2^n)/2$ (resp., $\sum_{n=0}^{\infty}(1/2^n)/2$) or, in other words, to zero (resp., one). As a more interesting example, consider $\mathrm{GF}(\chi_P(n);1/2)$, where P is the set of primes; which is called the **prime constant** and whose value is approximately 0.4146825 (see OEIS A051006).

A set S of non-negative integers is said to be **cofinite** if, and only if, $\mathbb{Z}_{\geq 0}\backslash S$ is finite (see Halpern [6, Section 2.2]).

For example, the set of positive integers is cofinite because $\{0\}$ is finite.

The function Φ is not injective because finite and cofinite sets share their images via Φ.

For example,

$$\mathrm{GF}(\chi_{\{0\}}(n);1/2)/2=(1/2^0)/2=\frac{1}{2}=\frac{1}{2}\sum_{n=1}^{\infty}(1/2^n)=\mathrm{GF}(\chi_{\mathbb{Z}_{>0}}(n);1/2)/2$$

and

$$\mathrm{GF}(\chi_{\{0,3,4,5\}}(n);1/2)/2=\frac{39}{64}=\mathrm{GF}(\chi_{\mathbb{Z}_{\geq 0}\backslash\{1,2,5\}}(n);1/2)/2.$$

Proposition 2.2.2.1. *The function Φ is surjective.*

Proof. Let x be any positive real number which does not exceed one. The binary expansion of x induces a set of positive integers S such that $\sum_{n=1}^{\infty}(\chi_S(n)2^{-n}) = x$, which is equivalent to $\sum_{n=0}^{\infty}(\chi_S(n)(1/2)^{n+1}) = x$. And the latter equality can be written as $\mathrm{GF}(\chi_S(n); 1/2)/2 = x$. □

The **irrationality measure** of a real number x, which is denoted by $\mu(x)$, is the infimum of the set

$$\{a \in \mathbb{R}_{>0} : \{(p, q) \in \mathbb{Z}^2 : 0 < |x - p/q| < 1/q^a\} \text{ is finite}\}$$

if it exists and ∞ otherwise (see Weisstein [24]).

For example, the irrationality measure of a real number equals one if and only if it is rational. In addition, the irrationality measure of any algebraic number whose degree exceeds one is two (see Weisstein [24]); result which is known as **Roth's theorem** and whose proof-theoretic analysis is one of the origins of extractive proof theory (cf. Kohlenbach [10, Section 1]).

An **arithmetic progression** is an integer sequence of the form $(an+b)_{n=0}^{\infty}$, where a and b are any two integers such that a is not zero (cf. Weisstein [18]).

For example, $(1 - 20n)_{n=0}^{\infty}$ is an arithmetic progression.

The **arithmetical hierarchy** measures the complexity of a set S of non-negative integers by counting the minimum number of quantifier alternations that a formula $\phi(x)$ in the language of Peano arithmetic must have in order to define S; i.e. in order to be such that the set of non-negative integers such that $\phi(S^n(0))$ is true (in the standard model of Peano arithmetic) is S (see Enderton [4, Section 5.1]).

It might be interesting to study how the arithmetical hierarchy and the irrationality measure interrelate via Φ. As an example, we have Proposition 2.2.2.2.

Proposition 2.2.2.2. *Given any set S of non-negative integers, $\mu(\Phi(S))$ equals one if and only if S is a finite union of finite sets of non-negative integers and image sets of arithmetic progressions of non-negative terms.*

Proof. The statement that $\mu(\Phi(S))$ equals one is equivalent to the rationality of the number $\Phi(S)$, which holds true if and only if χ_S is eventually periodic. And this happens if and only if S is a finite union of finite sets of non-negative integers and image sets of arithmetic progressions of non-negative terms. □

Chapter 3

Number-theoretic lattices

Given any $\mathbb{R}$-basis $(\vec{v}, \vec{w})$ of $\mathbb{R}^2$, the **point-lattice** or **number-theoretic lattice** generated by $(\vec{v}, \vec{w})$, which is denoted by $\mathcal{L}(\vec{v}, \vec{w})$, is the set $\{m\vec{v} + n\vec{w} : m \text{ and } n \text{ are integers}\}$ (cf. Hardy & Wright [8, Section 3.5]). And given any vector $\vec{u}$ of $\mathbb{R}^2$ and any point-lattice L, the set $\{\vec{u} + \vec{l} : \vec{l} \in L\}$ is denoted by $\vec{u} + L$.

For example, $(0, 32/7)$ belongs to $(1, -1) + \mathcal{L}((-2, 2), (3, 11/7))$ because $(0, 32/7)$ equals $(1, -1) + 2(-2, 2) + (3, 11/7)$.

The **cover** of any two integers a and b which exceed one, which is denoted by $\mathcal{C}(a, b)$, is the set of pairs (x, y) of non-negative rational numbers such that $a^x + b^y$ is an integer multiple of $ab + 1$.

For example, $(0, 32/7)$ belongs to $\mathcal{C}(5, 128)$ because $5 \cdot 128 + 1 = 641 \mid 2^{2^5} + 1 = 5^0 + 128^{32/7}$.

The reason to add the conditions $a > 1$ and $b > 1$ in the definition of cover is to avoid an "excess" of points which would probably fog the theory: for example, every rational number x is such that $1 \cdot 5 + 1$ factors $1^x + 5^3$.

Given any non-negative integer n, the n-th **Fermat number** is the number $2^{2^n} + 1$ (see Křížek et al. [11, Chapter 1]). The first five Fermat numbers are 3, 5, 17, 257, 65537 (see OEIS A000215); and notice that they are prime. However, the existence of any other prime Fermat number is currently unknown (see OEIS A019434).

Given any non-negative integer n, let $\mathcal{F}(n)$ denote the set

$$\left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \mathcal{L}\left(\begin{bmatrix} -2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2\lfloor \alpha(n) \rfloor - 1 \\ 2\alpha(n) - 2\lfloor \alpha(n) \rfloor + 1 \end{bmatrix} \right) \right) \cap \mathbb{Q}^2_{\geq 0},$$

where $\alpha(n)$ equals $2^{n-1}/(n+2)$.

Baaz [1] developed a technique of extractive proof theory, now known as **Baaz's generalization method**, which is re-explained in Section 2 of Article C in Section 3.2. This procedure was exemplified by means of a pioneer application to the factorization of Fermat numbers, Proposition 8 of Article C (see also Baaz [1, Theorem 15]), which led, through the realization of Article B and Article C, to a geometric characterization of these (i.e. Theorem 11 of Article C). And this characterization can be now nicely stated, in terms of point-lattices and covers, as Theorem 3.0.0.1.

Theorem 3.0.0.1. *Given any two integers* $m > 1$ *and* $n > 2$*, the number* $m2^{n+2}+1$ *is a factor of the* n*-th Fermat number if and only if* $\mathcal{F}(n)$ *is a subset of* $\mathcal{C}(m, 2^{n+2})$*.*

We now reproduce Article B and Article C, and then continue by showing some further results.

3.1 Article B

This is an Accepted Manuscript of an article published by the University of Primorska in *The Art Of Discrete And Applied Mathematics* on 15/Nov/2022, available online: `https://adam-journal.eu/index.php/ADAM/article/view/1473`.

Corrections:

1. in the statement of Lemma 2.4, the number i must exceed one;
2. in the statement of Theorem 2.3, the number n must exceed two (otherwise $n - \nu_2(n+2)$ becomes zero and Lemma 2.4 is no longer applicable);
3. the proof of Theorem 2.3 misses a final sentence such as "The thesis follows by applying Lemma 2.4.";
4. Lemma 2.4 (and its proof) should appear therefore just before the definition of dyadic valuation and
5. in the statement of Theorem 2.5, the number i must exceed one and the number n must exceed two.

THE ART OF DISCRETE AND APPLIED MATHEMATICS

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 6 (2023) #P2.05
https://doi.org/10.26493/2590-9770.1473.ec5
(Also available at http://adam-journal.eu)

Some properties of the factors of Fermat numbers

Lorenzo Sauras-Altuzarra*

Institut für Diskrete Mathematik und Geometrie (TU Wien),
Wiedner Hauptstrasse 8-10/104, Vienna (1040), Austria

Received 28 September 2021, accepted 9 January 2022, published online 15 November 2022

Abstract

This article reports some recent progress from an ongoing research project on the factors of Fermat numbers; most notably a necessary condition for a given value to be a factor and a characterization of the prime ones.

Keywords: Baaz's generalization method, Bézout's coefficient, Dyadic valuation, Fermat prime, integer sequence, permutation.

Math. Subj. Class.: 11A51, 11Y55

1 Introduction

The numbers of the form $2^{2^n}+1$, where n is a non-negative integer, are called *Fermat numbers*. Because of their quick growth, computing their factors is a challenge (only the first twelve are fully factored at the present time) and to characterize them is thus interesting. Remarkably, the so-called Pépin's test (see Weisstein [12]) has been utilized in order to prove the compositeness of $2^{2^{20}}+1$ (see Buell & Young [14]) and of $2^{2^{24}}+1$ (see Crandall et al. [3]), although no prime factor is yet known.

Section 2 is the one that properly revolves around characterizations of factors of Fermat numbers. The first main result (viz., Theorem 2.1) is a sufficient condition for a given value to be a factor of a Fermat number. It was obtained by applying Baaz's generalization method (see Baaz [1]) to a proof of the fact that $1071\cdot 2^{6+2}+1 \mid 2^{2^6}+1$ that a participant of the Mersenne Forum, nicknamed Literka, published on a web page at some point prior to March 25, 2012 (although the website is currently unavailable, it is possible to find a backup in the Way Back Machine). The condition also happened to be necessary, provided that the

*The author thanks Jinyuan Wang for his numerous contributions to this article, including the formula $n-v_2(n+2)$ from Theorem 2.3. Supported by FWF Austria (project numbers P31063 and P31955).
E-mail address: lorenzo.sauras@tuwien.ac.at (Lorenzo Sauras-Altuzarra)

candidate is prime or the Fermat number is squarefree (viz., Theorem 2.2). In addition, the study of the positive integers of the form $k^{2r} + 2^{2^n - 2r(n+2)}$ led to the observation that $1071^{2\cdot 4} + 2^{2^6 - 2\cdot 4(6+2)} = 1071^{2^3} + 1$ and to another subsequent necessary condition (viz., Theorem 2.3).

Section 3 analyzes several sequences that are useful in order to study Fermat numbers.

Section 4 presents a sequence that might share some properties with the sequence of Fermat numbers.

For the sake of brevity, throughout this text the notation "$a \underset{n}{\equiv} b$" is preferred over the standard one of "$a \equiv b \pmod{n}$".

2 Divisibility conditions

Observe that $1 \cdot 25 - 6 \cdot 4 = 19 \cdot 4 - 3 \cdot 25 = 1$ and $25^2 + 4^2$ (which equals 641) is a prime factor of $2^{2^5} + 1$, of $2^{2^5} - (6 \cdot 25 + 1 \cdot 4)^2$, and of $2^{2^5} - (3 \cdot 4 + 19 \cdot 25)^2$; and recall the so-called Diophantus' identity (see Bernstein [2, Fact 2.4.7]): $(ac + bd)^2 + (bc - ad)^2 = (a^2 + b^2)(c^2 + d^2)$, for every complex number a, b, c, and d.

Theorem 2.1. *If a, b, c, d, and n are integers such that n is non-negative, $(bc - ad)^2 = 1$, and $c^2 + d^2 \mid 2^{2^n} - (ac + bd)^2$, then $c^2 + d^2 \mid 2^{2^n} + 1$.*

Proof. Since $(bc-ad)^2 = 1$, it follows that $(ac+bd)^2 \underset{c^2+d^2}{\equiv} -1$ (by applying Diophantus' identity) and therefore $2^{2^n} \underset{c^2+d^2}{\equiv} -1$ (by applying that $c^2 + d^2 \mid 2^{2^n} - (ac + bd)^2$). □

Theorem 2.2. *If c, d, and n are integers such that n is non-negative, $c^2 + d^2 \mid 2^{2^n} + 1$, and $c^2 + d^2$ is prime or $2^{2^n} + 1$ is squarefree, then there exist integers a and b such that $(bc - ad)^2 = 1$ and $c^2 + d^2 \mid 2^{2^n} - (ac + bd)^2$.*

Proof. If $c^2 + d^2$ is prime or $2^{2^n} + 1$ is squarefree, then $\gcd(c, -d) = 1$ (by applying that $c^2 + d^2 \mid 2^{2^n} + 1$) and hence there exist integers a and b such that $bc + a(-d) = 1$ (by applying Bézout's lemma; see Křížek et al. [6, Theorem 1.3]); from which follows that $(bc - ad)^2 = 1$. In addition, Diophantus' identity implies that $c^2 + d^2 \mid (ac+bd)^2 + (bc-ad)^2$; which yields that $c^2 + d^2 \mid 2^{2^n} + 1 - (ac + bd)^2 - (bc - ad)^2$ (by applying that $c^2+d^2 \mid 2^{2^n}+1$) and therefore $c^2+d^2 \mid 2^{2^n} - (ac+bd)^2$ (by applying that $bc-ad = 1$). □

The *dyadic valuation* of a positive integer n, denoted by $\nu_2(n)$, is the maximum non-negative integer v such that $2^v \mid n$. It satisfies the property $\nu_2(mn) = \nu_2(m) + \nu_2(n)$, for every positive integer m (see the Encyclopedia of Mathematics [4]).

Observe that $38019230 \cdot 2^{11+2} + 1$ (i.e. $319489 \cdot 974849$) is a factor of $2^{2^{11}} + 1$ and of $38019230^{2^{11}(2j-1)} + 1$, for every positive integer j.

Theorem 2.3. *If k and n are positive integers such that $k2^{n+2} + 1 \mid 2^{2^n} + 1$, then $k2^{n+2} + 1 \mid k^{2^{n-\nu_2(n+2)}(2j-1)} + 1$, for every positive integer j.*

Proof. Since $\nu_2(2^{n-\nu_2(n+2)}(2j-1)(n+2)) = \nu_2(2^{n-\nu_2(n+2)}) + \nu_2(2j-1) + \nu_2(n+2) = n - \nu_2(n+2) - 0 + \nu_2(n+2) = n$, it follows that there exists an odd positive integer d such that $2^n d = 2^{n-\nu_2(n+2)}(2j-1)(n+2)$ and therefore $2^{2^{n-\nu_2(n+2)}(2j-1)(n+2)} = 2^{2^n d} = (2^{2^n})^d \underset{k2^{n+2}+1}{\equiv} (-1)^d = -1$ (by applying that $k2^{n+2} + 1 \mid 2^{2^n} + 1$). □

The converse implication of Theorem 2.3 does not hold: 4278255361 is not a factor of $2^{2^3}+1$ but divides $\left(\frac{4278255361-1}{2^{3+2}}\right)^{2^{3-\nu_2(3+2)}(2j-1)}+1$, for every positive integer j.

Lemma 2.4. *Given positive integers i, j, k, and n, $k2^{n+2}+1 \mid k^{2^{i-1}(2j-1)}+1$ if and only if $k2^{n+2}+1 \mid 2^{2^{i-1}(2j-1)(n+2)}+1$.*

Proof. Let

$$r=\frac{1-(-k2^{n+2})^{2^{i-1}(2j-1)}}{1-(-k2^{n+2})}=\sum_{l=0}^{2^{i-1}(2j-1)-1}\left((-k2^{n+2})^l\right),$$

which is an integer, and notice that

$$2^{2^{i-1}(2j-1)(n+2)}+1-(k2^{n+2}+1)r=2^{2^{i-1}(2j-1)(n+2)}(k^{2^{i-1}(2j-1)}+1). \qquad \square$$

Theorem 2.5 ensures the uniqueness of the exponent $n-\nu_2(n+2)$ in Theorem 2.3.

Theorem 2.5. *If i, j, k, and n are positive integers such that $k2^{n+2}+1 \mid 2^{2^n}+1$ and $i-1 \neq n-\nu_2(n+2)$, then $k2^{n+2}+1 \nmid k^{2^{i-1}(2j-1)}+1$.*

Proof. Let r be the odd positive integer such that

$$2^{i-1}(2j-1)(n+2)=r2^{i-1+\nu_2(n+2)}.$$

Let m and M be the minimum and the maximum of $\{n, i-1+\nu_2(n+2)\}$, respectively. Let d be a factor of $2^{r2^m}+1$ such that $d>1$. Because of $m<M$ (by applying that $i-1 \neq n-\nu_2(n+2)$), $2^{r2^M}=(2^{r2^m})^{2^{M-m}} \underset{d}{\equiv} (-1)^{2^{M-m}}=1$ and consequently $d \mid 2^{r2^M}-1$. Notice that $d \nmid 2^{r2^M}+1$ (by applying that consecutive odd numbers are coprime), from which follows that $\gcd(2^{r2^m}+1, 2^{r2^M}+1)=1$; that is to say, $2^{r2^n}+1$ and $2^{r2^{i-1+\nu_2(n+2)}}+1$ are coprime. Now, $k2^{n+2}+1 \mid k^{2^{n-\nu_2(n+2)}(2j-1)}+1$ (by applying Theorem 2.3); so $k2^{n+2}+1 \mid 2^{2^{n-\nu_2(n+2)}(2j-1)(n+2)}+1=2^{r2^n}+1$ (by applying Lemma 2.4) and therefore $k2^{n+2}+1 \nmid 2^{2^{i-1}(2j-1)(n+2)}+1=2^{r2^{i-1+\nu_2(n+2)}}+1$ (by applying the coprimality of $2^{r2^n}+1$ and $2^{r2^{i-1+\nu_2(n+2)}}+1$). In other words, $k2^{n+2}+1 \nmid k^{2^{i-1}(2j-1)}+1$ (by again applying Lemma 2.4). $\square$

3 Some useful sequences

Let $\boldsymbol{p}$ (resp., $\boldsymbol{q}$) be the (increasing) enumeration of primes (resp., prime factors of Fermat numbers). The first eight terms of the sequence $\boldsymbol{q}$ are 3, 5, 17, 257, 641, 65537, 114689, and 274177 (see OEIS A023394, but be aware that the sequence is indexed from 1 instead of from 0 there).

Recall that Ω and ω are the functions that map every positive integer into its number of prime factors counted with and without multiplicity, respectively. For example, $\Omega(1)=\omega(1)=0$, $\Omega(12)=3$, and $\omega(12)=2$. The only known terms of the sequence of numbers of the form $\Omega(2^{2^n}+1)$, where n is a non-negative integer, are 1, 1, 1, 1, 1, 2, 2, 2, 2, 3, 4, and 5 (see OEIS A046052). It is not known if this sequence is monotonic. In addition, it is not known if Fermat numbers are squarefree (i.e. if the sequence of numbers of the form $\omega(2^{2^n}+1)$, where n is a non-negative integer, is the same sequence).

Given a non-negative integer n, let $\boldsymbol{x}(n)$ be the only non-negative integer a such that $\boldsymbol{q}(n) \mid 2^{2^a}+1$. For example, $\boldsymbol{x}(0)=0$ because $\boldsymbol{q}(0)=3 \mid 3=2^{2^0}+1$. The uniqueness of a is guaranteed by Goldbach's theorem on Fermat numbers, which asserts that Fermat numbers are pairwise coprime (see Křížek et al. [5], Theorem 4.1). The first eight terms of the sequence $\boldsymbol{x}$ are 0, 1, 2, 3, 5, 4, 12, and 6 (see OEIS A023395, but be aware that the sequence is indexed from 1 instead of from 0 there). Note that the pairwise coprimality of the Fermat numbers induces a permutation of the non-negative integers (see OEIS A343767).

The *ordinal transform* of a sequence s is the sequence whose n-th term is the cardinality of the set $\{i \in \{0,\dots,n\} \mid s(i)=s(n)\}$, for every non-negative integer n. The first 27 terms of the ordinal transform of $\boldsymbol{x}$ are 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 2, 1, 2, 1, 3, 1, 1, 1, 2, 1, 4, 2, 1, 1, 1, and 1. Note that, given a non-negative integer n, $\omega(2^{2^n}+1)$ is the cardinality of the set $\{i \in \mathbb{N} \mid \boldsymbol{x}(i)=n\}$.

Euler proved that, if a is a non-negative integer and f is a factor of $2^{2^a}+1$ such that $f>1$, then $\nu_2(f-1)>a$. In particular, $\nu_2(\boldsymbol{q}(n)-1)>\boldsymbol{x}(n)$, for every non-negative integer n. Lucas proved later that, if in addition $a>1$, then $\nu_2(f-1)>a+1$. In particular, $\nu_2(\boldsymbol{q}(n)-1)>\boldsymbol{x}(n)+1$, for every integer n such that $n>1$. See Weisstein [10]. The first 27 terms of the sequence of numbers of the form $\nu_2(\boldsymbol{q}(n)-1)-\boldsymbol{x}(n)-1$, where n is a non-negative integer, are 0, 0, 1, 4, 1, 11, 1, 1, 1, 1, 6, 1, 1, 3, 1, 3, 1, 2, 5, 3, 1, 1, 1, 2, 2, 1, and 2. The results by Euler and Lucas imply that they are non-negative and, from the third on, positive.

Observe that $\boldsymbol{q}(5)=(2-1)^2+2^{14}(2^0+3^0)^2=(2-1)^2+2^{14}\boldsymbol{p}(0)^2$, $\boldsymbol{q}(10)=(2^7-1)^2+2^8(2^4+3^4)^2=(2^7-1)^2+2^8\boldsymbol{p}(24)^2$, and $\boldsymbol{q}(13)=(2^{11}-1)^2+2^{12}(2^6+3^2)^2=(2^{11}-1)^2+2^{12}\boldsymbol{p}(20)^2$; and recall that a *Pythagorean prime* is a prime of the form $4n+1$, where n is a positive integer.

Proposition 3.1. *If n is a positive integer, then there exist unique positive integers c and d such that c is odd, d is even, and $c^2+d^2=\boldsymbol{q}(n)$.*

Proof. Since $\boldsymbol{q}(n)>3=2^{2^0}+1$ (by applying that n is positive), it follows that $\nu_2(\boldsymbol{q}(n)-1)>\boldsymbol{x}(n)>0$ (by applying the above result by Euler). That is to say, $\boldsymbol{q}(n)$ is a Pythagorean prime, which ensures the existence of positive integers u and v such that $u^2+v^2=\boldsymbol{q}(n)$ (by applying Fermat's two squares theorem; see Shoup [8, Theorem 2.34]). If u and v were both even or both odd, then u^2+v^2 would be even, but it is odd. Take c to be the odd number in $\{u,v\}$ and d the other one. □

In fact, any factor of a Fermat number, except 1 and 3, is the sum of two squares (by applying Proposition 3.1 and the fact that the set of integers that are the sum of two squares is closed under multiplication, see OEIS A001481). However, the uniqueness cannot be ensured; observe for example that $2^{2^5}+1=\boldsymbol{q}(4)\boldsymbol{q}(11)=1+65536^2=20449^2+62264^2$.

Given a non-negative integer n, let $\boldsymbol{c}(n)$ and $\boldsymbol{d}(n)$ be the positive integers such that $\boldsymbol{c}(n)$ is odd, $\boldsymbol{d}(n)$ is even, and $\boldsymbol{c}(n)^2+\boldsymbol{d}(n)^2=\boldsymbol{q}(n+1)$. The first 26 terms of the sequence $\boldsymbol{c}$ are 1, 1, 1, 25, 1, 217, 89, 167, 985, 127, 409, 25, 2047, 2279, 7295, 12455, 19425, 34815, 55297, 243047, 424231, 704935, 755681, 1640929, 607847, and 1548319. The first 26 terms of the sequence $\boldsymbol{d}$ are 2, 4, 16, 4, 256, 260, 516, 540, 68, 1552, 2556, 3692, 4672, 6356, 3248, 3556, 21176, 1472, 58560, 107020, 101500, 387036, 1462840, 236920, 2028748, and 2049336; and the first 26 terms of the sequence $\nu_2 \circ \boldsymbol{d}$ are 1, 2, 4, 2, 8, 2, 2, 2, 2, 4, 2, 2, 6, 2, 4, 2, 3, 6, 6, 2, 2, 2, 3, 3, 2, and 3.

Proposition 3.2. *If n is a positive integer, then $\nu_2(\boldsymbol{d}(n))>1$.*

Proof. Since $\nu_2(\boldsymbol{q}(n+1)-1) > \boldsymbol{x}(n+1)+1 \geq 2+1$ (by applying that n is positive and the above result by Lucas), it follows that $\nu_2(\boldsymbol{q}(n+1)-1) \geq 4$. That is to say, $\nu_2(\boldsymbol{c}(n)^2+\boldsymbol{d}(n)^2-1) \geq 4$; which is equivalent to $\boldsymbol{c}(n)^2 \underset{16}{\equiv} 1-\boldsymbol{d}(n)^2$. Notice that the parity of $\boldsymbol{d}(n)$ implies that $\boldsymbol{d}(n) \underset{4}{\equiv} 0$ or $\boldsymbol{d}(n) \underset{4}{\equiv} 2$. Let $\widetilde{d}$ be the positive integer such that $2\widetilde{d} = \boldsymbol{d}(n)$. If $\boldsymbol{d}(n) \underset{4}{\equiv} 2$, then $\widetilde{d} \underset{4}{\equiv} 1$; from which follows that $\boldsymbol{d}(n)^2 = 4\widetilde{d}^2 \underset{4\cdot 4}{\equiv} 4\cdot 1$ and thus $\boldsymbol{c}(n)^2 \underset{16}{\equiv} 1-\boldsymbol{d}(n)^2 \underset{16}{\equiv} 1-4 \underset{16}{\equiv} 13$: impossible, because 13 is not a quadratic residue modulo 16. Therefore $\boldsymbol{d}(n) \underset{4}{\equiv} 0$; i.e. $\nu_2(\boldsymbol{d}(n)) > 1$. □

The first 26 terms of the sequence of numbers of the form $\frac{\operatorname{sgn}(\boldsymbol{d}(n)-\boldsymbol{c}(n))+1}{2}$, where sgn is the signum function and n is a non-negative integer, are 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, and 1.

Given a non-negative integer n, let $\boldsymbol{m}(n)$ be the smallest prime factor of $2^{2^n}+1$ (see OEIS A093179). An analysis of the algorithms described by Wang [9] suggests the interest of the sequence $\boldsymbol{y}$, whose n-th term is the minimum non-negative integer a such that $2^{2^n-a} < \boldsymbol{m}(n)$, for every non-negative integer n. The first 14 terms of the sequence $\boldsymbol{y}$ are 0, 0, 0, 0, 0, 23, 46, 73, 206, 491, 999, 2030, 4080, and 8151.

Conjecture 3.3. *The sequence $\boldsymbol{y}(n)$ is asymptotically equivalent to 2^n.*

The first 14 numbers of the form $2^n-\boldsymbol{y}(n)-\nu_2(\boldsymbol{m}(n)-1)$, where n is a non-negative integer, are 0, 0, 0, 0, 0, 2, 10, 46, 39, 5, 13, 5, 2, and 25.

Conjecture 3.4. *Given a non-negative integer n, $\nu_2(\boldsymbol{m}(n)-1) \leq 2^n-\boldsymbol{y}(n)$.*

4 A related sequence

Given an integer b such that $b > 1$, the numbers of the form $b^{b^n}+1$ (which is denoted by $F_b(n)$), where n is a non-negative integer, are called *base-$\boldsymbol{b}$ Fermat numbers* (see OEIS A129290). Given a non-negative integer n, let $\boldsymbol{z}(n)$ be the number $\frac{F_{\boldsymbol{p}(n+1)}(1)}{F_{\boldsymbol{p}(n+1)}(0)}$; which is equal to $\frac{\boldsymbol{p}(n+1)^{\boldsymbol{p}(n+1)}+1}{\boldsymbol{p}(n+1)+1}$ or, equivalently, to $\sum_{k=0}^{\boldsymbol{p}(n+1)-1}\left((-\boldsymbol{p}(n+1))^k\right)$. The first five terms of the sequence $\boldsymbol{z}$ are 7, 521, 102943, 23775972551, and 21633936185161; i.e. $\boldsymbol{p}(3)$, $\boldsymbol{p}(97)$, $\boldsymbol{p}(29)\boldsymbol{p}(155)$, $\boldsymbol{p}(8)\boldsymbol{p}(23)\boldsymbol{p}(45)\boldsymbol{p}(5907)$, and $\boldsymbol{p}(1590)\boldsymbol{p}(2295)\boldsymbol{p}(7770)$.

Problem 4.1. Are the terms of $\boldsymbol{z}$ pairwise coprime? If this is the case, compute some terms of the induced permutation of the non-negative integers.

Problem 4.2. Is every term of $\boldsymbol{z}$ squarefree?

Let $\operatorname{lh}(n)$ be the length (i.e. the number of digits) of a given non-negative integer n. Note that $\operatorname{lh}(n) = \lfloor \log_{10}(n) \rfloor + 1$ if n is positive. Observe now that the first five numbers of the form $\sum_{i=0}^{n}\left(\left\lfloor \frac{\boldsymbol{p}(n+1)}{\boldsymbol{p}(i)} \right\rfloor\right)$, where n is a non-negative integer, are 1, 3, 6, 11, and 14 (see OEIS A342173, but be aware that the sequence is indexed from 1 instead of from 0 there).

Theorem 4.3. *Given a non-negative integer n, $\sum_{i=0}^{n}\left(\left\lfloor \frac{\boldsymbol{p}(n+1)}{\boldsymbol{p}(i)} \right\rfloor\right) \leq \operatorname{lh}(\boldsymbol{z}(n))$.*

Proof. Let n be a non-negative integer such that $n > 1000$ (it is possible to check with a computer that the thesis holds if $n \leq 1000$). It is known that

$$3n \overset{n>18}{<} (\log(n) + \log(\log(n)) - 1)n \overset{n>1}{<} \boldsymbol{p}(n-1) \overset{n>5}{<} (\log(n) + \log(\log(n)))n \quad (4.1)$$

(see Weisstein [13] and Rosser & Schoenfeld [7, Theorem 3]). Thus,

$$\frac{1}{\boldsymbol{p}(n-1)} < \frac{1}{3n} \quad (4.2)$$

$$\sum_{i=0}^{1000} \left(\frac{1}{\boldsymbol{p}(i)}\right) = 2.457537428 < 2.495489954 = \sum_{i=1}^{1001} \left(\frac{\boldsymbol{p}(n+1)}{3i}\right) \quad (4.3)$$

$$\sum_{i=1}^{n+1} \left(\frac{1}{i}\right) < 0.57721\ldots + \frac{1}{2(n+1)} + \log(n+1) \text{(see Weisstein [11])}. \quad (4.4)$$

$$\begin{aligned}
\sum_{i=0}^{n} \left(\left\lfloor \frac{\boldsymbol{p}(n+1)}{\boldsymbol{p}(i)} \right\rfloor\right) &\leq \sum_{i=0}^{n} \left(\frac{\boldsymbol{p}(n+1)}{\boldsymbol{p}(i)}\right) \\
&\overset{(4.2),(4.3)}{<} \sum_{i=1}^{n+1} \left(\frac{\boldsymbol{p}(n+1)}{3i}\right) \\
&= \frac{\boldsymbol{p}(n+1)}{3} \sum_{i=1}^{n+1} \left(\frac{1}{i}\right) \\
&\overset{(4.4)}{<} \frac{\boldsymbol{p}(n+1)}{3} \left(0.57721\ldots + \frac{1}{2(n+1)} + \log(n+1)\right) \\
&\overset{n>0}{<} \boldsymbol{p}(n+1)(1 + \log(n+1))/3 \\
&\overset{(4.1)}{<} (\log(n+2) + \log(\log(n+2)))(n+2)(1 + \log(n+1))/3 \\
&\overset{n>331}{<} (\log(n+2) \\
&\qquad + (3/\log(10) - 1)\log(n+2))(n+2)(1 + \log(n+1))/3 \\
&= \log(n+2)(n+2)(1 + \log(n+1))/\log(10) \\
&\overset{n>10}{<} \log(n+2)(n+2)\log_{10}(\log(n+2)(n+2)) \\
&\overset{n>18}{<} ((\log(n+2) + \log(\log(n+2)) - 1)(n+2) - 2)\cdot
\end{aligned}$$

$$\begin{aligned}
\log_{10}((\log(n+2) + \log(\log(n+2)) - 1)(n+2)) &\overset{(4.2)}{<} (\boldsymbol{p}(n+1) - 2)\log_{10}(\boldsymbol{p}(n+1)) \\
&= \log_{10}(\boldsymbol{p}(n+1)^{\boldsymbol{p}(n+1)-2}) \\
&< \left\lfloor \log_{10}(\boldsymbol{p}(n+1)^{\boldsymbol{p}(n+1)-2}) \right\rfloor + 1 \\
&= \mathrm{lh}(\boldsymbol{p}(n+1)^{\boldsymbol{p}(n+1)-2}) \\
&< \mathrm{lh}\left(\frac{\boldsymbol{p}(n+1)^{\boldsymbol{p}(n+1)} + 1}{\boldsymbol{p}(n+1) + 1}\right) \\
&= \mathrm{lh}(\boldsymbol{z}(n))
\end{aligned}$$

□

ORCID iDs

Lorenzo Sauras-Altuzarra https://orcid.org/0000-0001-6893-7463

References

[1] M. Baaz, Note on the generalization of calculations, *Theoret. Comput. Sci.* **224** (1999), 3–11, doi:10.1016/S0304-3975(98)00304-1, https://doi.org/10.1016/S0304-3975(98)00304-1.

[2] D. S. Bernstein, *Scalar, vector, and matrix mathematics. Theory, facts, and formulas*, Princeton University Press, Princeton, NJ, 2018, doi:10.1515/9781400888252, https://doi.org/10.1515/9781400888252.

[3] R. E. Crandall, E. W. Mayer and J. S. Papadopoulos, The twenty-fourth Fermat number is composite, *Math. Comp.* **72** (2003), 1555–1572, doi:10.1090/S0025-5718-02-01479-5, https://doi.org/10.1090/S0025-5718-02-01479-5.

[4] Encyclopedia of Mathematics, *P-adic valuation*, https://encyclopediaofmath.org/index.php?title=P-adic_valuation.

[5] M. Křížek, F. Luca and L. Somer, *17 lectures on Fermat numbers*, volume 9 of *CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC*, Springer-Verlag, New York, 2001, doi:10.1007/978-0-387-21850-2, https://doi.org/10.1007/978-0-387-21850-2.

[6] M. Křížek, L. Somer and A. Šolcová, *From great discoveries in number theory to applications*, Cham: Springer, 2021, doi:10.1007/978-3-030-83899-7, https://doi.org/10.1007/978-3-030-83899-7.

[7] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94, doi:10.1215/ijm/1255631807, https://doi.org/10.1215/ijm/1255631807.

[8] V. Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press, Cambridge, 2005, doi:10.1017/CBO9781139165464, https://doi.org/10.1017/CBO9781139165464.

[9] X. Wang, Algorithm available for factoring big fermat numbers, *Journal of Software* (2020), 86–97, doi:10.17706/jsw.15.3.86-97, https://doi.org/10.17706/jsw.15.3.86-97.

[10] E. W. Weisstein, *Fermat Number*, MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/FermatNumber.html.

[11] E. W. Weisstein, *Harmonic Number*, MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/HarmonicNumber.html.

[12] E. W. Weisstein, *Pépin's Test*, MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/PepinsTest.html.

[13] E. W. Weisstein, *Rosser's Theorem*, MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/RossersTheorem.html.

[14] J. Young and D. A. Buell, The twentieth Fermat number is composite, *Math. Comp.* **50** (1988), 261–263, doi:10.1090/S0025-5718-1988-0917833-8, https://doi.org/10.1090/S0025-5718-1988-0917833-8.

3.2 Article C

This is a pre-copyedited, author-produced version of an article accepted for publication in the *Journal of Logic and Computation* following peer review. The version of record:

- Lorenzo Sauras-Altuzarra,
- Some applications of Baaz's generalization method to the study of the factors of Fermat numbers,
- *Journal of Logic and Computation*,
- 2022,
- exac056

is available online at: `https://doi.org/10.1093/logcom/exac056`.

Correction: the phrase "for geometric configurations" at the very end of Section 2.2 should be replaced with "for some geometric configurations".

Some applications of Baaz's generalization method to the study of the factors of Fermat numbers

LORENZO SAURAS-ALTUZARRA, *Institut für Diskrete Mathematik und Geometrie, TU Wien, Wiedner Hauptstrasse 8-10/104, A-1040, Vienna, Austria.*
E-mail: lorenzo.sauras@tuwien.ac.at

Abstract

This paper revisits a method of generalization of proofs of universal sentences that was introduced by Baaz and provides several applications to the study of the factors of Fermat numbers; remarkably an improvement of his sufficient condition for a given value to be one of such factors.

Keywords: Fermat prime, Pépin's test, proof analysis, proof generalization, proof mining, universal formula

1 Introduction

The present article is divided into two main parts. The first one (viz., Section 2) consists on a small summary of concepts from first-order logic that is necessary afterwards, some words on the ideas behind the development of Baaz's generalization method, a brief description of the method itself and a little discussion about two of its possible extensions. The second one (viz., Section 3) collects three properties of Fermat numbers (including an apparently new one, Proposition 3); provides three applications of Baaz's generalization method to the study of the factors of such numbers (viz., Theorem 7, Theorem 14 and Theorem 15); and introduces the concept of cover, in terms of which the main result of the article (viz., Theorem 11) is formulated.

2 Baaz's generalization method

2.1 Preliminaries in first-order logic

Recall that, in a mathematical statement, every variable must be declared by using a **universal quantifier** or an **existential quantifier** (i.e. a phrase such as '*for every*', denoted by ∀; or a phrase such as '*for some*', denoted by ∃).

A **sentence** is a mathematical statement. For example, '*For every nonnegative integer n, if n is even and $n > 2$, then, for some nonnegative integers p and $\hat{p}$, p and $\hat{p}$ are prime and their sum equals n.*' is a sentence (known as **Goldbach's conjecture**, see Weisstein (16)).

The notion of **formula** is the generalization of the concept of sentence that allows nonquantified variables. For example, '*For some nonnegative integer n, m equals n.*' is a formula.

A **prenex formula** is a formula in which the quantified variables are quantified at the very beginning. It is always possible to compute a prenex formula equivalent to a given formula (see Hamilton (6, Proposition 4.28)). For example, a prenex version of Goldbach Conjecture is '*For every nonnegative integer n, for some nonnegative integers p and $\hat{p}$, if n is even and $n > 2$, then p and $\hat{p}$ are prime and their sum equals n.*'.

Vol. 00, No. 0,
https://doi.org/10.1093/logcom/exac056

A **universal formula** (resp., **existential formula**) is a prenex formula in which the quantified variables are universally (resp., existentially) quantified. For example, '*For all nonnegative integers a and b,* $a + b = b + a$.' is a universal sentence (the commutative rule for the addition).

A **quantifier-free formula** is a formula in which no variable is quantified. It is consequently a particular case shared between universal formulas and existential formulas. For example, '$641 \mid 2^{32} + 1$.', which does not even have variables, is a quantifier-free sentence.

Universal quantifiers can be replaced with existential quantifiers (and vice versa) by applying the rule $[\forall x P(x) \Leftrightarrow \neg\exists x \neg P(x)]$. For example, '*For every nonnegative integer n,* $n + 0 = n$.' is equivalent to '*There does not exist a nonnegative integer n such that* $n + 0 \neq n$.'.

An existential quantifier can be eliminated by defining new relations (in particular, new operations (and, in particular, new constants)). For example, '*For some nonnegative integer k,* $641k = 2^{32} + 1$.' can be transformed into '$641 \mid 2^{32} + 1$.' by defining the divisibility relation (denoted by $|$). This process is known as **Skolemization**.

Sometimes it is also possible to eliminate universal quantifiers (resp., existential quantifiers) by bounding the quantified variable and writing a conjunction (resp., disjunction) instead. For example, '*For every nonnegative integer n, if* $n < 2$*, then n is not prime.*' can be transformed into '0 is not prime and 1 is not prime.'.

2.2 Motivation

> '*Suppose you want to teach the commutative rule for addition, then* $0 + 4 = 4 + 0$ *is a bad example, since it also illustrates another rule (that* 0 *is neutral). Also* $1 + 1 = 1 + 1$ *is a bad example, since it illustrates the rule* $a = a$*. But* $2 + 1 = 1 + 2$ *is an excellent example, since you can actually prove it:* $2 + 1 = (1 + 1) + 1 = 1 + 1 + 1 = 1 + (1 + 1) = 1 + 2$*. It is a much better example than* $987 + 1989 = 1989 + 987$.' — Zeilberger, Opinion 65 (available at his website).

In mathematics, examples are very important, but not all of them are equally good. Intuitively, the more an example reflects the potential of a theorem, the better it is. In fact, if an example sufficiently represents the essence of a theorem, then it can be almost as instructive as the proof itself.

Mathematical teaching through examples has many endorsements, notably Babylonian mathematics, which mainly consisted of collections of examples (see Van der Waerden (10, Chapter 3)); or the so-called **Gelfand's principle**, which asserts that every new definition/result in a mathematical text should be accompanied by a nontrivial but minimally simple example.

Baaz's generalization method (see Baaz (1)) is based on this idea of extracting general information from a concrete example: given an example (i.e. an instance) E of a certain universal sentence T, it generates another universal sentence $t(E)$, with its corresponding proof. A subsequent comparison between T and $t(E)$ may show how well E 'approximates' T ($t(E)$ might be a particularization, a generalization or an equivalent form of T). The ideal scope of this algorithm are problems that are solved only for particular cases. That is to say, problems in which T is conjectural, incomplete or simply unknown; but instances E are proved: $t(E)$ may be then (instanced to) a partial answer to the question. Two examples of this kind of problem are the **kissing number problem**, which is only solved for certain dimensions (see Weisstein (17)); and the **rational distance problem**, which is only solved for geometric configurations (see Weisstein (19)).

2.3 Description

Baaz's generalization method generalizes proofs of universal sentences. Table 1 provides a succinct explanation of this procedure (see Baaz (1) for a fully detailed explanation), accompanied by an application to a proof of $641 \mid 2^{32}+1$ (which is due to Bennet and Kraïtchik (see Křížek et al. (7, p. 39)) (note that $2^{32}+1$, with ten digits, is a relatively 'big' number and it made sense to search for a small proof that 641 divides it; especially in times in which there were no computers). Although it is a quantifier-free sentence, it is sufficient to explain the algorithm because in any proof of a universal sentence the variables are fixed from the very beginning and therefore they can be treated as constants. In other words, free parameters are allowed; albeit this is not the case of the example shown.

The main interest of this method is possibly the fact that it allows to perform generalizations in a systematic way by keeping track of (a large amount of) variables that occur simultaneously rather than sequentially, task that is typically difficult for a human.

Note that step 3 allows certain freedom: the existence of the unifications simply follows from the existence of the proof to be generalized; however, they are not necessarily unique, and different outputs can be obtained depending on the chosen unification. For example, the formulas $uv = w$ and $x^y = z$ can be unified as $\alpha\beta = \gamma$ by taking $(u, v, w, x^{y-t}, x^t, z) \mapsto (\alpha, \beta, \gamma, \alpha, \beta, \gamma)$ or as $\alpha^\beta = \gamma$ by taking $(u, v, w, x, y, z) \mapsto (\alpha^{\beta-\delta}, \alpha^\delta, \gamma, \alpha, \beta, \gamma)$.

2.4 Two possible extensions

A usual kind of generalization to which Baaz's generalization method might be extended is the generalization of relations. It can be achieved by considering relations as (quantifiable) variables (i.e. by working with second-order logic) and then applying the procedure. For example (this example is inspired by Ramanujan's problem '*Solve* $x = \sqrt{1+2\sqrt{1+3\sqrt{1+4\sqrt{\ldots}}}}$', see Berndt et al. (2)),

$$\begin{aligned}
&`\underbrace{n(n+2) = n\sqrt{1+(n+1)(n+3)}}_{[0]} \overset{[0]}{\Rightarrow}\\
&n(n+2) = n\sqrt{1+(n+1)\sqrt{1+(n+2)(n+4)}} \overset{[0]}{\Rightarrow}\\
&n(n+2) = n\sqrt{1+(n+1)\sqrt{1+(n+2)\sqrt{1+(n+3)(n+5)}}}',
\end{aligned}$$

could be generalized as

$$\begin{aligned}
&`\underbrace{n(n+2) = nG((n+1)(n+3))}_{[0]} \overset{[0]}{\Rightarrow}\\
&n(n+2) = nG((n+1)G((n+2)(n+4))) \overset{[0]}{\Rightarrow}\\
&n(n+2) = nG((n+1)G((n+2)G((n+3)(n+5))))';
\end{aligned}$$

by abstracting the unary operation (i.e. sequence) $(\sqrt{1+n})_{n=0}^{\infty}$ into any unary operation G satisfying the corresponding condition [0].

Another one is the generalization of conjunctions/disjunctions. For example (here the notation '$a \underset{n}{\equiv} b$' was preferred over the standard one '$a \equiv b \pmod n$' for the sake of compactness),

$$`\left[2n \underset{8}{\equiv} 0 \vee 2n \underset{8}{\equiv} 2 \vee 2n \underset{8}{\equiv} 4 \vee 2n \underset{8}{\equiv} 6\right]'$$

TABLE 1. Description of Baaz's generalization method.

Baaz's generalization method	Example
Input: proof of a universal sentence (in the form of a tree of quantifier-free formulas) (it may be then necessary to first perform some techniques (such as Skolemizations) on the inputed nodes to ensure that they indeed become quantifier-free).	Input: • $641 \mid \underbrace{5^4+2^4}_{641} \Rightarrow 641 \mid 5^4 2^{28}+2^{32} \Rightarrow 641 \mid (5^4 2^{28}-1)+(2^{32}+1)$. [0] • $\underbrace{5\cdot 2^7+1}_{641} \mid 5^4 2^{28}-1 \overset{[0]}{\Rightarrow} 641 \mid 2^{32}+1$. □
1. For every leaf (i.e. node without predecessors), replace every constant with a variable (without repeating them) (there is no need to keep the operations, but keep the rest of the relations).	1. • $641 \mid 641 \mapsto a_0 \mid b_0$. • $5\cdot 2^7+1 \mid 5^4 2^{28}-1 \mapsto c_0 \mid d_0$.
2. For every implication, replace every constant with a variable (without repeating them) (keep the operations that are necessary to justify the step and the rest of the relations).	2. • $[641 \mid 5^4+2^4 \Rightarrow 641 \mid 5^4 2^{28}+2^{32}] \mapsto [a_1 \mid b_1+c_1 \Rightarrow a_1 \mid b_1 d_1+c_1 d_1]$. • $[641 \mid 5^4 2^{28}+2^{32} \Rightarrow 641 \mid (5^4 2^{28}-1)+(2^{32}+1)] \mapsto [a_2 \mid b_2+c_2 \Rightarrow a_2 \mid (b_2-d_2)+(c_2+d_2)]$. • $[[641 \mid (5^4 2^{28}-1)+(2^{32}+1) \wedge 641 \mid 5^4 2^{28}-1] \Rightarrow 641 \mid 2^{32}+1] \mapsto [[a_3 \mid b_3+c_3 \wedge a_3 \mid b_3] \Rightarrow a_3 \mid c_3]$.
3. Minimize the number of variables, by simultaneously unifying all pairs of formulas that are assigned to the same node (all the relations (and, in particular, all the operations) must be kept).	3. • $\{a_0 \mid b_0, a_1 \mid b_1+c_1\} \mapsto A \mid D+B$. • $\{a_1 \mid b_1 d_1+c_1 d_1, a_2 \mid b_2+c_2\} \mapsto A \mid DC+BC$. • $\{a_2 \mid (b_2-d_2)+(c_2+d_2), a_3 \mid b_3+c_3\} \mapsto A \mid (DC-E)+(BC+E)$. • $\{c_0 \mid d_0, a_3 \mid b_3\} \mapsto A \mid DC-E$.
Output: a generalized proof (and, in particular, a generalized theorem, whose hypotheses are the generalized leaves and whose thesis is the generalized root).	Output: • $A \mid D+B \Rightarrow A \mid DC+BC \Rightarrow A \mid (DC-E)+(BC+E)$. [0] • $A \mid DC-E \overset{[0]}{\Rightarrow} A \mid BC+E$. □ (generalized theorem: if $A \mid D+B$ and $A \mid DC-E$, then $A \mid BC+E$).

could be generalized as

$$\text{`}\left[(i+1)n \underset{(i+1)^3}{\equiv} (i+1)0 \vee \ldots \vee (i+1)n \underset{(i+1)^3}{\equiv} (i+1)((i+1)^2-1)\right]\text{'}.$$

3 Study of the factors of Fermat numbers

3.1 Some properties of Fermat numbers

Given a nonnegative integer n, the value $2^{2^n}+1$ is known as the n-th **Fermat number**. For example, $2^{32}+1$, which has been mentioned in Section 2, is the fifth Fermat number.

Due to their fast growth (only the first twelve ones are fully factored so far), to calculate factors of Fermat numbers is challenging; and analyzing their properties is consequently interesting. Notably, the so-called **Pépin's test** (see Weisstein (18)) has been used in order to demonstrate the compositeness of $2^{2^{20}}+1$ (see Young & Buell (20)) and of $2^{2^{24}}+1$ (see Crandall et al. (3)); but no prime factor is currently known.

Many results about factors of Fermat numbers assume them to be in the form $m2^{n+2}+1$ because of Theorem 1 (see Lucas (8)).

THEOREM 1
Given an integer $n>1$ and a factor r of the n-th Fermat number, there exists a nonnegative integer m such that $m2^{n+2}+1=r$.

For example, $5\cdot 2^{5+2}+1$ is a factor of the fifth Fermat number (see Table 1).

Proposition 2 (see Weisstein (13)) states another property of Fermat numbers that is necessary later on.

PROPOSITION 2
If n is a nonnegative integer, then $\prod_{k=0}^{n}(2^{2^k}+1)$ equals $2^{2^{n+1}}-1$.

For example, $(2^{2^0}+1)(2^{2^1}+1)=15=2^{2^{1+1}}-1$.

Finally, Proposition 3 reveals a connection with Ramanujan's problem above. Let F be the sequence $(k\sqrt{1+(k+1)(k+3)})_{k=0}^{\infty}$.

PROPOSITION 3
If n is a nonnegative integer, then $\prod_{k=0}^{n}(2^{2^k}+1)$ equals $F^{n+1}(1)$.

PROOF. By induction on n. Note that $F(k)$ is equal to $k(k+2)$, for every nonnegative integer k.
Case 0 The number $\prod_{k=0}^{0}(2^{2^k}+1)$ is equal to 3 or, equivalently, to $1(1+2)$.
Case n Induction hypothesis.
Case $n+1$ The number $F^{n+2}(1)$ is equal to $F(F^{n+1}(1))$ or, equivalently, to $F(\prod_{k=0}^{n}(2^{2^k}+1))$ (by applying the induction hypothesis). This value is equal to $F(2^{2^{n+1}}-1)$ (by applying Proposition 2); which is equal to $(2^{2^{n+1}}-1)(2^{2^{n+1}}+1)$ or, in other words, to $\prod_{k=0}^{n+1}(2^{2^k}+1)$ (by applying again Proposition 2). □

For example, $(2^{2^0}+1)(2^{2^1}+1)=15=3\sqrt{1+(3+1)(3+3)}=F(3)=F(1\sqrt{1+(1+1)(1+3)})=F(F(1))=F^{1+1}(1)$.

3.2 Covers

Let the **cover** of a pair of integers $a>1$ and $b>1$ be the set of pairs of nonnegative rationals x and y such that a^x+b^y is (an integer) multiple of $ab+1$. Note that, if x (resp., y) is positive, then its denominator divides the maximum positive integer m such that a (resp., b) is an m-th power.

For example, $(4,4/7)$ belongs to the cover of 5 and 2^7 because $5\cdot 2^7+1$ divides (and, in fact, equals) 5^4+2^4 (see Table 1).

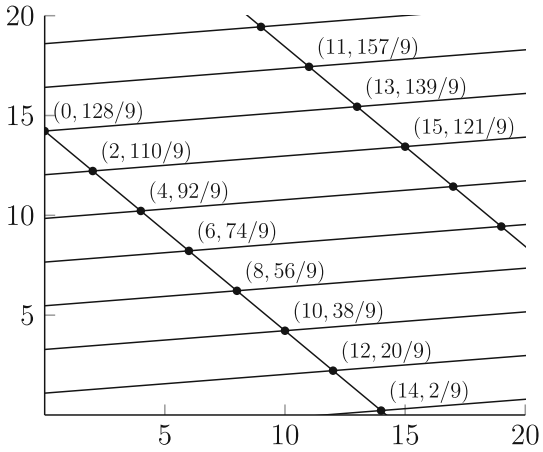


FIGURE 1. Some points of the cover of 116503103764643 and 2^{7+2}.

Pairs of integers whose cover contains the element $(2, 2)$ already appeared in the literature. For instance, Problem 6 at the 29th International Mathematical Olympiad (see Engel (5, p. 127)) asked the contestants to prove that, if a and b are positive integers such that $ab + 1$ divides $a^2 + b^2$, then $(a^2 + b^2)/(ab + 1)$ is a perfect square.

The computational visualization of subsets of covers of some pairs of small integers led to the following experimental result.

CONJECTURE 4
For every two integers $a > 1$ and $b > 1$, there exist bivariate linear polynomials with rational coefficients p and q such that any element of the cover of a and b equals $(p(u, v), q(u, v))$, for some integers u and v.

Geometrically, Conjecture 4 means that covers are determined by the intersection of two families of parallel straight lines: indeed, the system of linear equations $\begin{cases} x = p(u, v) \\ y = q(u, v) \end{cases}$ is equivalent to $\begin{cases} y = \alpha x + \beta + \gamma u \\ y = \delta x + \epsilon + \phi v \end{cases}$ for certain rationals α, β, γ, δ, ϵ and ϕ. See for instance Figure 1, in which some points of the cover of 116503103764643 and 2^{7+2} are displayed (the reason to choose this example was the fact that $116503103764643 \cdot 2^{7+2} + 1$ is a factor of the seventh Fermat number).

Recall now the following result about summation of geometric series, Proposition 5 (see Weisstein (15)).

PROPOSITION 5
If r is a complex number different than 1 and n is a nonnegative integer, then $\sum_{k=0}^{n}(r^k) = (r^{n+1} - 1)/(r - 1)$.

In regard to Conjecture 4, Proposition 6 provides some insightful information.

PROPOSITION 6
If a, b and k are positive integers such that $a > 1$, $b > 1$ and k is odd; and (x, y) is an element of the cover of a and b, then (kx, ky) is also an element of the cover of a and b.

PROOF. It suffices to check that the value $(a^{kx} + b^{ky})/(a^x + b^y)$ is an integer: indeed, it is equal to $b^{(k-1)y}((-a^x/b^y)^k - 1)/(-a^x/b^y - 1)$ (by applying that k is odd) or, in other words, to $b^{(k-1)y} \sum_{i=0}^{k-1}((-a^x/b^y)^i)$ (by applying Proposition 5); which is clearly an integer. □

For example, $(4, 4/7)$ has been shown to be an element of the cover of 5 and 2^7; so $(12, 12/7)$ must be another of its elements. And indeed, $(5^{12} + 2^{12})/(5 \cdot 2^7 + 1)$ equals 380881.

Let f be the sequence $(\lfloor 2^{n-1}/(n+2)\rfloor)_{n=0}^{\infty}$. The generalization obtained in Table 1 can be refined into Theorem 7.

THEOREM 7
If m, n and r are nonnegative integers such that $m > 1$, $r \leq f(n)$ and $(2r, 2^n/(n+2) - 2r)$ belongs to the cover of m and 2^{n+2}, then $m2^{n+2} + 1$ is a factor of the n-th Fermat number.

PROOF. If r equals 0, then the result is immediate. Assume therefore that r is positive and let $A = m2^{n+2} + 1$, $B = 2^{2^n - 2r(n+2)}$, $C = 2^{2r(n+2)}$, $D = m^{2r}$ and $E = 1$. The number $\sum_{k=0}^{2r-1}((-m2^{n+2})^k)$ equals $(DC - E)/(-A)$ (by applying Proposition 5), so A divides $DC - E$ and, in addition, A divides $D + B$ (by hypothesis). Hence, A divides $BC + E$ (by the generalization obtained in Table 1); that is to say, $m2^{n+2} + 1$ is a factor of the n-th Fermat number. □

For example, it is easier to check that $1184 \cdot 2^{9+2} + 1$ is a factor of $1184^{2 \cdot 12} + 2^{2^9 - 2 \cdot 12(9+2)}$ (75 digits) than to check that it is a factor of the ninth Fermat number (155 digits).

The assumptions $m > 1$ and $r \leq f(n)$ in Theorem 7 are necessary to respect the conditions of the definition of cover (note that if r were strictly greater than $f(n)$, then $2^n/(n+2) - 2r$ would be negative).

Baaz (1, Theorem 15) obtained Proposition 8, which is an immediate particularization of Theorem 7, as a result of generalizing a different proof of $641 \mid 2^{32} + 1$ (which is due to Kraïtchik, see Křížek et al. (7, p. 39)).

PROPOSITION 8
If m, n and r are nonnegative integers such that $m > 1$, $r \leq f(n)$ and $m2^{n+2} + 1$ equals $m^{2r} + 2^{2^n - 2r(n+2)}$, then $m2^{n+2} + 1$ is a factor of the n-th Fermat number.

For example, $5 \cdot 2^7 + 1$ is equal to $5^{2 \cdot 2} + 2^{2^5 - 2 \cdot 2(5+2)}$ and a factor of the fifth Fermat number.

Note that Theorem 7 is equivalent to Theorem 9 (by taking $u = f(n) - r$).

THEOREM 9
If m, n and u are nonnegative integers such that $m > 1$, $u \leq f(n)$ and $(-2u + (2f(n) - 1)1 + 1, 2u + (2^n/(n+2) - 2f(n) + 1)1 - 1)$ belongs to the cover of m and 2^{n+2}, then $m2^{n+2} + 1$ is a factor of the n-th Fermat number.

Recall Theorem 10, also known as **binomial theorem** (see Weisstein (12)).

THEOREM 10
If x and y are complex numbers and n is a nonnegative integer, then $(x+y)^n$ equals $\sum_{k=0}^{n}\left(\binom{n}{k}x^{n-k}y^k\right)$.

Theorem 9 leads to the main result of the article, Theorem 11.

THEOREM 11
Given integers $m > 1$ and $n > 3$, $m2^{n+2} + 1$ is a factor of the n-th Fermat number if and only if the cover of m and 2^{n+2} contains all the pairs of the form $(-2u + (2f(n) - 1)v + 1, 2u + (2^n/(n + 2) - 2f(n) + 1)v - 1)$, where u is an integer such that $(-2^{n-1}/(n+2) + f(n) - 1/2)v + 1/2 \leq u \leq (f(n) - 1/2)v + 1/2$ and v is a positive integer.

PROOF. Note that $2u + (2^n/(n+2) - 2f(n) + 1)v - 1$ and $-2u + (2f(n) - 1)v + 1$ are nonnegative, which implies that $(-2^{n-1}/(n+2) + f(n) - 1/2)v + 1/2 \leq u \leq (f(n) - 1/2)v + 1/2$. Their sum, $2^n v/(n+2)$, is also nonnegative; so v is nonnegative. If v were equal to 0, u would be equal to 1/2 (by applying the previous bounds), which is impossible because u is an integer. Thus, v is positive.
$\Rightarrow$) By induction on v. Let $d = m2^{n+2} + 1$.
Case 1 Note that, in this case, $u \leq f(n)$. If u equals $f(n)$, then Case 1 is equivalent to the hypothesis that d is a factor of the n-th Fermat number. Assume therefore $u < f(n)$. Since d is a factor of the n-th Fermat number, d is also a factor of

$$2^{2^n} + 1 + \sum_{k=0}^{2(f(n)-u)-1} \left(\binom{2(f(n)-u)}{k} d^{2(f(n)-u)-k} (-1)^k \right);$$

which equals $2^{2^n} + (d-1)^{2(f(n)-u)}$ (by applying Theorem 10). Hence, d divides $2^{2^n - 2(f(n)-u)(n+2)} + m^{2(f(n)-u)}$ (by applying that d is odd); that is to say, $(-2u + (2f(n) - 1)1 + 1, 2u + (2^n/(n+2) - 2f(n) + 1)1 - 1)$ belongs to the cover of m and 2^{n+2}.
Case v Induction hypothesis.
Case $v+1$ The number $(2^{n+2})^{2u+(2^n/(n+2)-2f(n)+1)(v+1)-1}$ is equal to $(2^{n+2})^{2u+(2^n/(n+2)-2f(n)+1)v-1}(2^{n+2})^{2^n/(n+2)-2f(n)+1}$; which is congruent to $-m^{-2u+(2f(n)-1)v+1}(2^{n+2})^{2^n/(n+2)-2f(n)+1} \pmod d$ (by induction hypothesis). It suffices then to check that $(2^{n+2})^{2^n/(n+2)-2f(n)+1}$ is congruent to $m^{2f(n)-1} \pmod d$ (it is an integer because $n > 3$). And indeed, $(2^{n+2})^{2^n/(n+2)-2f(n)+1}$ is equal to $(2^{n+2})^{2\cdot 0+(2^n/(n+2)-2f(n)+1)1-1}2^{n+2}$, which is congruent to $-m^{-2\cdot 0+(2f(n)-1)1+1}2^{n+2} \pmod d$ (by applying Case 1). This number equals $-m^{2f(n)-1}(m2^{n+2})$, which is congruent to $m^{2f(n)-1} \pmod d$.
$\Leftarrow$) The particular case in which $u = f(n)$ and $v = 1$ yields that $(0, 2^n/(n+2))$ belongs to the cover of m and 2^{n+2} or, equivalently, that $m2^{n+2} + 1$ is a factor of the n-th Fermat number. □

For example, $(15, 121/9)$ (i.e. $(-2 \cdot 6 + (2f(7) - 1)2 + 1, 2 \cdot 6 + (2^7/(7+2) - 2f(7) + 1)2 - 1)$) belongs to the cover of 116503103764643 and 2^{7+2} (see Figure 1).

Proposition 12, originally conjectured by the author and later extended and proved by Wang (see Sauras-Altuzarra (9, Theorem 2.3 and Lemma 2.4)), can be now obtained from Theorem 11. Recall that the **dyadic valuation** of a positive integer n, denoted by $\nu_2(n)$, is the maximum nonnegative integer v such that 2^v divides n (see the Encyclopedia of Mathematics (11)). For example, the dyadic valuation of 12 is 2.

PROPOSITION 12
If j, m and n are positive integers such that $m > 1$, $n > 3$ and $m2^{n+2} + 1$ is a factor of the n-th Fermat number, then it also divides $m^{2^{n-\nu_2(n+2)}(2j-1)} + 1$ and $2^{2^{n-\nu_2(n+2)}(2j-1)(n+2)} + 1$.

PROOF. Let $v = (2j-1)(n+2)/2^{\nu_2(n+2)}$, $u_2 = (f(n) - 1/2)v + 1/2$ and $u_1 = u_2 - 2^{n-1}v/(n+2)$ (note that u_1 and u_2 satisfy the bounds from the statement of Theorem 11; in fact, they are coincident). The value v is an odd integer, so u_2 is an integer. In addition, $\nu_2(n+2) \leq n-1$ (indeed, even if $n+2$ were a r-th power of 2 for some integer $r > 2$, then $\nu_2(n+2) = r \leq 2^r - 3 = n - 1$), so $2^{n-1}v/(n+2)$ is an integer and consequently u_1 is an integer too. The value $m2^{n+2} + 1$ is a factor of the n-th Fermat number, so $(-2u_1 + (2f(n) - 1)v + 1, 2u_1 + (2^n/(n+2) - 2f(n) + 1)v - 1)$ and $(-2u_2 + (2f(n) - 1)v + 1, 2u_2 + (2^n/(n+2) - 2f(n) + 1)v - 1)$ belong to the cover of m and 2^{n+2} (by applying Theorem 11) or, equivalently, $(2^{n-\nu_2(n+2)}(2j-1), 0)$ and $(0, 2^{n-\nu_2(n+2)}(2j-1))$

belong to the cover of m and 2^{n+2}. In other words, $m2^{n+2}+1$ divides $m^{2^{n-\nu_2(n+2)}(2j-1)}+1$ and $2^{2^{n-\nu_2(n+2)}(2j-1)(n+2)}+1$. □

For example, $1071 \cdot 2^{6+2}+1$, which is a factor of the sixth Fermat number, is also a factor of $1071^{2^{6-\nu_2(6+2)}(2\cdot 1-1)}+1$ and of $2^{2^{6-\nu_2(6+2)}(2\cdot 1-1)(6+2)}+1$.

3.3 Other generalizations

Recall Theorem 13, also called **Fermat's little theorem** (see Weisstein (14)).

THEOREM 13
If a is a positive integer and p is a prime that does not divide a, then p divides $a^{p-1}-1$.

Theorems 14 and 15 characterize the prime factors of a Fermat number and of the product of arbitrarily many initial Fermat numbers, respectively. They were initially obtained as sufficient conditions, after applying Baaz's generalization method to another proof of $641 \mid 2^{32}+1$ (which is due to Broda, see Dickson (4, Chapter XV)), and Wang later proved that they are also necessary (see OEIS A308695 and A332416).

THEOREM 14
Given integers $m>0$, $n>1$ and p such that p is prime and equal to $m2^{n+2}+1$, p divides the n-th Fermat number if and only if $(2^{2^n}+1)p$ does not divide $2^{p-1}-1$.

PROOF. $\Rightarrow$) The value p divides the n-th Fermat number. That is to say, -2^{2^n} is congruent to 1 (mod p); so $(-2^{2^n})^k$ is congruent to 1 (mod p), for every nonnegative integer k. Hence, $\sum_{k=0}^{4m-1}((-2^{2^n})^k)$ is congruent to $4m$ (mod p); i.e. $(2^{m2^{n+2}}-1)/(-2^{2^n}-1)$ is congruent to $4m$ (mod p) (by applying Proposition 5). Thus, p does not divide $(2^{m2^{n+2}}-1)/(-2^{2^n}-1)$ (by applying that $0<4m<p$); from which follows that $(2^{2^n}+1)p$ does not divide $2^{m2^{n+2}}-1$ or, in other words, that $(2^{2^n}+1)p$ does not divide $2^{p-1}-1$.
$\Leftarrow$) The value p is a prime factor of $2^{p-1}-1$ (by applying the fact that p is a prime that does not divide 2 and Theorem 13), $2^{2^n}+1$ also divides $2^{p-1}-1$ (because $2^{p-1}-1$ is equal to $2^{m2^{n+2}}-1$ or, equivalently, to $\sum_{k=0}^{m-1}((2^{2^{n+2}})^k)\prod_{k=0}^{n+1}(2^{2^k}+1)$ (by applying Proposition 2 and Proposition 5)), but $(2^{2^n}+1)p$ does not divide $2^{p-1}-1$; so p must divide the n-th Fermat number. □

For example, $(2^{2^5}+1)(5\cdot 2^{5+2}+1)$ does not divide $2^{5\cdot 2^5}-1$.

THEOREM 15
Given integers $m>0$, $n>1$, p and P such that p is prime, p equals $m2^{n+2}+1$ and P equals $\prod_{k=0}^{n+1}(2^{2^k}+1)$, p divides P if and only if Pp does not divide $2^{p-1}-1$.

PROOF. $\Rightarrow$) The value p divides P, which equals $2^{2^{n+2}}-1$ (by applying Proposition 2). That is to say, $2^{2^{n+2}}$ is congruent to 1 (mod p); so $(2^{2^{n+2}})^k$ is congruent to 1 (mod p), for every nonnegative integer k. Hence, $\sum_{k=0}^{m-1}((2^{2^{n+2}})^k)$ is congruent to m (mod p); i.e. $(2^{m2^{n+2}}-1)/(2^{2^{n+2}}-1)$ is congruent to m (mod p) (by applying Proposition 5). Thus, p does not divide $(2^{m2^{n+2}}-1)/(2^{2^{n+2}}-1)$ (by applying that $0<m<p$); from which follows that $p(2^{2^{n+2}}-1)$ does not divide $2^{m2^{n+2}}-1$ or, in other words, that Pp does not divide $2^{p-1}-1$ (by applying again Proposition 2).
$\Leftarrow$) The value p is a prime factor of $2^{p-1}-1$ (by applying the fact that p is a prime that does not divide 2 and Theorem 13), P also divides $2^{p-1}-1$ (because $2^{p-1}-1$ is equal to $2^{m2^{n+2}}-1$ or,

equivalently, to $\sum_{k=0}^{m-1}((2^{2^{n+2}})^k)P$ (by applying Proposition 2 and Proposition 5)), but Pp does not divide $2^{p-1}-1$; so p must divide P. □

For example, $1\cdot 2^{2+2}+1$ equals $2^{2^2}+1$ and $\prod_{k=0}^{1+1}(2^{2^k}+1)(1\cdot 2^{2+2}+1)$ does not divide $2^{2^{2+2}}-1$.

See Sauras-Altuzarra (9) for other applications of Baaz's generalization method to the study of the factors of Fermat numbers.

Acknowledgements

The author is grateful to the anonymous referees for their interesting comments, among which include Proposition 6.
This research was partly supported by FWF Austria, project numbers I 4427 and P 31955.

References

[1] M. Baaz. Note on the generalization of calculations. *Theoretical Computer Science*, **224**, 1–2, 1999. https://www.sciencedirect.com/science/article/pii/S0304397598003041.
[2] B. C. Berndt, R. L. Lamphere and B. M. Wilson. Chapter 12 of Ramanujan's second notebook: continued fractions. *Rocky Mountain Journal of Mathematics*, **15**, 235–310, 1985. https://doi.org/10.1216/RMJ-1985-15-2-235.
[3] R. E. Crandall, E. W. Mayer and J. S. Papadopoulos. The twenty-fourth Fermat number is composite. *Mathematics of Computation*, **72**, 1555–1572, 2003. https://www.ams.org/journals/mcom/2003-72-243/S0025-5718-02-01479-5/S0025-5718-02-01479-5.pdf.
[4] L. E. Dickson. *History of the Theory of Numbers*. Carnegie Institution of Washington, 1919.
[5] A. Engel. *Problem Solving Strategies*. Problem Books in Mathematics, Springer, 1998.
[6] A. G. Hamilton. *Logic for Mathematicians*. Cambridge University Press, 1978.
[7] M. Křížek, F. Luca and L. Somer. *17 Lectures on Fermat Numbers: From Number Theory to Geometry*. CMS Books in Mathematics. Springer, New York, 2001.
[8] É. Lucas. Théorèmes d'arithmétique. *Atti della Reale Accademia delle Scienze di Torino*, **13**, 271–284, 1878.
[9] L. Sauras-Altuzarra. Some properties of the factors of Fermat numbers. *The Art of Discrete and Applied Mathematics*. The Wilfried Imrich Issue (to appear). https://adam-journal.eu/index.php/ADAM/article/view/1473/1365
[10] B. L. Van der Waerden. *Science Awakening*. Oxford University Press, 1961.
[11] Various. P-adic valuation. *Encyclopedia of Mathematics*. https://encyclopediaofmath.org/index.php?title=P-adic_valuation
[12] E. W. Weisstein. Binomial Theorem. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/BinomialTheorem.html
[13] E. W. Weisstein. Fermat Number. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/FermatNumber.html
[14] E. W. Weisstein. Fermat's Little Theorem. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/FermatsLittleTheorem.html
[15] E. W. Weisstein. Geometric Series. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/GeometricSeries.html
[16] E. W. Weisstein. Goldbach Conjecture. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/GoldbachConjecture.html

[17] E. W. Weisstein. Kissing Number. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/KissingNumber.html
[18] E. W. Weisstein. Pépin's Test. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/PepinsTest.html
[19] E. W. Weisstein. Rational Distance Problem. *MathWorld—A Wolfram Web Resource*. https://mathworld.wolfram.com/RationalDistanceProblem.html
[20] J. Young and D. A. Buell. The twentieth Fermat number is composite. *Mathematics of Computation*, **50**, 261–263, 1988. https://www.ams.org/journals/mcom/1988-50-181/S0025-5718-1988-0917833-8/S0025-5718-1988-0917833-8.pdf.

Received 10 June 2022

3.3 Related work

We now present some other results and problems which are related to covers, Fermat numbers, point-lattices and computation of large prime numbers.

3.3.1 Covers

This work consists of further results on covers, distinguishing among general results, results which are related to the factorization of Fermat numbers and results in which the analyzed points have special forms.

3.3.1.1 General results

Theorem 3.3.1.1 (i.e. Proposition 6 of Article C in Section 3.2) indicated that any non-empty cover contains infinitely many points, but it was still unknown if every cover is non-empty.

Theorem 3.3.1.1. *Let a, b and k be any three positive integers such that a and b exceed one and k is odd. Let (x, y) be any point of $\mathcal{C}(a, b)$. Then (kx, ky) is also a point of $\mathcal{C}(a, b)$.*

For example, if k is any odd positive integer, then the point $(4k, 4k/7)$ belongs to $\mathcal{C}(5, 128)$.

The **Euler phi-function**, which is denoted by φ, is the unary operation on the set of positive integers which maps every positive integer n into the number of positive integers that do not exceed n and are coprime with n (see Rosen [15, Section 6.3]).

For example, $\varphi(9)$ and $\varphi(25)$ equal 6 and 20 respectively.

Theorem 3.3.1.2 is known as **Euler's theorem** (see Rosen [15, Theorem 6.14]).

Theorem 3.3.1.2. *If a and m are any two integers such that m exceeds one and is coprime with a, then $a^{\varphi(m)}$ is congruent to one modulo m.*

For example, $2^{\varphi(9)}$, which equals 64, is congruent to one modulo nine.

René Schoof applied Theorem 3.3.1.2 in order to obtain Theorem 3.3.1.3 (pers. comm.), which shows in particular that indeed no cover is empty.

Theorem 3.3.1.3. *If a and b are any two integers exceeding one, then*

$$\left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \mathcal{L}\left(\begin{bmatrix} -2 \\ 2 \end{bmatrix}, \begin{bmatrix} \varphi(ab+1) \\ 0 \end{bmatrix}\right)\right) \cap \mathbb{Q}^2_{\geq 0} \subseteq \mathcal{C}(a, b).$$

Proof. First notice that one equals $\gcd(a, a+1)$, i.e. $\gcd(n, a(b-1)+a+1)$ or, equivalently, $\gcd(a, ab+1)$. Now, let i and j be positive integers such that $1-2i+\varphi(ab+1)j \geq 0$. Then $a^{1-2i+\varphi(ab+1)j} + b^{-1+2i}$ is an integer congruent to $a^{-1+2i}(a^{1-2i}(a^{\varphi(ab+1)})^j + b^{-1+2i})$ and hence congruent to $1+(ab)^{-1+2i}$ modulo $ab+1$ (by applying Euler's theorem (i.e. Theorem 3.3.1.2), which is applicable because a and $ab+1$ are coprime). In other words, it is congruent to $1+(-1)^{-1+2i}$ modulo $ab+1$; which is zero. □

For example, $\varphi(18 \cdot 29 + 1)$ equals 522; and indeed $(521, 1)$ belongs to $\mathcal{C}(18, 29)$.

Still, some important questions about covers remain open, specially Conjecture 3.3.1.4 (i.e. Conjecture 4 of Article C in Section 3.2).

Conjecture 3.3.1.4. *For every two integers a and b exceeding one, there is some vector $\vec{u}$ of $\mathbb{Q}^2$ and some $\mathbb{Q}$-basis $(\vec{v}, \vec{w})$ of $\mathbb{Q}^2$ such that $(\vec{u} + \mathcal{L}(\vec{v}, \vec{w})) \cap \mathbb{Q}^2_{\geq 0}$ equals $\mathcal{C}(a, b)$.*

Given any two coprime integers $a \neq 0$ and $m > 1$, the **multiplicative order** of a modulo m, which is denoted by $\mathrm{ord}_m(a)$, is the minimum positive integer k such that a^k is congruent to one modulo m (note that it exists because of Euler's theorem, i.e. Theorem 3.3.1.2) (cf. Rosen [15, Section 9.1]).

And a **primitive root** modulo any integer m exceeding one is any non-negative integer r which is coprime with m and for which $\mathrm{ord}_m(r)$ equals $\varphi(m)$ (cf. Rosen [15, Section 9.1]).

For example, 3 and 8 are primitive roots modulo 25 because they are coprime with 25 and their multiplicative order modulo 25 is $\varphi(25)$ (that is, 20).

Given any three integers $m > 1$, $n > 0$ and $r \geq 0$ such that m is coprime with n and r is a primitive root modulo m, there is a unique $k \in \{1, \ldots, \varphi(m)\}$, which is known as the **discrete logarithm** of n to the base r modulo m, such that r^k is congruent to n modulo m (cf. Crandall & Pomerance [2, Subsection 6.4.1] and Rosen [15, Section 9.4]).

For example, the discrete logarithms of 24 and of 8 to the base 3 modulo 25 are 9 and 10 respectively because $3^{10} \equiv 24 \pmod{25}$ and $3^9 \equiv 8 \pmod{25}$.

By means of the previous concepts, Mabud Sarkar obtained another partial answer to Conjecture 3.3.1.4, Theorem 3.3.1.5 (pers. comm.).

Theorem 3.3.1.5. *If a and b are any two primitive roots modulo $ab+1$ exceeding one, and c and d are the discrete logarithms of ab and b to the base a modulo $ab+1$*

respectively, then

$$\left(\begin{bmatrix} c \\ 0 \end{bmatrix} + \mathcal{L}\left(\begin{bmatrix} 2c \\ 0 \end{bmatrix}, \begin{bmatrix} d \\ 1 \end{bmatrix}\right)\right) \cap \mathbb{Q}^2_{\geq 0} \subseteq \mathcal{C}(a,b).$$

Proof. Let i and j be any two non-negative integers. Then $-1 \equiv (-1)^{2i+1} \equiv (ab)^{2i+1} \equiv (a^c)^{2i+1} \pmod{ab+1}$, so $-(a^d)^j \equiv a^{c(2i+1)+dj} \pmod{ab+1}$ or, equivalently, $0 \equiv a^{c(2i+1)+dj} + b^j \pmod{ab+1}$. □

For example, if $a = 3$ and $b = 8$, then a and b are primitive roots modulo $ab+1$; and the discrete logarithms of ab and b to the base a modulo $ab+1$ are 10 and 9 respectively. Theorem 3.3.1.5 ensures then that

$$\left(\begin{bmatrix} 10 \\ 0 \end{bmatrix} + \mathcal{L}\left(\begin{bmatrix} 20 \\ 0 \end{bmatrix}, \begin{bmatrix} 9 \\ 1 \end{bmatrix}\right)\right) \cap \mathbb{Q}^2_{\geq 0} \subseteq \mathcal{C}(a,b).$$

Other pairs (a,b) satisfying the conditions of Theorem 3.3.1.5 are $(2,2)$, $(2,6)$, $(3,3)$, $(6,2)$, $(6,10)$, $(8,3)$ and $(10,6)$.

Daniele Parisse observed the following connection with other area of number theory (pers. comm.). Let Pillai$(a,b,c,r,s;u,v,x,y)$ denote the expression $(-1)^u ra^x + (-1)^v sb^y - c$, where all the involved parameters are positive integers. When a, b, c, r and s are given, and a and b exceed one, the equation Pillai$(a,b,c,r,s;u,v,x,y) = 0$ is known as the **generalized Pillai equation** (see Scott & Styer [16]). Proposition 3.3.1.6 is then immediate.

Proposition 3.3.1.6. *Given any four positive integers a, b, x, y such that a and b exceed one, the point (x,y) belongs to $\mathcal{C}(a,b)$ if and only if there is some positive integer k such that* Pillai$(a,b,k(ab+1),1,1;2,2,x,y) = 0$.

3.3.1.2 The case of the factors of Fermat numbers

Proposition 3.3.1.7, whose proof is essentially due to Jinyuan Wang (pers. comm.), determines all the solutions of the Diophantine equation from Proposition 8 of Article C in Section 3.2. Matthias Baaz reported that apparently Georg Kreisel had another unpublished proof of Proposition 3.3.1.7 (pers. comm.).

Proposition 3.3.1.7. *Given any three non-negative integers $m > 1$, n and $r \leq \lfloor 2^{n-1}/(n+2) \rfloor$ such that*

$$m^{2r} + 2^{2^n - 2r(n+2)} = m2^{n+2} + 1, \tag{3.1}$$

either $r = 0$, in which case $n > 1$ and $m = 2^{2^n - n - 2}$, or $r = 2$, in which case $(m,n) = (5,5)$.

Proof. Let us discuss the possible cases.

Case 1: $r = 0$ Then $1 + 2^{2^n} = m2^{n+2} + 1$ (by Equality 3.1), which does not hold if $n < 2$ (because $m > 1$) and implies that $m = 2^{2^n-n-2}$ otherwise.

Case 2: $r > 0$

• Case 2.1: $2^{2^n-2r(n+2)} = 1$ Then $2^n - 2r(n+2) = 0$, so $r = 2^{n-1}/(n+2)$ (because n is non-negative). Note that $n > 2$ (because r is a non-negative integer). Equality 3.1 implies that $m^{2^n/(n+2)} = m2^{n+2}$, and consequently $m = 2^{(n+2)^2/(2^n-n-2)}$ (because $m > 1$): impossible, because $(n+2)^2/(2^n - n - 2)$ is not a positive integer if $n > 2$.

• Case 2.2: $2^{2^n-2r(n+2)} > 1$

• • Case 2.2.1: $m = 2$ Then $2^{2r} + 2^{2^n-2r(n+2)} = 2^{n+3} + 1$ (by Equality 3.1), so 0 belongs to $\{2r, 2^n - 2r(n+2)\}$ (because $2^{n+3} + 1$ is odd) and consequently $2^n - 2r(n+2) = 0$ (because $r > 0$): impossible, because $2^{2^n-2r(n+2)} > 1$.

• • Case 2.2.2: $m > 2$

• • • Case 2.2.2.1: $n = 0$ Then $r = 0$ (because $r \leq \lfloor 2^{n-1}/(n+2) \rfloor$): impossible, because $r > 0$.

• • • Case 2.2.2.2: $n > 0$ We have that $2^{2^n-2r(n+2)} - 1 = m(2^{n+2} - m^{2r-1})$ (by Equality 3.1 and the condition $r > 0$), so $m(2^{n+2} - m^{2r-1}) > 0$ (because $2^{2^n-2r(n+2)} > 1$) and consequently $2^{n+2} > m^{2r-1}$ (because $m > 1$). Thus $2^{n+2} > 2^{2r-1}$ (because $m > 2$), so $n + 2 > 2r - 1$ or, equivalently, $r < (n+3)/2$. In addition, we have that $(2^{2^{n-1}-r(n+2)} - 1)(2^{2^{n-1}-r(n+2)} + 1) = m(2^{n+2} - m^{2r-1})$ (because $n > 0$), so $2^{2^{n-1}-r(n+2)} - 1 < \max(m, 2^{n+2} - m^{2r-1})$ (because, if a, b, c, d are any four non-negative integers such that $a < b$ and $ab = cd$, then $a < \max(c, d)$) and therefore $n \leq 6$ (see the cases below). And an easy computation reveals that, if $n \leq 6$, then no integer $m > 2$ satisfies Equality 3.1, with the exception of 5 when $(n, r) = (5, 2)$.

• • • • Case 2.2.2.2.1: $2^{2^{n-1}-r(n+2)} \leq m$ We have seen that $2^{n+2} > m^{2r-1}$, which in this case implies that $2^{n+2} > 2^{(2^{n-1}-r(n+2))(2r-1)}$ and therefore $n+2 > 2^{n-1} - r(n+2)$ (because $r > 0$). Then $(r+1)(n+2) > 2^{n-1}$ and hence $((n+3)/2+1)(n+2) > 2^{n-1}$ (because $r < (n+3)/2$); which only holds if $n \leq 6$.

• • • • Case 2.2.2.2.2: $2^{2^{n-1}-r(n+2)} \leq 2^{n+2} - m^{2r-1}$ Then $2^{2^{n-1}-r(n+2)} + m^{2r-1} \leq 2^{n+2}$, so $2^{2^{n-1}-r(n+2)} + 2^{2r-1} \leq 2^{n+2}$ (because $m > 2$) and it is easy to verify that this inequality only holds if $n \leq 6$. □

Conjecture 3.3.1.8, which is a slight modification of Theorem 3.0.0.1, also seems to be true.

Conjecture 3.3.1.8. *Given any two integers $m > 1$ and $n > 2$, the number $m2^{n+2} + 1$ is a factor of the n-th Fermat number if and only if $\mathcal{F}(n)$ equals $\mathcal{C}(m, 2^{n+2})$.*

For example, $5 \cdot 128 + 1$ and $52347 \cdot 128 + 1$ are the prime factors of the fifth Fermat number and apparently $\mathcal{C}(5, 128) = \mathcal{C}(52347, 128) = \mathcal{F}(5)$. The equality $\mathcal{C}(63, 128) = \mathcal{C}(65, 128)$ also seem to hold, although $63 \cdot 128 + 1$ and $65 \cdot 128 + 1$ do not factor any Fermat number (see OEIS A307843).

3.3.1.3 Points of special forms

Theorem 3.3.1.9, whose proof is immediate, is known as **Aurifeuillean factorization** (see Riesel [14, Appendix 6]) or **Lucas formula** (see Křížek et al. [11]).

Theorem 3.3.1.9. *If n is any non-negative integer, then the number $2^{4n+2} + 1$ equals $(2^{2n+1} - 2^{n+1} + 1)(2^{2n+1} + 2^{n+1} + 1)$.*

For example, $4 + 1$ equals $(2 - 2 + 1)(2 + 2 + 1)$.

As an application of Theorem 3.3.1.9, we get Proposition 3.3.1.10.

Proposition 3.3.1.10. *If n is any positive integer, then the point $(0, 4n + 2)$ belongs to $\mathcal{C}(4^n - 2^n, 2)$ and to $\mathcal{C}(4^n + 2^n, 2)$.*

Proof. The numbers $2^{2n+1} - 2^{n+1} + 1$ and $2^{2n+1} + 2^{n+1} + 1$ factor $2^{4n+2} + 1$ (by applying Theorem 3.3.1.9) or, in other words, the numbers $(4^n - 2^n)2 + 1$ and $(4^n + 2^n)2 + 1$ factor $1 + 2^{4n+2}$; which is equivalent to say that the point $(0, 4n + 2)$ belongs to $\mathcal{C}(4^n - 2^n, 2)$ and to $\mathcal{C}(4^n + 2^n, 2)$. □

For example, the point $(0, 6)$ belongs to $\mathcal{C}(2, 2)$ and to $\mathcal{C}(6, 2)$.

Note that, given any two integers $b \neq 1$ and $n \geq 2$, the number $((-b)^{n-1} - 1)/(b+1)$ is also an integer because it is equal to $-((-b)^{n-1} - 1)/((-b) - 1)$ or, equivalently, to $-\sum_{k=0}^{n-2}((-b)^k)$ (by applying Proposition 5 of Article C in Section 3.2).

Proposition 3.3.1.11. *If b and n are any two integers such that $b \geq 2$, $n \geq 3$, n is odd and $(b, n) \neq (2, 3)$, then*

$$(0, n) \in \mathcal{C}\left(\frac{(-b)^{n-1} - 1}{b + 1}, b\right).$$

Proof. The number $\sum_{k=0}^{n-1}((-b)^k)$ is an integer; and it is equal to

$$\frac{(-b)^n - 1}{(-b) - 1}$$

(by applying Proposition 5 of Article C in Section 3.2) or, equivalently, to $(1 + b^n)/(1 + b)$ (because n is odd). Therefore, $(1 + b^n)/(1 + b)$ is a factor of $1 + b^n$ and it equals

$$\frac{(-b)^{n-1} - 1}{b + 1} b + 1$$

(again because n is odd); so the thesis holds. □

For example, the point $(0, 3)$ belongs to $\mathcal{C}(2, 3)$.

The condition $(b, n) \neq (2, 3)$ in Proposition 3.3.1.11 was imposed to avoid the case $((-b)^{n-1} - 1)/(b + 1) = 1$.

In addition, Jinyuan Wang obtained Proposition 3.3.1.12 (pers. comm.).

Proposition 3.3.1.12. *If n is any integer exceeding one, then the point $(1, n)$ belongs to $\mathcal{C}(n, n + 2)$.*

Proof. By applying the binomial theorem (i.e. Theorem 10 of Article C in Section 3.2), the following equalities hold:

$$\frac{n^1 + (n + 2)^n}{n(n + 2) + 1} =$$

$$\frac{n + ((n + 1) + 1)^n}{(n + 1)^2} =$$

$$\frac{1}{(n + 1)^2} \left(n + \sum_{i=0}^{n} \left(\binom{n}{i} (n + 1)^i \right) \right) =$$

$$\frac{1}{(n + 1)^2} \left(n + 1 + n(n + 1) + \sum_{i=2}^{n} \left(\binom{n}{i} (n + 1)^i \right) \right) =$$

$$\frac{1}{(n + 1)^2} \left((n + 1)^2 + \sum_{i=2}^{n} \left(\binom{n}{i} (n + 1)^i \right) \right) =$$

$$1 + \sum_{i=2}^{n} \left(\binom{n}{i} (n + 1)^{i-2} \right),$$

which is an integer. □

For example, the point $(1, 11)$ belongs to $\mathcal{C}(11, 13)$. But note that the point $(1, n)$, where n is any integer exceeding one, may belong to other covers apart from $\mathcal{C}(n, n + 2)$; for example, $(1, 260)$ belongs to $\mathcal{C}(18, 29)$.

The **Legendre symbol** is the function from the Cartesian product of the set of integers with the set of odd primes to the set $\{-1, 0, 1\}$ which maps every pair (a, p) into the only element of the codomain that is congruent to $a^{(p-1)/2}$ modulo p; element which is denoted by $(a \mid p)$ (cf. Weisstein [25]).

For example, $(22 \mid 7)$ equals one because $22^3 \equiv 1 \pmod 7$.

The following result, Theorem 3.3.1.13, was conjectured by the author and proved by Jinyuan Wang (pers. comm.).

Theorem 3.3.1.13. *If n is any odd positive integer such that $2n + 1$ is prime, then the point (n, n) belongs to $\mathcal{C}(2, n)$.*

Proof. Let k be any non-negative integer such that $2k + 1$ equals n, which exists because n is an odd positive integer; and let $p = 2n + 1$.

The Legendre symbol is a completely multiplicative function on its left argument, so $((p-1)/2 \mid p)(-2 \mid p)$ is equal to $(1-p \mid p)$. And, by applying basic properties of the Legendre symbol, $(1-p \mid p) = (1 \mid p) = 1$; from which follows that $((p-1)/2 \mid p)$ is equal to $(-2 \mid p)$.

We want to show that -2^n (i.e. $-2^{(p-1)/2}$) is congruent to n^n (i.e. $((p-1)/2)^{(p-1)/2}$) modulo p, which is equivalent to $-(2 \mid p) = ((p-1)/2 \mid p)$ or, in other words, to $-(2 \mid p) = (-2 \mid p)$. And this equality is equivalent to $-2^{2k+1} \equiv (-2)^{2k+1} \pmod p$; which is clearly true. □

3.3.2 Factorization of near-square numbers

Given any two integers $n \geq 0$ and r, the n-th **near-square number** of shift r is the number $n^2 - r$ (cf. Weisstein [26]).

For example, if n is a positive integer, then the n-th Fermat number is a near-square number of shift -1 because it equals $(2^{2^{n-1}})^2 - (-1)$.

Vasile Brînzănescu observed that the equality $(bc - ad)^2 = 1$ from Theorem 2.2 of Article B in Section 3.1 resembles the definition of special linear group (pers. comm.). This observation led to Theorem 3.3.2.1 on the factorization of near-square numbers of shift -1, obtained in collaboration with Gergely Harcos.

Theorem 3.3.2.1. *Given any integer m and any prime p, the number p divides m^2+1 if and only if there exist Gaussian integers u and v such that $v\overline{v} = p \mid m^2 - \Re(uv)^2$ and*

$$\begin{bmatrix} \Im(u) & \Re(u) \\ -\Im(v) & \Re(v) \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}). \tag{3.2}$$

Proof. First of all, note that Condition 3.2 is equivalent to the equality $\Im(uv) = 1$ (because one is equal to $\Im(u)\Re(v) + \Re(u)\Im(v)$ or, in other words, to $\Im((\Re(u) + \Im(u)\iota)(\Re(v) + \Im(v)\iota))$).

Now, for the direct implication, observe that, in $\mathbb{Z}[\iota]$, p divides $(m+\iota)(m-\iota)$; but it divides neither $m+\iota$ nor $m-\iota$. Hence p is not a Gaussian prime, which yields the existence of non-invertible Gaussian integers r and s such that rs equals p. Therefore, we have that $pp = p\overline{p} = rs\overline{r}\overline{s} = r\overline{r}s\overline{s}$; so p is equal to $r\overline{r}$ (because $r\overline{r}$ and $s\overline{s}$ are rational integers). We also have that $p^2 = N(p) = N(r\overline{r}) = N(r)N(\overline{r})$, which implies that $N(r) = N(\overline{r}) = p$ and thus r and $\overline{r}$ are Gaussian primes. Let v be the greatest common divisor of p and $m+\iota$ in $\mathbb{Z}[\iota]$, which belongs to $\{r, \overline{r}\}$ (because r and $\overline{r}$ are Gaussian primes and $r\overline{r} = p \mid (m+\iota)(m-\iota)$), and let u be the Gaussian integer such that $uv = m+\iota$. Then $v\overline{v} = p \mid m^2 - \Re(uv)^2$ and $\Im(uv) = 1$, as desired.

For the converse implication, let k be $\Re(uv)$. Then uv equals $k+\iota$ (because $\Im(uv) = 1$), so $p \mid u\overline{u}p = u\overline{u}v\overline{v} = uv\overline{uv} = k^2 + 1$ (because $v\overline{v} = p$). We have in addition that p divides $m^2 - k^2$, so p is a divisor of $(m^2 - k^2) + (k^2 + 1)$ or, in other words, of $m^2 + 1$. □

As an example for Theorem 3.3.2.1, set $m = 5$, $p = 2$, $u = 5 - 4\iota$ and $v = 1 + \iota$.

3.3.3 Factorization of Mersenne numbers

This joint work with Jinyuan Wang explores the problem of the factorization of **Mersenne numbers**, i.e. numbers of the form $2^n - 1$, where n is any non-negative integer (see OEIS A000225); and recall that Proposition 2 of Article C in Section 3.2 shows a very important connection between Fermat numbers and Mersenne numbers.

It is also worth mentioning the following generalization of the Mersenne numbers and of many other important sequences: given any two integers P and Q such that $P^2 \neq 4Q$ the **Lucas sequence** of the first (resp., second) kind, which is denoted by $U_n(P, Q)$ (resp., $V_n(P, Q)$), is the sequence x such that $x(0) = 0$ (resp., $x(0) = 2$), $x(1) = 1$ (resp., $x(1) = P$) and $x(n+2) = Px(n+1) - Qx(n)$ for every non-negative integer n.

Theorem 3.3.3.1 shows that Lucas sequences have a very nice closed form (see the Encyclopedia of Mathematics [17]).

Theorem 3.3.3.1. *If n, P and Q are any three integers such that $n \geq 0 \neq P^2 - 4Q$, and α and β are the numbers $(P + \sqrt{P^2 - 4Q})/2$ and $(P - \sqrt{P^2 - 4Q})/2$*

respectively, then $U_n(P,Q)$ *and* $V_n(P,Q)$ *equal* $(\alpha^n - \beta^n)/(\alpha - \beta)$ *and* $\alpha^n + \beta^n$ *respectively.*

For example, if n is any non-negative integer, then $U_n(3,2)$ is equal to the n-th Mersenne number; and the sequence $(U_k(1,-1))_{k=0}^{\infty}$ is the famous **Fibonacci sequence** (see Křížek et al. [11, Remark 10.12]).

Let D denote the function from the non-negative integers to the set of sets of positive integers which maps every non-negative integer i into the set of positive integers n such that $n^{2^i} - 1$ divides $2^n - 1$. We now study the sequence D, distinguishing between the observations on general terms and observations on the second term.

3.3.3.1 General terms

Proposition 3.3.3.2 characterizes when the a term of D contains a power of the form 2^{2^j}, where j is any non-negative integer.

Proposition 3.3.3.2. *Given any two non-negative integers* i *and* j, 2^{2^j} *belongs to* $D(i)$ *if and only if* $i + j \leq 2^j$.

Proof I. The statement follows from the fact that

$$\frac{2^{2^{2^j}} - 1}{(2^{2^j})^{2^i} - 1} = \sum_{k=0}^{2^{2^j - j - i} - 1} \left(2^{k 2^{j+i}}\right)$$

holds if and only if $i + j \leq 2^j$ (by applying Proposition 5 of Article C in Section 3.2). □

Proof II. The statement follows from the fact that

$$(2^{2^j})^{2^i} - 1 = 2^{2^{i+j}} - 1 = \prod_{k=0}^{i+j-1} (2^{2^k} + 1) \mid \prod_{k=0}^{2^j - 1} (2^{2^k} + 1) = 2^{2^{2^j}} - 1$$

holds if and only if $i + j \leq 2^j$ (by applying Proposition 2 of Article C in Section 3.2). □

However, $D(0)$ and $D(1)$ contain elements that are not of the form 2^{2^j}; for example 6^2 and 6^4 belong to $D(0) \cap D(1)$. The existence of elements of $D(2)$ that are not of the form 2^{2^j} is currently unknown (see OEIS A247219).

Conjecture 3.3.3.3. *If* i *is any non-negative integer, then* $D(i)$ *contains some element which is not of the form* 2^{2^j}.

A similar situation is the following one: if a positive integer n is a power of three, then n factors $2n+1$ (see OEIS A006521); but the converse is not always true (171 is a counterexample).

Proposition 3.3.3.4. *If i is any non-negative integer, then $D(i+1) \subseteq D(i)$.*

Proof. Let n be any positive integer. The number $(n^{2^i}-1)(n^{2^i}+1)$ is equal to $n^{2^{i+1}}-1$. Therefore, if $n^{2^{i+1}}-1$ divides 2^n-1, then by transitivity $n^{2^i}-1$ also divides 2^n-1. □

Conjecture 3.3.3.5. *If i is any non-negative integer, then $D(i+1) \neq D(i)$.*

Unfortunately, currently it is not even known if $D(3)$ differs from $D(4)$.

Proposition 3.3.3.6. *If j, u and v are any three non-negative integers such that $u \leq 2^j - j < v$, then $D(v) \neq D(u)$.*

Proof. $u \leq 2^j - j < v$ implies that $2^{2^j} \in D(u) \backslash D(v)$ (by applying Proposition 3.3.3.2), so $D(v) \neq D(u)$. □

Now we need a property of the multiplicative orders, Lemma 3.3.3.7.

Lemma 3.3.3.7. *If a, n and r are any three integers such that r is positive and n exceeds one, is coprime with a and divides $a^r - 1$, then $\mathrm{ord}_n(a)$ divides r.*

Proof. Suppose the contrary. Then there are two positive integers b and c such that $b\,\mathrm{ord}_n(a) + c = r$ and $c < \mathrm{ord}_n(a)$ (because, by definition, $\mathrm{ord}_n(a) < r$). Consequently,

$$1 \equiv a^r = a^{b\,\mathrm{ord}_n(a)+c} = (a^{\mathrm{ord}_n(a)})^b a^c \equiv 1^b a^c = a^c \pmod{n}$$

(because n divides $a^r - 1$); which contradicts the fact that $\mathrm{ord}_n(a)$ is the minimum positive integer k such that n divides $a^k - 1$. □

For example, 25 is coprime with 3 and divides $3^{20} - 1$; and $\mathrm{ord}_{25}(3)$ equals 20.

Given any integer $m > 1$, a **modular multiplicative inverse** of any integer a modulo m is any integer x such that ax is congruent to one modulo m; and it exists if and only if a and m are coprime (cf. Rosen [15, Section 4.2]).

For example, 9 is a modular multiplicative inverse of 7 modulo 31 because $7 \cdot 9 \equiv 1 \pmod{31}$.

Theorem 3.3.3.8. *Given any odd integer $n > 1$, $\gcd(n, \mathrm{ord}_n(2)) = 1$ if and only there exist integers $i \geq 0$ and $j > 0$ such that $n \mid \gcd(2^j - 1, j^{2^i} - 1)$.*

Proof. For the direct implication, let w be a modular multiplicative inverse of $\mathrm{ord}_n(2)$ modulo n (which exists because $\gcd(n, \mathrm{ord}_n(2)) = 1$), let i be any non-negative integer and let j be the number $\mathrm{ord}_n(2)w$. Then 2^j is equal to $(2^{\mathrm{ord}_n(2)})^w$ and hence congruent to one modulo n. And j^{2^i} is also congruent to one modulo n (because j equals $\mathrm{ord}_n(2)w$ and w is a modular multiplicative inverse of $\mathrm{ord}_n(2)$ modulo n), from which follows that n divides $\gcd(2^j - 1, j^{2^i} - 1)$.

Now, let us prove the contrapositive equivalent of the converse implication; that is, if $\gcd(n, \mathrm{ord}_n(2)) > 1$, then, for every two integers $i \geq 0$ and $j > 0$, the number n does not divide $\gcd(2^j - 1, j^{2^i} - 1)$.

Indeed, let i and j be any two non-negative integers such that j is positive; and suppose that n divides $\gcd(2^j - 1, j^{2^i} - 1)$. Then n divides $2^j - 1$, so $\mathrm{ord}_n(2)$ divides j (by also considering that j is positive and n is an odd integer which exceeds one; and then applying Lemma 3.3.3.7) and thus $\gcd(n, \mathrm{ord}_n(2))$ divides j.

We have that $\gcd(j, j-1) = 1$ (because every integer is coprime with its successor), so

$$\gcd\left(j, \sum_{h=1}^{j^{2^i-1}} (j) - 1\right) = 1$$

or, equivalently, $\gcd(j, j^{2^i} - 1) = 1$. Thus $\gcd(\gcd(n, \mathrm{ord}_n(2)), j^{2^i} - 1) = 1$ (because $\gcd(n, \mathrm{ord}_n(2))$ divides j).

We also have that n divides $\gcd(n, j^{2^i} - 1)$ (because n divides $\gcd(2^j - 1, j^{2^i} - 1)$), so $\gcd(n, \mathrm{ord}_n(2))$ divides $\gcd(n, j^{2^i} - 1)$ and therefore $\gcd(n, \mathrm{ord}_n(2))$ divides $\gcd(\gcd(n, \mathrm{ord}_n(2)), j^{2^i} - 1)$. Consequently, $\gcd(\gcd(n, \mathrm{ord}_n(2)), j^{2^i} - 1) > 1$ (because $\gcd(n, \mathrm{ord}_n(2)) > 1$); which is impossible because $\gcd(\gcd(n, \mathrm{ord}_n(2)), j^{2^i} - 1) = 1$. □

For example, 5 is coprime with $\mathrm{ord}_5(2)$ (which equals 4) and divides $\gcd(2^4 - 1, 4^{2^1} - 1)$ (which equals 15).

3.3.3.2 The second term

Recall, from Section 2 of Article B in Section 3.1, the notion of **dyadic valuation** and its notation ν_2; and let G denote the sequence $(\gcd(2^n - 1, n^{2^2} - 1))_{n=0}^{\infty}$.

We need to make use of Lemma 3.3.3.9 (see Graham et al. [5, Exercise 38 from Chapter 4]).

Lemma 3.3.3.9. *If a, b, m and n are any four integers such that a is coprime with b, a exceeds b and $0 \leq m < n$, then $\gcd(a^m - b^m, a^n - b^n)$ equals $a^{\gcd(m,n)} - b^{\gcd(m,n)}$.*

For example, 20 is coprime with 11 and $\gcd(20^3 - 11^3, 20^4 - 11^4)$ equals $20 - 11$.

Proposition 3.3.3.10. *Given any integer $n > 2$, the number $G(2^n)$ is equal to $2^{2^{\nu_2(n)+2}} - 1$.*

Proof. It is easy to check that $(G(2^k))_{k=3}^5$ is equal to $(15, 65535, 15)$ or, equivalently, to $(2^{2^{\nu_2(k)+2}} - 1)_{k=3}^5$.

Now suppose that n exceeds five; and note that $\gcd(2^{4n}, 2^{4n} - 1) = 1$ (because every integer is coprime with its successor).

We have that $G(2^n) =$

$\gcd(2^{2^n} - 1, 2^{4n} - 1) =$

$\gcd(2^{2^n} - 2^{4n}, 2^{4n} - 1) =$

$\gcd(2^{4n}(2^{2^n - 4n} - 1), 2^{4n} - 1) =$ (because $n > 3$)

$\gcd(2^{2^n - 4n} - 1, 2^{4n} - 1) =$ (because $\gcd(2^{4n}, 2^{4n} - 1) = 1$)

$2^{\gcd(2^n - 4n, 4n)} - 1 =$ (by applying that $n > 5$ and Lemma 3.3.3.9)

$2^{\gcd(2^n, 4n)} - 1 =$

$2^{\gcd(2^n, 2^{\nu_2(n)+2} i)} - 1 =$ (by denoting by i the odd part of n)

$2^{2^{\min(n, \nu_2(n)+2)}} - 1 =$

$2^{2^{\nu_2(n)+2}} - 1$ (see the proof of Proposition 12 of Article C in Section 3.2). □

For example, $G(2^6) = 255 = 2^{2^{1+2}} - 1 = 2^{2^{\nu_2(6)+2}} - 1$.

Proposition 3.3.3.11. *Any positive integer n such that $G(2n)$ equals one is a multiple of three.*

Proof. Suppose that n is equal to $3k+1$ or to $3k+2$, for some non-negative integer k. Then $16n^4$ is equal to $(6k+2)^4$ or to $(6k+4)^4$, which in both cases is congruent to one modulo three. And 2^{2n} is equal to 4^{3k+1} or to 4^{3k+2}, which is in both cases also congruent to one modulo three. Therefore three divides $\gcd(2^{2n} - 1, 16n^4 - 1)$, which contradicts the fact that $G(2n)$ equals one. □

The first 15 positive integers n such that $G(2n)$ equals one are 27, 57, 93, 117, 147, 159, 177, 195, 201, 237, 267, 279, 327, 357 and 387.

Theorem 3.3.3.12 is known as **Dirichlet's theorem on arithmetic progressions** (see Hardy & Wright [8, Theorem 15]).

Theorem 3.3.3.12. *Given any two coprime integers $a > 0$ and b, the arithmetic progression $(an + b)_{n=0}^{\infty}$ has infinitely many prime terms.*

For example, the arithmetic progression $(20n + 1)_{n=0}^{\infty}$ has infinitely many prime terms; such as $20 \cdot 2 + 1$, $20 \cdot 3 + 1$ and $20 \cdot 5 + 1$.

Proposition 3.3.3.13. *There are infinitely many primes p for which $G(2p - 1)$ exceeds one.*

Proof. Let n and p be any two positive integers such that $21n+8$ is a prime number equal to p (they exist because of Dirichlet's theorem of arithmetic progressions, i.e. Theorem 3.3.3.12). Then $G(2p-1)$ is equal to $\gcd(2^{42n+15}-1, (42n+15)^4-1)$, so seven divides $G(2p-1)$ (because $(2^3)^{14n+5}$ and $(42n+15)^4$ are congruent to one modulo seven) and therefore $G(2p - 1)$ exceeds one. □

The first 15 primes p such that $G(2p - 1)$ exceeds one are 29, 71, 113, 197, 239, 281, 293, 373, 449, 491, 617, 659, 683, 701 and 743.

Conjecture 3.3.3.14. *There are infinitely many primes p such that $G(12p-7) > G(12p - 6) = 1$.*

The first 15 primes p such that $G(12p - 7) > G(12p - 6) = 1$ are 821, 1217, 1721, 2797, 3271, 4591, 6311, 6521, 6991, 7451, 8231, 9049, 9161, 9511 and 9781.

3.3.4 Products of consecutive generalized Fermat numbers

A **generalized Fermat number** is a number of the form $b^{2^n} + 1$, where b is any integer exceeding one and n is any non-negative integer (cf. Křížek et al. [11, Remark 8.4]). Notice that we have already seen a result on the factorization of generalized Fermat numbers, namely Theorem 2.3 of Article B in Section 3.1; which can be re-stated as Theorem 3.3.4.1.

Theorem 3.3.4.1. *Given any three integers $f > 1$, $j > 0$ and $n > 2$ such that f is a factor of the n-th Fermat number, the number f is also a factor of the generalized Fermat number*

$$\left(\frac{f-1}{2^{n+2}}\right)^{2^{n-\nu_2(n+2)}(2j-1)} + 1.$$

For example, $5 \cdot 2^7 + 1$ divides the fifth Fermat number and $(5^r)^{2^5} + 1$, for every odd positive integer r.

Proposition 3 of Article C in Section 3.2 can be generalized into the following iterative expression of the products of the first consecutive generalized Fermat numbers, Theorem 3.3.4.2.

Theorem 3.3.4.2. *If b is an integer exceeding one, n is a non-negative integer and s is the sequence $((k+2)k)_{k=0}^{\infty}$, then*

$$\sum_{k=0}^{2^{n+1}-1}\left(b^k\right)=\prod_{k=0}^{n}\left(b^{2^k}+1\right)=\frac{s^{n+1}(b-1)}{b-1}=\frac{b^{2^{n+1}}-1}{b-1}.$$

Proof. The equality $\sum_{k=0}^{2^{n+1}-1}(b^k)=(b^{2^{n+1}}-1)/(b-1)$ is a direct application of Proposition 2 of Article C in Section 3.2.

The equality $\prod_{k=0}^{n}(b^{2^k}+1)=(b^{2^{n+1}}-1)/(b-1)$ holds because $b^{2^{n+1}}-1=(b^{2^n}+1)(b^{2^n}-1)=(b^{2^n}+1)(b^{2^{n-1}}+1)(b^{2^{n-1}}-1)=\ldots=(b^{2^n}+1)(b^{2^{n-1}}+1)\ldots(b^{2^{n-n}}+1)(b^{2^{n-n}}-1)$.

The equality $(s^{n+1}(b-1))/(b-1)=(b^{2^{n+1}}-1)/(b-1)$ can be obtained by induction, by first noticing that $s^{0+1}(b-1)=(b+1)(b-1)=b^{2^{0+1}}-1$ and secondly connecting the equalities $s^{n+2}(b-1)=s(s^{n+1}(b-1))$ and $s(b^{2^{n+1}}-1)=(b^{2^{n+1}}+1)(b^{2^{n+1}}-1)=b^{2^{n+2}}-1$ by means of the induction hypothesis. □

For example,

$$\sum_{k=0}^{3}\left(17^k\right)=\prod_{k=0}^{1}\left(17^{2^k}+1\right)=\frac{s^2(16)}{16}=\frac{17^{2^2}-1}{16}=5220.$$

3.3.5 Hervás-Contreras chains

A **lesser twin prime** is a prime p such that $p+2$ is also a prime. The cardinality of the set of lesser twin primes is currently unknown (see Weisstein [29]).

Computing factors of Fermat numbers can be regarded as a particular case of the more general problem of computing large primes. Hervás-Contreras observed the very interesting sub-sequence 11, 311, 18311, 1518311 and 421518311 of lesser twin primes (see OEIS A350246), which incidentally produces a relatively easy way of obtaining **titanic primes** (i.e. primes of at least 1000 digits, see Weisstein [28]); as it will be exemplified in Subsubsection 3.3.5.5.

3.3.5.1 Technical results

The **digit sum** of a positive integer is the sum of its digits, and it is denoted by ds (see Weisstein [22]).

For example, ds(18311) equals 14.

Lemma 3.3.5.1. *A positive integer is divisible by three if and only if its digit sum is congruent to zero, three or six modulo nine.*

Proof. It is well-known that any positive integer n is divisible by three if and only if $\mathrm{ds}(n)$ is so. And this is case if and only if $\mathrm{ds}(n)$ is congruent to some element of $\{0, 3, 6\}$ modulo nine. □

Lemma 3.3.5.2. *If n is any positive integer, then $\mathrm{ds}(n+2)$ is congruent to $\mathrm{ds}(n)+2$ modulo nine.*

Proof. It is well-known that any positive integer is congruent to its digit sum modulo nine, so $n + 2 \equiv \mathrm{ds}(n + 2) \pmod 9$ and, by again applying this fact, $\mathrm{ds}(n) + 2 \equiv \mathrm{ds}(n + 2) \pmod 9$. □

The concatenation of two positive integers a and b is denoted by $a||b$ (see Weisstein [20]).

For example, $3||11$ equals 311.

Lemma 3.3.5.3. *If p is any lesser twin prime exceeding five and n is any positive integer such that $n||p$ is also a lesser twin prime, then n is a multiple of three.*

Proof I. Suppose that n is not a multiple of three. Then $\mathrm{ds}(n)$ is congruent modulo nine to some element i of $\{1, 2, 4, 5, 7, 8\}$ (by applying Lemma 3.3.5.1). And the numbers p and $n||p$ are primes which exceed three, so $\mathrm{ds}(p)$ and $\mathrm{ds}(n||p)$ are congruent modulo nine to some elements j and k of $\{1, 2, 4, 5, 7, 8\}$, respectively (by again applying Lemma 3.3.5.1).

Let A and B be the sets $\{(2, 2, 4), (2, 5, 7), (2, 8, 1), (5, 2, 7), (5, 5, 1), (5, 8, 4), (8, 2, 1), (8, 5, 4), (8, 8, 7)\}$ and $\{(1, 1, 2), (1, 4, 5), (1, 7, 8), (4, 1, 5), (4, 4, 8), (4, 7, 2), (7, 1, 8), (7, 4, 2), (7, 7, 5)\}$, respectively. The number $\mathrm{ds}(n||p)$ equals $\mathrm{ds}(n)+\mathrm{ds}(p)$, so $k \equiv i + j \pmod 9$ and therefore (i, j, k) belongs to the union of A and B.

Case 1: (i, j, k) belongs to A Then $\mathrm{ds}((n||p) + 2)$ is congruent modulo nine to $\mathrm{ds}(n||p) + 2$ (by applying Lemma 3.3.5.2) or, in other words, to $k + 2$; which in this case is congruent to zero, to three or to six modulo nine. Hence $(n||p) + 2$ is divisible by three (by applying Lemma 3.3.5.1), which contradicts the fact that $(n||p) + 2$ is a prime exceeding three.

Case 2: (i, j, k) belongs to B Then $\mathrm{ds}(p+2)$ is congruent modulo nine to $\mathrm{ds}(p)+2$ (by applying Lemma 3.3.5.2) or, in other words, to $j + 2$; which in this case is congruent to zero, to three or to six modulo nine. Hence $p+2$ is divisible by three

(by applying Lemma 3.3.5.1), which contradicts the fact that $p+2$ is a prime exceeding three. □

The following alternative proof is essentially due to José-Antonio Hervás-Contreras (pers. comm.).

Proof II. Let l be the number of digits of p.

The number $n||p$ is prime and equal to $10^l n + p$.

Therefore, $10^l n + p \equiv 1 \pmod 3$ or $10^l n + p \equiv 2 \pmod 3$; from which follows that $10^l n + p + 2 \equiv 0 \pmod 3$ or $10^l n + p + 2 \equiv 1 \pmod 3$.

But $10^l n + p$ is a lesser twin prime, so $10^l n + p + 2$ is prime and thus the only possibility is $10^l n + p + 2 \equiv 1 \pmod 3$; which implies that $2 \cdot 10^l n + 2p + 4 \equiv 2 \pmod 6$.

The condition that p exceeds five yields that $p \equiv 5 \pmod 6$ (see the comment from the 11th of May of 2013 at OEIS A001359), so $2 \cdot 10^l n \equiv 0 \pmod 6$.

Hence, $10^l n \equiv 0 \pmod 3$; and consequently $n \equiv 0 \pmod 3$. □

Lemma 3.3.5.3 proves Conjecture III from the 21th of December of 2021 at OEIS A001359.

Note that there are positive integers n and p such that three divides n and $n||p$ is a lesser twin prime but p is not, consider for example the case in which $n = 3$ and $p = 47$.

3.3.5.2 General observations

Given any positive integer n, a tuple $(t_1, \ldots, t_n)$ of positive integers is said to be a **Hervás-Contreras chain** for a lesser twin prime p exceeding five if and only if $t_k|| \ldots ||t_1||p$ is also a lesser twin prime, for every $k \in \{1, \ldots, n\}$.

For example, $(3, 18, 15, 42)$ is a Hervás-Contreras chain for 11.

Proposition 3.3.5.4 is a direct consequence of Lemma 3.3.5.3.

Proposition 3.3.5.4. *Every term of a Hervás-Contreras chain is a multiple of three.*

Note that, given any lesser twin prime p exceeding five, there are infinitely many positive integers n such that $n||p$ (i.e. $n10^l + p$, where l is the number of digits of p) is prime (by applying Dirichlet's theorem on arithmetic progressions, i.e. Theorem 3.3.3.12). Conjecture 3.3.5.5 is a strengthening of this fact.

Conjecture 3.3.5.5. *Given any lesser twin prime p exceeding five, there are infinitely many positive integers n such that $n||p$ is also a lesser twin prime.*

In particular, Conjecture 3.3.5.5 claims that Hervás-Contreras chains can always be prolonged.

The weakening of Conjecture 3.3.5.5 which claims the existence of at least one n (instead of infinitely many) is Conjecture I from the 21th of December of 2021 at OEIS A001359.

Conjecture 3.3.5.6 claims however that arbitrarily prolonging Hervás-Contreras chains without increasing the number of digits of some of the new terms is impossible.

Conjecture 3.3.5.6. *Given any lesser twin prime p exceeding five and any positive integer r, there is some positive integer m such that any Hervás-Contreras chain for p whose length is at least m has some term of more than r digits.*

For example, any Hervás-Contreras chain for 11 of length two, such as $(3, 18)$, has some term of more than one digit.

Conjecture 3.3.5.7. *If k is any positive integer, then there are infinitely many lesser twin primes p such that $(3k)||p$ is also a lesser twin prime.*

In particular, Conjecture 3.3.5.7 asserts that every multiple of three appears in infinitely many Hervás-Contreras chains.

The weakening of Conjecture 3.3.5.7 which claims the existence of at least one p (instead of infinitely many) is Conjecture II from the 21th of December of 2021 at OEIS A001359.

The **level** of a lesser twin prime p exceeding five is the length of the longest Hervás-Contreras chain that reaches p and zero if there is none (or, more formally, if, for every positive integer n and every lesser twin prime q exceeding five, p is not equal to $n||q$).

For example, the level of 17 is 0 because no Hervás-Contreras chain reaches it and the level of 618888336126249111111117 is 8 because the longest Hervás-Contreras chain that reaches it is $(111, 111, 249, 6, 12, 336, 888, 618)$.

Figure 3.1 displays some lesser twin primes of different levels.

Observe that, if Conjecture 3.3.5.5 holds, then there are infinitely many lesser twin primes of each level.

The first 50 lesser twin primes p exceeding five of level 0 are 11, 17, 29, 41, 59, 71, 101, 107, 137, 149, 179, 191, 197, 227, 239, 269, 281, 347, 419, 431, 461, 521, 569,

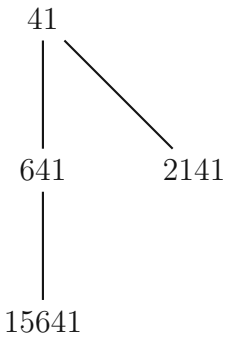


Figure 3.1: Some lesser twin primes of different levels.

599, 809, 821, 827, 857, 881, 1019, 1031, 1049, 1061, 1091, 1151, 1277, 1289, 1301, 1319, 1427, 1451, 1481, 1487, 1607, 1619, 1667, 1697, 1721, 1787 and 1871.

3.3.5.3 Hervás-Contreras forests

A **forest** is a graph whose connected components are trees (cf. Diestel [3, Section 1.5]).

Hervás-Contreras [9] paid special attention to Hervás-Contreras chains whose terms have the same number of digits, which led to the following concept.

Given any lesser twin prime p exceeding five and any positive integer r, let the **Hervás-Contreras forest** of p and r be the forest $F_H(p, r)$ which is obtained by merging all the Hervás-Contreras chains for p in which every term has exactly r digits; as exemplified in Figure 3.2 and Figure 3.3 (for simplicity, instead of writing the full numbers (e.g. 42 17 and 90 42 17), we write only the terms of the Hervás-Contreras chains (e.g. 42_1^2 and 90_2^2); where the subscript indicates the term and the superscript indicates the tree).

Conjecture 3.3.5.6 yields that, if the number of digits is fixed, then the Hervás-Contreras forests cannot be arbitrarily large.

For example, the longest branches of $F_H(17, 2)$ are of length 6.

Another interesting question is Problem 3.3.5.8 on which kinds of shapes the trees from the Hervás-Contreras forests can take.

Problem 3.3.5.8. *What class of trees do the connected components of the Hervás-Contreras forests form?*

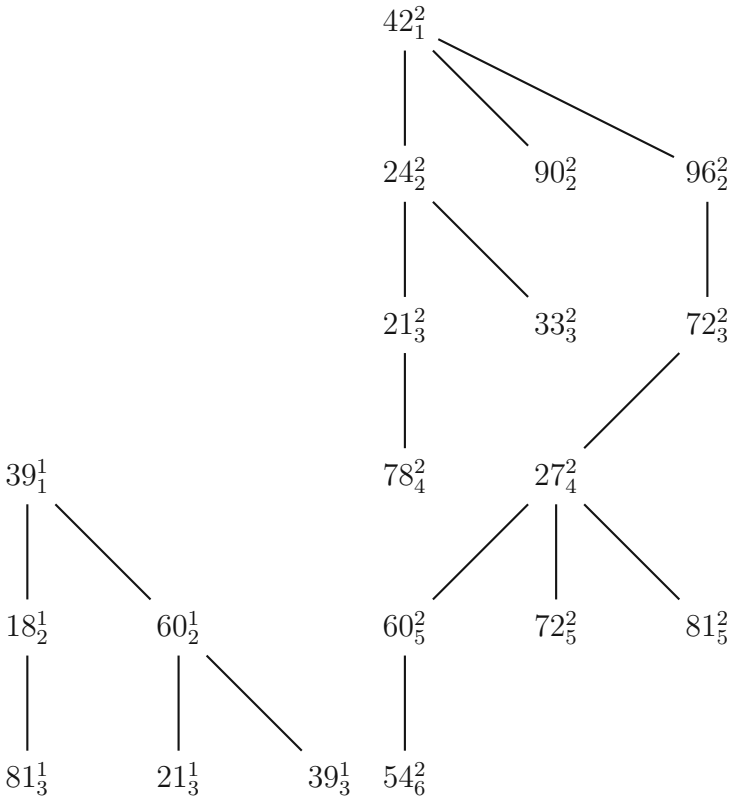


Figure 3.2: The forest $F_H(17, 2)$ (part 1 of 2).

3.3.5.4 Some similar problems

Given any positive integer n, a tuple of primes $(p_1, \ldots, p_n)$ is said to be a **Cunningham chain** if and only if p_{k+1} equals $2p_k + 1$, for every positive integer $k < n$ (cf. Weisstein [21]).

For example, $(2, 5, 11, 23, 47)$ is a Cunningham chain.

Conjecture 3.3.5.6 resembles Theorem 3.3.5.9 (see Löh [12, Section 1]).

Theorem 3.3.5.9. *If p is any prime and f is the sequence $(2n+1)_{n=0}^{\infty}$, then there is some positive integer m such that $f^m(p)$ is composite.*

For example, if f is the sequence $(2n + 1)_{n=0}^{\infty}$, then $f^5(2)$ (i.e. 95) is composite.

Given any positive integer n, let the **forest of prime decimal descendants** of n be the biggest forest $F_P(n)$ which can be obtained by appending digits to the right, starting from n and under the condition that every new number is prime; as exemplified in Figure 3.4.

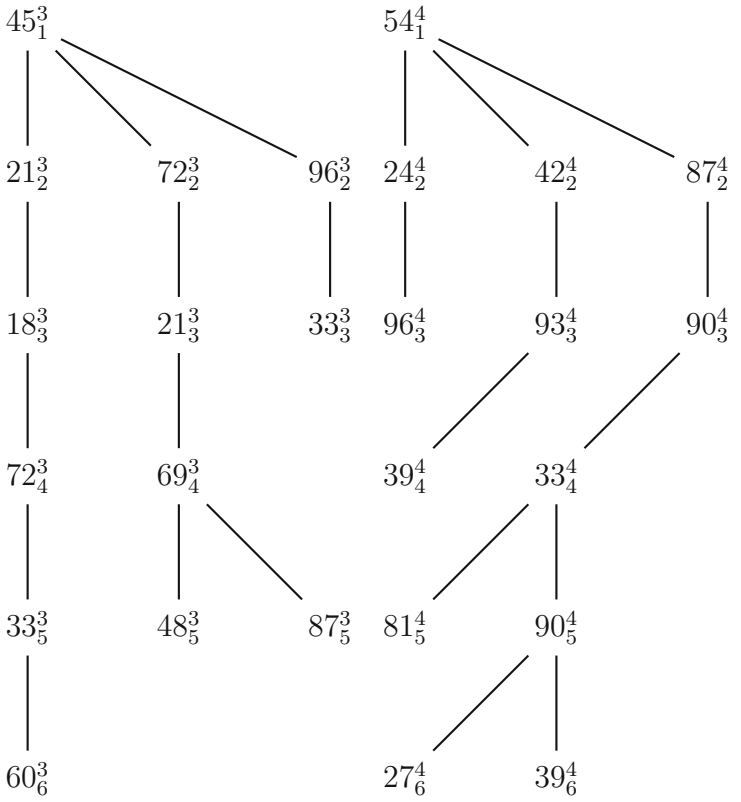


Figure 3.3: The forest $F_H(17, 2)$ (part 2 of 2).

Another statement which resembles Conjecture 3.3.5.6 is Conjecture 3.3.5.10 on the existence of a global upper-bound to the size of the forests of prime decimal descendants.

Conjecture 3.3.5.10. *there is some positive integer m such that, for every positive integer n, the length of any branch of any tree of $F_P(n)$ is upper-bounded by m.*

Lu conjectured that, if n is any positive integer, then the number of vertices of $F_P(n)$ is upper-bounded by 83 (see OEIS A346979); which would imply Conjecture 3.3.5.10. Ratushnyak conjectured in addition that, if p is any prime, then the number of vertices of $F_P(p)$ is upper-bounded by 40 (see OEIS A214342).

Problem 3.3.5.11 poses the question of which kinds of shapes the trees from the forests of prime decimal descendants can take, in correspondence with Problem 3.3.5.8.

Problem 3.3.5.11. *What class of trees do the connected components of the forests*

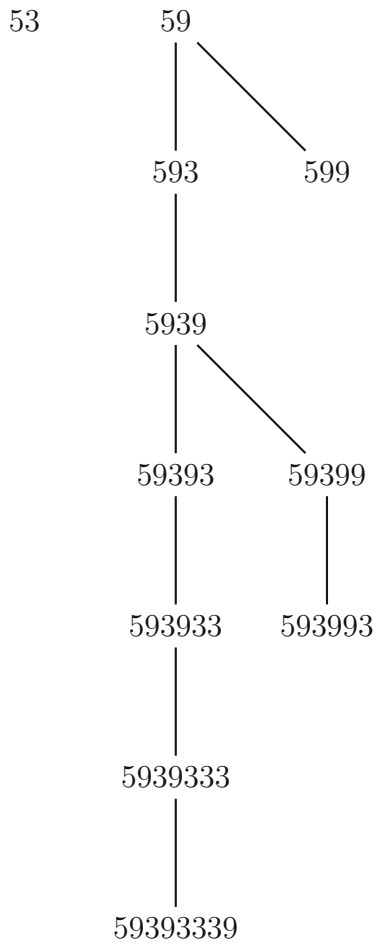


Figure 3.4: The forest $F_P(5)$.

of prime decimal descendants form?

For example, Figure 3.4 shows that the **singleton graph** (i.e. the graph which has a single vertex, see Weisstein [27]) belongs to the class of trees that the connected components of the forests of prime decimal descendants form.

3.3.5.5 Computation of titanic primes

The generation of Hervás-Contreras forests is, apparently, not very hard from a computational point of view; which provides in particular a reasonable method for calculating titanic primes.

For example, the prime 2958270 1216143 1761123 3938925 4492917 1364220 2349657 4647687 1647525 1804998 3513576 1932348 2100459 1041771 2593878 3385542 2413764

4538508 5962971 1999497 1788375 1008042 3126972 2075523 3830547 4507380 1377654 2974935 2301855 3231174 3474906 6242973 3440235 2262138 1992303 2554431 1687920 1388025 1966770 1929618 1708806 1814376 1035954 2253180 1021818 2365269 2972505 3314070 2735712 1467468 2006169 3319458 1888350 1084587 3168327 2288223 2128833 3097125 1197645 1190931 3477006 1104564 1062366 1764999 2349660 1720455 1536618 1385961 1115646 1259502 2147508 3326766 1178982 2705901 1080714 1250160 1131351 1160409 1201917 1631001 1206663 1755225 1044393 1195347 1515930 1726017 2722275 1075104 1040481 1473210 2168298 1897107 1970853 1293804 2186904 1412232 1059834 1520847 1679784 1100325 1863591 1170660 1121262 1153293 1618737 1097898 1197219 1262100 2233488 1896357 1290885 1285395 1107192 1613235 1242639 1132545 1640016 1403988 1347363 1066677 1054788 1272795 1167558 1496904 1271424 1425228 1488843 1042692 1241601 1062768 1028637 1017636 1015497 1084104 1175787 1054602 1163256 1098006 1123422 1103280 1071165 1092666 1017600 1069140 1030389 1102191 1038156 1304601 1059432 1063242 1020987 1111164 1001496 1043073 1082610 1032780 1009092 1225644 1002834 1154049 1077201 1028250 1034412 1006500 1022352 1001265 1049562 1015926 1026258 1078080 1031073 1000284 1008459 1008648 1001043 1033776 1003884 1004328 1009908 1001601 1002849 1005267 1002606 1002453 1000041 1000026 1000524 1000053 17, of 1318 digits, was obtained after computing a branch of $F_H(17, 7)$; concluding in particular the calculation started in Hervás-Contreras [9].

But even more generally, it seems easy to find titanic primes simply because many integers of three produce a prime when concatenated to some lesser twin prime.

For example, we can choose a lesser twin prime p and a positive integer n and then randomly trying small positive integers k until the value $10^{150n} + (3k+2)10^{100n} + p$ happens to be prime: this procedure quickly found that $10^{150\cdot 100} + (3 \cdot 74192 + 2)10^{100\cdot 100} + 11$, of 15001 digits, is prime.

Given any lesser twin prime p exceeding five and any positive integer r, let $A(p, r)$ denote the set of positive integers n of exactly r digits and such that $n||p$ is also a lesser twin prime. In order to study the aforementioned phenomena, one of the concrete questions that can be considered is Problem 3.3.5.12.

Problem 3.3.5.12. *Given any lesser twin prime p exceeding five, evaluate*

$$\lim_r \left(\frac{|A(p, r)|}{|A(p, r+1)|} \right).$$

For example, $|A(11, 6)|/|A(11, 7)|$ equals 12651/99646; a rational number which is approximately equal to 0.12695 and whose period has exactly 49822 digits .

References

[1] M. Baaz, Note on the generalization of calculations, *Theoretical Computer Science* **224** (1999), 1–2. https://www.sciencedirect.com/science/article/pii/S0304397598003041

[2] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective* [2nd ed.], Springer, 2005.

[3] R. Diestel, *Graph Theory* [3rd ed.], Springer, 2005.

[4] H. B. Enderton, *Computability Theory: An Introduction to Recursion Theory*, Academic Press, 2010.

[5] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, 1989.

[6] J. Y. Halpern, *Reasoning about Uncertainty*, The MIT Press, 2005.

[7] A. G. Hamilton, *Logic for Mathematicians*, Cambridge University Press, 1978.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* [6th ed.], Oxford University Press, 2008.

[9] J. A. Hervás Contreras, Ristras de números primos gemelos [in Spanish], *La Gaceta de la Real Sociedad Matemática Española* **26** (2023).

[10] U. Kohlenbach, Effective bounds from proofs in abstract functional analysis, in B. Cooper, B. Loewe and A. Sorbi, eds., *New Computational Paradigms: Changing Conceptions of What is Computable*, Springer, 2008, pp. 223–258.

[11] M. Křížek, F. Luca and L. Somer, *17 Lectures on Fermat Numbers: from Number Theory to Geometry*, CMS Books in Mathematics, Springer, New York, 2001.

[12] G. Löh, Long chains of nearly doubled primes, *Mathematics of Computation* **53** (1989), 751–759. https://doi.org/10.1090/S0025-5718-1989-0979939-8

[13] E. Mendelson, *Introduction to Mathematical Logic* [6th ed.], Taylor & Francis, 2015.

[14] H. Riesel, *Prime Numbers and Computer Methods for Factorization* [2nd ed.], Boston, MA: Birkhäuser, 1994.

[15] K. H. Rosen, *Elementary Number Theory and Its Applications* [6th ed.], Addison-Wesley, 2011.

[16] R. Scott and R. Styer, The generalized Pillai equation $\pm ra^x \pm sb^y = c$, *Journal of Number Theory* **131** (2011), 1037–1047. https://doi.org/10.1016/j.jnt.2010.11.004

[17] Various, "Lucas sequence", Encyclopedia of Mathematics. https://encyclopediaofmath.org/wiki/Lucas_sequence

[18] E. W. Weisstein, "Arithmetic Progression", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/ArithmeticProgression.html

[19] E. W. Weisstein, "Characteristic Function", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/CharacteristicFunction.html

[20] E. W. Weisstein, "Concatenation", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/Concatenation.html

[21] E. W. Weisstein, "Cunningham Chain", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/CunninghamChain.html

[22] E. W. Weisstein, "Digit Sum", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/DigitSum.html

[23] E. W. Weisstein, "Generating Function", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/GeneratingFunction.html

[24] E. W. Weisstein, "Irrationality Measure", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/IrrationalityMeasure.html

[25] E. W. Weisstein, "Legendre Symbol", from MathWorld – A Wolfram Web Resource. https://mathworld.wolfram.com/LegendreSymbol.html

[26] E. W. Weisstein, "Near-Square Prime", from MathWorld – A Wolfram Web Resource. `https://mathworld.wolfram.com/Near-SquarePrime.html`

[27] E. W. Weisstein, "Singleton Graph", from MathWorld – A Wolfram Web Resource. `https://mathworld.wolfram.com/SingletonGraph.html`

[28] E. W. Weisstein, "Titanic Prime", from MathWorld – A Wolfram Web Resource. `https://mathworld.wolfram.com/TitanicPrime.html`

[29] E. W. Weisstein, "Twin Primes", from MathWorld – A Wolfram Web Resource. `https://mathworld.wolfram.com/TwinPrimes.html`

Index