Elementary analytic functions in VTC^0

Emil Jeřábek

Institute of Mathematics, Czech Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

March 14, 2023

Abstract

It is known that rational approximations of elementary analytic functions (exp, log, trigonometric, and hyperbolic functions, and their inverse functions) are computable in the weak complexity class TC^0. We show how to formalize the construction and basic properties of these functions in the corresponding theory of bounded arithmetic, VTC^0.

Keywords: bounded arithmetic; elementary analytic functions; models of arithmetic; threshold circuits

MSC (2020): 03F20, 03F30, 33B10

1 Introduction

The complexity class[1] TC^0 is a weak subclass of polynomial time and logarithmic space; we can think of TC^0, conflated with the corresponding function class, as the complexity class of elementary integer arithmetic operations: $+$, $-$, $\cdot$, $\lfloor x/y \rfloor$, and $<$ are TC^0-computable, with $\cdot$ and $\lfloor x/y \rfloor$ being TC^0-complete (under AC^0 Turing reductions). Iterated addition $\sum_{i<n} x_i$ and multiplication $\prod_{i<n} x_i$ are also TC^0-complete. (The TC^0-computability of $\prod_{i<n} x_i$ and $\lfloor x/y \rfloor$ was a difficult problem, finally settled by Hesse, Allender, and Barrington [7].) Apart from integers, TC^0 can compute the corresponding operations in various related structures: $\mathbb{Q}$, $\mathbb{Q}(i)$, and other number fields, or polynomial rings. Using iterated sums and products, TC^0 can compute approximations of analytic functions given by power series with TC^0-computable coefficients [20, 21, 14, 7], such as the *elementary analytic functions* [1, 18]: exp, log, trigonometric, hyperbolic, inverse trigonometric, and inverse hyperbolic functions.

One of the basic themes in proof complexity is that for many complexity classes C, we can associate to C a theory of bounded arithmetic T whose reasoning power is captured by C: the axiom schemata of T that provide the bulk of its deductive capabilities (induction, comprehension, minimization, ...) are postulated for formulas that express predicates computable in C, while the provably total computable functions of T (of suitable syntactic shape) are exactly

[1] Originally defined by Hajnal et al. [6] in a non-uniform setting, but in this paper we always mean the DLOGTIME-uniform version of the class, which gives a robust notion of "fully uniform" TC^0 with several equivalent definitions across various computational models (cf. [2]).

the C-functions. We may consider T to be a formalization of *feasible reasoning* of complexity C: what properties of concepts from C are derivable if we restrict our deductions to only use C-predicates and C-computable objects, shunning any higher-level reasoning?

In this paper, we are interested in feasible reasoning of complexity TC^0. The basic theory of bounded arithmetic corresponding to TC^0 is the Zambella-style two-sorted theory $\mathsf{VTC^0}$ introduced by Nguyen and Cook [16], or equivalently (up to the *RSUV* isomorphism), the Buss-style one-sorted theory[2] Δ^b_1-CR of Johannsen and Pollett [13]. It turns out that $\mathsf{VTC^0}$ is quite powerful when it comes to proving properties of TC^0-computable arithmetic operations, even though this can be rather challenging to prove. Notably, as shown in Jeřábek [9] by formalizing a variant of the Hesse–Allender–Barrington algorithm, $\mathsf{VTC^0}$ proves the existence of iterated products $\prod_{i<n} x_i$ satisfying the defining recurrence

$$\prod_{i<0} x_i = 1, \qquad \prod_{i<n+1} x_i = x_n \prod_{i<n} x_i,$$

and of integer division satisfying $y\lfloor x/y\rfloor \le x < y\bigl(\lfloor x/y\rfloor + 1\bigr)$. Earlier, Jeřábek [8] formalized in $\mathsf{VTC^0}$ (augmented with an iterated multiplication axiom, redundant by [9]) approximation of complex roots of constant-degree univariate polynomials; as a consequence, $\mathsf{VTC^0}$ includes IOpen (quantifier-free induction in the language of ordered rings) on the binary number sort, and even the *RSUV* translation of Σ^b_0 induction and minimization in Buss's language.

We continue the investigation of the power of $\mathsf{VTC^0}$, shifting the focus from integer (or rational) operations to real and complex analytic functions. As we already mentioned, a vast number of such functions can be approximated by TC^0 functions, and it's not clear to what extent we can develop a general theory of such functions in $\mathsf{VTC^0}$; in this paper, we start with the most notorious examples—the elementary analytic functions: exp, trigonometric functions (sin, cos, tan, . . .), hyperbolic functions (sinh, cosh, tanh, . . .), and their inverse functions (log, arcsin, arsinh, . . .). We mostly concentrate on complex exp and log, as the other functions can be defined in terms of these.

It would be extremely laborious to work directly in the language of $\mathsf{VTC^0}$ all the time, expressing everything in terms of rational approximations. We follow a different approach—we present the constructions and arguments model-theoretically, considering an extension of a given model $\mathfrak{M} \vDash \mathsf{VTC^0}$ to a larger structure where we can define the elementary analytic functions properly as bona fide functions: the model itself gives the ordered ring of "integers" $\mathbf{Z}^{\mathfrak{M}}$, its fraction field is the ordered field of "rationals" $\mathbf{Q}^{\mathfrak{M}}$, and the *completion* of $\mathbf{Q}^{\mathfrak{M}}$ (in the sense of ordered, topological, or valued field theory) gives the "reals" $\mathbf{R}^{\mathfrak{M}}$ and "complex numbers" $\mathbf{C}^{\mathfrak{M}} = \mathbf{R}^{\mathfrak{M}}(i)$. (The completion $\mathbf{R}^{\mathfrak{M}}$ was already used as a technical tool in [8], but here we make it the central structure of interest, along with $\mathbf{C}^{\mathfrak{M}}$.) We still need to consider rational approximations so that we have a way of translating our results back into the language of $\mathsf{VTC^0}$, and in particular, so that we can refer to the newly constructed functions in more sophisticated arguments that employ induction or related axiom schemata of $\mathsf{VTC^0}$, which only hold for properties expressible by TC^0 formulas in $\mathfrak{M}$.

[2]Earlier, Johannsen and Pollett [12] defined a theory C^0_2 that might be more convenient to work with; C^0_2 is a $\forall\exists\Sigma^b_1$-conservative extension of Δ^b_1-CR. Johannsen [11] introduced an extension $\mathsf{C}^0_2[\mathsf{div}]$ of C^0_2, which is however essentially identical to C^0_2 by results of [9].

The very fact that rational or Gaussian rational (i.e., $\mathbb{Q}(i)$) approximations of exp and log on suitable domains are TC^0-computable ensures that they are representable as provably total computable functions in VTC^0. But by itself, this only means that for each standard rational input, VTC^0 proves that the function has the right value, which is a very low bar to clear: e.g., it does not even imply that the approximations converge to a unique real or complex value. What we really need is that the functions can be represented in such a way that VTC^0 proves the most fundamental properties they have in the real world.

What these properties are is a judgement call. We consider the most salient properties of exp to be the identity $\exp(z+w) = \exp z \exp w$, and the shape of its domain, codomain, and preimages: real exp is an increasing bijection from $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}}$ (the logarithmically bounded reals) onto $\mathbf{R}^{\mathfrak{M}}_{>0}$; complex exp maps $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i\mathbf{R}^{\mathfrak{M}}$ to $\mathbf{C}^{\mathfrak{M}}_{\neq 0}$, and there is a constant π such that exp is $2\pi i$-periodic and maps $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i(-\pi, \pi]$ bijectively onto $\mathbf{C}^{\mathfrak{M}}_{\neq 0}$. (Actually, we also define $\exp z$ when $\operatorname{Re} z$ is negative, but not logarithmically bounded, putting $\exp z = 0$.) Of these, the most difficult to prove will be the surjectivity of exp, including the existence of π; we will need to construct log to prove this. The main properties of log are that it is a bijection from $\mathbf{C}^{\mathfrak{M}}_{\neq 0}$ onto $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i(-\pi, \pi]$, and a right inverse of exp, i.e., $\exp \log z = z$ (which implies the surjectivity of exp, as mentioned).

Our construction of exp is fairly straightforward, using the common power series (though we will need the existence of π and the $2\pi i$-periodicity of exp to extend its domain from $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}}$ to $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i\mathbf{R}^{\mathfrak{M}}$). The proof of $\exp(z+w) = \exp z \exp w$ is not very difficult either. The construction of log is much more complicated, as a power series only defines it on a neighbourhood of 1; we will need to extend it in several stages to eventually define it on all of $\mathbf{C}^{\mathfrak{M}}_{\neq 0}$. It will also take us a lot of work to prove the key right-inverse property $\exp \log z = z$: the basic strategy of our argument is to show $\log zw = \log z + \log w$ under suitable restrictions on z and w, which ensures that $\log \exp z$ obeys Cauchy's functional equation $\log \exp(z+w) = \log \exp z + \log \exp w$ (again, under certain conditions on z, w); coupled with the asymptotic expansion of exp near 0 and log near 1, we will derive $\log \exp z = z$ for small enough z, and use the injectivity of log to infer $\exp \log z = z$.

After we finish with exp and log, we proceed to define and show basic properties of complex powering z^w (with $\sqrt[n]{z}$ as a special case), iterated multiplication $\prod_{j<n} z_j$ for sequences of Gaussian rationals $z_j \in \mathbf{Q}^{\mathfrak{M}}(i)$, and last but not least, the promised hyperbolic, trigonometric, inverse hyperbolic, and inverse trigonometric functions.

Our principal motivation for developing the theory of exp, log, and other elementary analytic functions in VTC^0 is that it is intrinsically interesting. However, we also have one specific application concerning models of arithmetic in mind. Recall that an *integer part* of an ordered field R is a discretely ordered subring D such that all elements of R can be approximated within distance 1 in D; Shepherdson [24] proved that a model of arithmetic is an integer part of a real-closed field iff it satisfies IOpen.

An (ordered) *exponential field* is an ordered field $\langle R, +, \cdot, < \rangle$ endowed with an ordered group isomorphism $\exp\colon \langle R, +, < \rangle \to \langle R_{>0}, \cdot, < \rangle$. Ressayre [22] introduced the notion of an *exponential integer part* (EIP) of an exponential field $\langle R, \exp \rangle$, which is essentially an integer part of R whose positive part is closed under exp (here, we should think of exp as 2^x rather than the usual e^x).

In view of Shepherdson's characterization, we may wonder when a model of arithmetic is an EIP of a real-closed exponential field (RCEF), and in particular, whether this implies EXP (the totality of the usual 2^n function) or at least some nontrivial consequences of EXP. Note that the definition of EIP does not require exp to extend the usual 2^n.

Using our results on the construction of exp, we can show that the property of being an EIP of a RCEF has few (if any) first-order consequences: every countable model of $\mathsf{VTC^0}$ is an EIP of a RCEF, and every model of $\mathsf{VTC^0}$ has an elementary extension to an EIP of a RCEF. Notice that this is still nontrivial: while an $\mathfrak{M} \vDash \mathsf{VTC^0}$ is an integer part of $\mathbf{R}^{\mathfrak{M}}$ which is a real-closed field, the natural exp or 2^x function we construct is an isomorphism $\langle \mathbf{R}^{\mathfrak{M}}_{\mathbf{L}}, +, < \rangle \simeq \langle \mathbf{R}^{\mathfrak{M}}_{>0}, \cdot, < \rangle$ rather than $\langle \mathbf{R}^{\mathfrak{M}}, +, < \rangle \simeq \langle \mathbf{R}^{\mathfrak{M}}_{>0}, \cdot, < \rangle$, hence there is additional work needed. Since this is somewhat tangential to the main part of the present—already long—article, we relegated these results to the follow-up paper [10].

This paper is organized as follows. After this Introduction, Section 2 includes preliminaries on $\mathsf{VTC^0}$, its models, and approximation of real-valued functions. Section 3 is the core of the paper in which we construct exp and log and prove their fundamental properties: it starts with a summary of the main results, followed by a construction of exp in Section 3.1 and a construction of log in several steps in Sections 3.2–3.6. In Section 4, we introduce complex powering and iterated multiplication of Gaussian rationals, and in Section 5, we treat trigonometric, hyperbolic, inverse trigonometric, and inverse hyperbolic functions. Concluding remarks are presented in Section 6. Appendix A gives the formal details of proofs of the existence of TC^0 approximations of exp and log.

2 Preliminaries

We work with two-sorted (second-order) theories of bounded arithmetic in the style of Zambella [26]. Our main reference for these theories is Cook and Nguyen [4], including a detailed treatment of $\mathsf{VTC^0}$, however we present the main definitions here in order to fix notation.

The language $\mathcal{L}_2 = \langle 0, S, +, \cdot, \leq, \in, \|\cdot\| \rangle$ of two-sorted bounded arithmetic is a first-order language with equality with two sorts of variables, one for natural numbers (called *small* or *unary* numbers), and one for finite sets of small numbers, which can also be interpreted as *large* or *binary* numbers so that X represents $\sum_{u \in X} 2^u$. The standard convention is that variables of the first sort are written with lowercase letters $x, y, z, \dots$, and variables of the second sort with uppercase letters $X, Y, Z, \dots$; while we adhere to this convention in the introductory material here, we will not follow it in the rest of the paper (we will mostly work with binary numbers of various kind, and generally write them all in lower case in accordance with common mathematical practice). The symbols $0, S, +, \cdot, \leq$ of $\mathcal{L}_2$ denote the usual arithmetic operations and relation on the unary sort; $x \in X$ is the elementhood predicate, also written as $X(x)$, and the intended meaning of the $\|X\|$ function is the least unary number strictly greater than all elements of X. This function is usually denoted as $|X|$, however we reserve the latter symbol for the absolute value function, which we will use much more often. We write $x < y$ as an abbreviation for $x \leq y \wedge x \neq y$.

Bounded quantifiers are introduced by

$$\begin{aligned}\exists x \le t\, \varphi &\iff \exists x\, (x \le t \wedge \varphi),\\ \exists X \le t\, \varphi &\iff \exists X\, \bigl(\|X\| \le t \wedge \varphi\bigr),\end{aligned}$$

where t is a term of unary sort not containing x or X (respectively), and similarly for universal bounded quantifiers. A formula is Σ^B_0 if it contains no second-order quantifiers, and all its first-order quantifiers are bounded. A formula is Σ^B_i if it consists of i alternating blocks of bounded quantifiers, the first of which is existential, followed by a Σ^B_0 formula.

The theory V^0 in $\mathcal{L}_2$ can be axiomatized by the basic axioms

$$\begin{array}{ll} x + 0 = x & x + Sy = S(x+y)\\ x \cdot 0 = 0 & x \cdot Sy = x \cdot y + x\\ Sy \le x \to y < x & \|X\| \ne 0 \to \exists x\, \bigl(x \in X \wedge \|X\| = Sx\bigr)\\ x \in X \to x < \|X\| & \forall x\, (x \in X \leftrightarrow x \in Y) \to X = Y \end{array}$$

and the comprehension schema

$$(\varphi\text{-}\mathsf{COMP}) \qquad \exists X \le x\, \forall u < x\, \bigl(u \in X \leftrightarrow \varphi(u)\bigr)$$

for Σ^B_0 formulas φ, possibly with parameters not shown (but with no occurrence of X). We denote the set X whose existence is postulated by φ-COMP as $\{u < x : \varphi(u)\}$. Using COMP, V^0 proves the (unary number) induction and minimization schemata

$$\begin{array}{ll} (\varphi\text{-}\mathsf{IND}) & \varphi(0) \wedge \forall x\, \bigl(\varphi(x) \to \varphi(x+1)\bigr) \to \forall x\, \varphi(x),\\ (\varphi\text{-}\mathsf{MIN}) & \varphi(x) \to \exists y\, \bigl(\varphi(y) \wedge \forall z < y\, \neg\varphi(z)\bigr) \end{array}$$

for Σ^B_0 formulas φ.

Following [4], a set X codes a sequence (indexed by small numbers) of sets whose uth element is $X^{[u]} = \bigl\{x : \langle u, x\rangle \in X\bigr\}$, where $\langle x, y\rangle = \frac{1}{2}(x+y)(x+y+1)+y$. Likewise, we can code sequences of small numbers using $X^{(u)} = \|X^{[u]}\|$. While we stick to the official notation in formal contexts such as when stating axioms, elsewhere we will generally write $X = \langle X_i : i < n\rangle$ to indicate that X codes a sequence of length n whose ith element is X_i. The theory VTC^0 extends V^0 by the axiom

$$\forall n, X\, \exists Y\, \bigl[Y^{(0)} = 0 \wedge \forall i < n\, \bigl((i \notin X \to Y^{(i+1)} = Y^{(i)}) \wedge (i \in X \to Y^{(i+1)} = Y^{(i)} + 1)\bigr)\bigr],$$

asserting that for any set X, there is a sequence Y supplying the counting function $Y^{(i)} = \operatorname{card}(X \cap \{0, \dots, i-1\})$.

TC^0 was originally introduced by Hajnal et al. [6] as a non-uniform class, but we define it as the class of languages $L \subseteq \{0,1\}^*$ recognizable by a DLOGTIME-uniform family of polynomial-size constant-depth circuits using $\neg$ and unbounded fan-in $\wedge$, $\vee$, and Majority gates; equivalently, it consists of languages computable by $O(\log n)$-time threshold Turing machines with $O(1)$ thresholds, or by constant-time TRAM with polynomially many processors [19]. In terms of descriptive complexity, a language is in TC^0 iff the corresponding class of finite structures is definable in FOM, first-order logic with majority quantifiers [2].

In connection with bounded arithmetic, it is convenient to consider not just the complexity of languages, but of predicates $P(X_1,\dots,X_n,x_1,\dots,x_m)$ with several inputs, where $X_i \in \{0,1\}^*$ as usual, and $x_i \in \mathbb{N}$ are written in unary. It is straightforward to generalize TC^0 and similar classes to this context, see [4, §IV.3] for details. Likewise, we consider computability of functions. A function $F\colon (\{0,1\}^*)^n \times \mathbb{N}^m \to \{0,1\}^*$ is a TC^0 function if $\|F(X_1,\dots,X_n,x_1,\dots,x_m)\| \le p\big(\|X_1\|,\dots,x_1,\dots\big)$ for some polynomial p, and the bit-graph $\big\{\langle\vec{X},\vec{x},i\rangle : \mathrm{bit}\big(F(\vec{X},\vec{x}),i\big)=1\big\}$ is a TC^0 predicate; a unary number function $f\colon (\{0,1\}^*)^n \times \mathbb{N}^m \to \mathbb{N}$ is a TC^0 function if $f(\vec{X},\vec{x}) \le p\big(\|X_1\|,\dots,x_1,\dots\big)$, and the graph $\big\{\langle\vec{X},\vec{x},y\rangle : f(\vec{x},\vec{X})=y\big\}$ is TC^0. The class of TC^0 functions is denoted FTC^0. We note that by results of [7], class $\mathcal{K}$ of Constable [3] consists exactly of TC^0 functions $(\{0,1\}^*)^n \to \{0,1\}^*$ where the inputs and output are interpreted as natural numbers written in binary.

All TC^0 functions have provably total Σ^B_1 definitions in VTC^0. More precisely, as shown in [4, §IX.3], VTC^0 has a conservative extension $\overline{\mathsf{VTC}^0}$ by Σ^B_1-definable functions such that every TC^0 function is represented by a function symbol in $\overline{\mathsf{VTC}^0}$, and $\overline{\mathsf{VTC}^0}$ proves comprehension, induction, and minimization for Σ^B_0 formulas in the expanded language of $\overline{\mathsf{VTC}^0}$; we will call such formulas TC^0 *formulas*, and identify $\overline{\mathsf{VTC}^0}$ with VTC^0, using TC^0 functions freely when working in VTC^0 or in its models.

VTC^0 can define (as TC^0 functions) $+$, $-$, $\cdot$, and $<$ on binary natural numbers, and prove that they form a non-negative part of a discretely ordered ring; in fact, they satisfy IOpen (induction for open formulas in the language of ordered rings, which entails integer division) by the results of [8, 9].

If $\mathfrak{M} \vDash \mathsf{VTC}^0$, we denote by $\langle \mathbf{N}^{\mathfrak{M}},0,1,+,\cdot,<\rangle$ the second sort of $\mathfrak{M}$ interpreted as a set of binary natural numbers along with its arithmetic structure. We extend it with negative numbers to form the discretely ordered ring $\langle \mathbf{Z}^{\mathfrak{M}},0,1,+,\cdot,<\rangle$ (the *integers of* $\mathfrak{M}$). Let $\langle \mathbf{Q}^{\mathfrak{M}},0,1,+,\cdot,<\rangle$ (the *rationals of* $\mathfrak{M}$) be the fraction field of $\mathbf{Z}^{\mathfrak{M}}$, let $\langle \mathbf{R}^{\mathfrak{M}},0,1,+,\cdot,<\rangle$ (the *reals of* $\mathfrak{M}$) be the *completion* (see below for more details) of $\mathbf{Q}^{\mathfrak{M}}$, which is a real-closed field by [8, 9], and let $\langle \mathbf{C}^{\mathfrak{M}},0,1,+,\cdot\rangle$ (the *complex numbers of* $\mathfrak{M}$) be its algebraic closure, i.e., $\mathbf{C}^{\mathfrak{M}} = \mathbf{R}^{\mathfrak{M}}(i)$ where $i^2=-1$. We also consider the field $\mathbf{Q}^{\mathfrak{M}}(i)$ of *Gaussian rationals of* $\mathfrak{M}$. The structures $\mathbf{Z}^{\mathfrak{M}}$, $\mathbf{Q}^{\mathfrak{M}}$, and $\mathbf{Q}^{\mathfrak{M}}(i)$ are interpretable in $\mathfrak{M}$, by formulas independent of $\mathfrak{M}$ (albeit with non-absolute equality in the cases of $\mathbf{Q}^{\mathfrak{M}}$ and $\mathbf{Q}^{\mathfrak{M}}(i)$, as we do not know how to reduce fractions to lowest terms in VTC^0), but in general, $\mathbf{R}^{\mathfrak{M}}$ and $\mathbf{C}^{\mathfrak{M}}$ are not (e.g., it is easy to show that $\mathbf{R}^{\mathfrak{M}}$ is always uncountable; moreover, if $\mathfrak{M}$ has countable cofinality, then $|\mathbf{R}^{\mathfrak{M}}| = |\mathfrak{M}|^{\omega}$).

The completion of an ordered field $\langle F,+,\cdot,<\rangle$ can be described in several equivalent ways. One way using only the basic structure of ordered fields is as follows (cf. [23]). A *cut* in F is a pair $\langle A,B\rangle$ of sets such that $F = A\cup B$, $\inf\{b-a : b\in B, a\in A\}=0$, and A has no largest element; F is *complete* if $\min B$ exists for every cut $\langle A,B\rangle$. The *completion* of F is a complete ordered field $\langle \hat{F},+,\cdot,<\rangle$ such that F is a dense subfield of $\hat{F}$ (i.e., every non-degenerate interval of $\hat{F}$ intersects F). The completion of F is unique up to F-isomorphism; it can be explicitly constructed by endowing the set of all cuts of F with suitable structure.

We will most often use a topological description of $\hat{F}$ (see [25]). The interval topology makes

F a topological field, and therefore a uniform space[3] with a fundamental system of entourages $\mathcal{U} = \{U_\varepsilon : \varepsilon \in F_{>0}\}$, where $U_\varepsilon = \{\langle x, y\rangle \in F^2 : |x - y| \le \varepsilon\}$. F is *complete* as a uniform space if every Cauchy net in F converges. Here, a *net* is an indexed set $A = \{a_i : i \in I\} \subseteq F$ where $\langle I, \le\rangle$ is a directed poset; A is a *Cauchy net* if for every $U \in \mathcal{U}$, there exists $i_0 \in I$ such that $\langle a_i, a_j\rangle \in U$ for all $i, j \ge i_0$, and A *converges* to $a \in F$, written $a = \lim_{i\in I} a_i$, if for every $U \in \mathcal{U}$, there exists $i_0 \in I$ such that $\langle a_i, a\rangle \in U$ for all $i \ge i_0$. (In our applications, I will usually be a totally ordered set such as $\langle \mathbf{L}^{\mathfrak{M}}, \le\rangle$.) The *completion* of F is a complete uniform space $\hat{F}$ such that F is a (topologically) dense subspace of $\hat{F}$; it is again unique up to F-isomorphism. The key property of $\hat{F}$ is that every uniformly continuous function from F to a complete uniform space S extends uniquely to a uniformly continuous function $\hat{F} \to S$. The ring operations on F extend to continuous operations on $\hat{F}$ that make it a topological ring. For ordered fields F, the completion $\hat{F}$ is in fact an ordered field, and coincides with the order-theoretic completion of F as above.

Apart from the ordered fields $\mathbf{Q}^{\mathfrak{M}}$ and $\mathbf{R}^{\mathfrak{M}}$, we will also consider $\mathbf{Q}^{\mathfrak{M}}(i)$ and $\mathbf{C}^{\mathfrak{M}}$ as topological fields; in particular, $\mathbf{C}^{\mathfrak{M}}$ is the completion of $\mathbf{Q}^{\mathfrak{M}}(i)$. Consequently, a Cauchy net in $\mathbf{Q}^{\mathfrak{M}}(i)$ has a unique limit in $\mathbf{C}^{\mathfrak{M}}$, and any uniformly continuous function $D \to \mathbf{C}^{\mathfrak{M}}$, $D \subseteq \mathbf{Q}^{\mathfrak{M}}(i)$, has a unique uniformly continuous extension to a function $\overline{D} \to \mathbf{C}^{\mathfrak{M}}$; we will commonly use these facts.

If an ordered field F is archimedean (which for our $\mathbf{Q}^{\mathfrak{M}}$ happens only when $\mathfrak{M}$ is the standard model), it embeds in $\mathbb{R}$, and its completion is just $\mathbb{R}$. Otherwise, F is a *valued field* with valuation ring $\{x \in F : \exists n \in \mathbb{N}\, |x| \le n\}$, and $\hat{F}$ can be described as the valued field completion of F; see [5] and [8, §6] for details.

The unary number sort of $\mathfrak{M}$ embeds (via a TC^0 function) into $\mathbf{N}^{\mathfrak{M}}$ as an initial segment of *logarithmic numbers*, which we denote $\mathbf{L}^{\mathfrak{M}}$. We define the *logarithmically bounded* integers, reals, etc., by

$$\mathbf{C}^{\mathfrak{M}}_{\mathbf{L}} = \{z \in \mathbf{C}^{\mathfrak{M}} : \exists n \in \mathbf{L}^{\mathfrak{M}}\, |z| \le n\},$$

$\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} = \mathbf{R}^{\mathfrak{M}} \cap \mathbf{C}^{\mathfrak{M}}_{\mathbf{L}}$, $\mathbf{Q}^{\mathfrak{M}}_{\mathbf{L}} = \mathbf{Q}^{\mathfrak{M}} \cap \mathbf{C}^{\mathfrak{M}}_{\mathbf{L}}$, and $\mathbf{Z}^{\mathfrak{M}}_{\mathbf{L}} = \mathbf{Z}^{\mathfrak{M}} \cap \mathbf{C}^{\mathfrak{M}}_{\mathbf{L}}$. Here, the complex absolute value $|z| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$ for $z = x + iy \in \mathbf{C}^{\mathfrak{M}}$ is a well-defined element of $\mathbf{R}^{\mathfrak{M}}$ as the latter is real-closed. However, notice that the definition of $\mathbf{C}^{\mathfrak{M}}_{\mathbf{L}}$ would not change if we used $|x| + |y|$, $\max\{|x|, |y|\}$, or $x^2 + y^2$ in place of $|z|$.

We also write $\mathbf{R}^{\mathfrak{M}}_{>0} = \{x \in \mathbf{R}^{\mathfrak{M}} : x > 0\}$, $\mathbf{C}^{\mathfrak{M}}_{\ne 0} = \{z \in \mathbf{C}^{\mathfrak{M}} : z \ne 0\}$, etc. We define the open and closed disks $D^{\mathfrak{M}}_r(z_0) = \{z \in \mathbf{C}^{\mathfrak{M}} : |z - z_0| < r\}$, $\overline{D}^{\mathfrak{M}}_r(z_0) = \{z \in \mathbf{C}^{\mathfrak{M}} : |z - z_0| \le r\}$ for $z_0 \in \mathbf{C}^{\mathfrak{M}}$, $r \in \mathbf{R}^{\mathfrak{M}}_{>0}$.

We will usually work with a fixed model $\mathfrak{M} \vDash \mathsf{VTC}^0$, in which case we will omit the $\mathfrak{M}$ superscripts to simplify the notation; we do this for the rest of this section as well.

When manipulated (as inputs or outputs) by TC^0 functions, elements of $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{Q}(i)$ are represented in binary in the expected way (i.e., rationals are represented by fractions of binary integers, and Gaussian rationals by their real and imaginary parts), while elements of $\mathbf{L}$ or $\mathbf{Z}_{\mathbf{L}}$ are represented as unary integers. However, we do not introduce a standard representation for elements of $\mathbf{Q}_{\mathbf{L}}$ or $\mathbf{Q}_{\mathbf{L}}(i)$; they will be treated as elements of $\mathbf{Q}$ or $\mathbf{Q}(i)$, and if needed,

[3] We require all uniform spaces and topological groups to be Hausdorff.

the function will explicitly take another input enforcing the logarithmic restriction (such as an element of $\mathbf{L}$ bounding the absolute value).

Some of our results will state the existence of TC^0 functions with certain properties. Even though we otherwise work relative to a fixed model $\mathfrak{M} \vDash \mathsf{VTC}^0$, such statements are always meant to be *uniform*: i.e., interpreted as "there is a specific function symbol of $\overline{\mathsf{VTC}^0}$ such that for every model $\mathfrak{M} \vDash \mathsf{VTC}^0$, etc."

If n is a unary natural number, 2^n is represented as a binary number by the set $\{n\}$. Thus, we can define a TC^0 function $2^n \colon \mathbf{L} \to \mathbf{N}$ satisfying $2^1 = 2$ and $2^{n+m} = 2^n 2^m$. Much more generally, given a sequence $\langle x_j : j < n \rangle$ coded in $\mathfrak{M}$, where $x_j \in \mathbf{Z}$ and $n \in \mathbf{L}$, there is a TC^0 definition of $\sum_{j<n} x_j$ and (due to [9]) $\prod_{j<n} x_j$ satisfying

$$\sum_{j<0} x_j = 0, \qquad \sum_{j<n+1} x_j = x_n + \sum_{j<n} x_j,$$
$$\prod_{j<0} x_j = 1, \qquad \prod_{j<n+1} x_j = x_n \cdot \prod_{j<n} x_j.$$

We can extend these operations to coded sequences of rational fractions by

$$\sum_{j<n} \frac{p_j}{q_j} = \frac{\sum_{j<n} p_j \prod_{l \neq j} q_l}{\prod_{j<n} q_j},$$
$$\prod_{j<n} \frac{p_j}{q_j} = \frac{\prod_{j<n} p_j}{\prod_{j<n} q_j}.$$

We can further extend $\sum$ to coded sequences of Gaussian rationals with

$$\sum_{j<n} (x_j + i y_j) = \sum_{j<n} x_j + i \sum_{j<n} y_j.$$

Defining $\prod$ for such sequences is problematic, as the obvious formula requires a sum of 2^n terms; we will see later how to do it using exp and log, but at this point, we can at least define powering using

$$(x+iy)^n = \sum_{m \le n/2} \binom{n}{2m} (-1)^m x^{n-2m} y^{2m} + i \sum_{m<n/2} \binom{n}{2m+1} (-1)^m x^{n-2m-1} y^{2m+1}.$$

We can extend z^n to a function $\mathbf{C} \times \mathbf{L} \to \mathbf{C}$ as follows: for a fixed $n \in \mathbf{L}$, z^n is uniformly continuous on $\overline{D}_r(0) \cap \mathbf{Q}(i)$ for each $r \in \mathbf{R}_{>0}$, as

$$|z - w| \le \delta \implies |z^n - w^n| = \Big| (z-w) \sum_{j<n} z^j w^{n-1-j} \Big| \le (n-1) r^{n-1} \delta$$

using Lemma 2.1 below. Thus, it has a unique continuous extension to each $\overline{D}_r(0)$, and therefore a unique continuous extension to $\mathbf{C}$, which we still denote z^n. For $z \neq 0$, we also define $z^{-n} = 1/z^n$. Powering satisfies the basic identities $z^0 = 1$, $z^1 = z$, $z^{n+m} = z^n z^m$, $z^{nm} = (z^n)^m$, and $(zw)^n = z^n w^n$: for $z, w \in \mathbf{Q}(i)$, this either holds immediately, or can be proved by induction on m; then we use the density of $\mathbf{Q}(i)$ in $\mathbf{C}$, observing that both sides of each identity are continuous in z. (For $(zw)^n = z^n w^n$, we do it in two steps: first as a function of $z \in \mathbf{C}$ with fixed $w \in \mathbf{Q}(i)$, then as a function of $w \in \mathbf{C}$ for fixed $z \in \mathbf{C}$.) It is also easy to check that x^n is increasing on $\mathbf{R}_{>0}$ for $n > 0$, and decreasing for $n < 0$.

For any $z \in \mathbf{C}$, the absolute value $|z|$ is a well-defined element of $\mathbf{R}$, but if $z \in \mathbf{Q}(i)$, we do not necessarily have $|z| \in \mathbf{Q}$. This is a hindrance to its use in arguments by induction, bounded sums and products, etc. For this reason, we consider the predicate $|z| \le r$ for $z = x + iy \in \mathbf{Q}(i)$ and $r \in \mathbf{Q}$, which can be equivalently defined without reference to $\mathbf{R}$ by

$$|z| \le r \iff r \ge 0 \wedge r^2 \ge x^2 + y^2 (= z\overline{z}).$$

The following lemma summarizes its basic properties (some of which hold even for real arguments, as indicated).

Lemma 2.1

(i) *Let $z, w \in \mathbf{C}$ and $r, s \in \mathbf{R}$. If $|z| \le r$ and $|w| \le s$, then $|z + w| \le r + s$ and $|zw| \le rs$.*

(ii) *Let $\langle z_j : j < n \rangle$ and $\langle r_j : j < n \rangle$ be sequences of elements of $\mathbf{Q}(i)$ and $\mathbf{Q}$ (respectively) coded in $\mathfrak{M}$. If $|z_j| \le r_j$ for each $j < n$, then $\left|\sum_{j<n} z_j\right| \le \sum_{j<n} r_j$.*

(iii) *Let $z \in \mathbf{C}$ and $r \in \mathbf{R}$. If $|z| \le r$, then $|z^n| \le r^n$ for each $n \in \mathbf{L}$.*

Proof: (i): $|zw| \le rs$ follows immediately from $(zw)\overline{zw} = (z\overline{z})(w\overline{w})$. Write $z = x + iy$ and $w = u + iv$. Since

$$(xu + yv)^2 \le (xu + yv)^2 + (xv - yu)^2 = (x^2 + y^2)(u^2 + v^2) \le r^2 s^2,$$

we have $xu + yv \le rs$, thus

$$(x + u)^2 + (y + v)^2 = x^2 + y^2 + u^2 + v^2 + 2(xu + yv) \le r^2 + s^2 + 2rs = (r + s)^2,$$

which means $|z + w| \le r + s$.

(ii) follows from (i) by induction on n.

(iii): If $z \in \mathbf{Q}(i)$ and $r \in \mathbf{Q}$, then $|z| \le r$ implies $|z^n| \le r^n$ by induction on n using (i). For general z and r, we then use the density of $\mathbf{Q}(i)$ in $\mathbf{C}$ and the continuity of z^n and r^n. □

It will be most convenient for us to present constructions and arguments in a model-theoretic way, working directly with functions $f\colon \mathbf{C} \to \mathbf{C}$ and the like. However, we need to keep in mind that $\mathbf{R}$ and $\mathbf{C}$ are not definable in $\mathfrak{M}$, and most of their elements cannot be represented as objects of $\mathfrak{M}$. Since we are ultimately interested in what is provable in the theory VTC^0, we need a way of restating properties of $\mathbf{C}$-valued functions as first-order properties of $\mathfrak{M}$. Moreover, we want these properties to be definable by low-complexity (TC^0) formulas so that they can be used in induction arguments, comprehension instances, etc. We will accomplish this by means of *approximation* by TC^0 functions. We formalize this concept as follows.

Consider $f\colon D \to \mathbf{C}$, where $D \subseteq \mathbf{C}$ is such that $D \cap \mathbf{Q}(i)$ is dense in D. An *additive* TC^0 *approximation* of f is a TC^0 function $f_+\colon \mathbf{Q}(i) \times \mathbf{L} \to \mathbf{Q}(i)$ such that

$$|f_+(z, n) - f(z)| \le 2^{-n}$$

for all $z \in D \cap \mathbf{Q}(i)$ and $n \in \mathbf{L}$. A *multiplicative* TC^0 *approximation* of f is $f_\times\colon \mathbf{Q}(i) \times \mathbf{L} \to \mathbf{Q}(i)$ such that

$$|f_\times(z,n) - f(z)| \le 2^{-n}|f(z)|$$

for all $z \in D \cap \mathbf{Q}(i)$ and $n \in \mathbf{L}$; i.e., if $f(z) = 0$, then $f_\times(z,n) = 0$, and if $f(z) \ne 0$, then

$$\left|\frac{f_\times(z,n)}{f(z)} - 1\right| \le 2^{-n}.$$

Multiplicative approximation is stronger than additive approximation in the following sense.

Lemma 2.2 *For any function $f\colon D \to \mathbf{C}$, $D \subseteq \mathbf{C}$, the following are equivalent.*

(i) *f has a multiplicative TC^0 approximation $f_\times$.*

(ii) *f has an additive TC^0 approximation f_+, and there exists a TC^0 function $h\colon \mathbf{Q}(i) \to \mathbf{L}$ (with unary output) such that*

$$f(z) \ne 0 \implies |f(z)| \ge 2^{-h(z)}$$

for all $z \in D \cap \mathbf{Q}(i)$.

Proof:

(i) $\to$ (ii): Observe that $|f(z)| \le 2|f_\times(z,1)|$. This allows us to define a TC^0 function $t\colon \mathbf{Q}(i) \to \mathbf{L}$ such that $|f(z)| \le 2^{t(z)}$ for all $z \in D \cap \mathbf{Q}(i)$: given z, we compute $|f_\times(z,1)|^2 \in \mathbf{Q}_{\ge 0}$, and using integer division and the length function, we compute $t' = \big\|\lceil |f_\times(z,1)|^2 \rceil\big\| \in \mathbf{L}$ so that $2^{t'} > |f_\times(z,1)|^2$; then $t(z) = 1 + \lceil t'/2 \rceil$ works. Thus, $f_+(z,n) = f_\times\big(z, n + t(z)\big)$ is an additive approximation of f.

If $f(z) \ne 0$, then $f_\times(z,1) \ne 0$, and a similar argument as above gives us a TC^0 function h' such that $2^{h'(z)} \ge |f_\times(z,1)|^{-2}$; then $h(z) = 1 + \lceil h'/2 \rceil$ satisfies $|f(z)| \ge 2^{-h(z)}$, using the fact that $|f_\times(z,1)| \le \frac{3}{2}|f(z)|$.

(ii) $\to$ (i): First, given $z \in D \cap \mathbf{Q}(i)$, we can decide in TC^0 whether $f(z) = 0$, as

$$\begin{aligned} f(z) = 0 &\implies \big|f_+\big(z, h(z)+2\big)\big| \le \tfrac{1}{4}2^{-h(z)}, \\ f(z) \ne 0 &\implies \big|f_+\big(z, h(z)+2\big)\big| \ge |f(z)| - \tfrac{1}{4}2^{-h(z)} \ge \tfrac{3}{4}2^{-h(z)}. \end{aligned}$$

Thus,

$$f_\times(z,n) = \begin{cases} 0 & \text{if } f(z) = 0, \\ f_+\big(z, h(z)+n\big) & \text{otherwise} \end{cases}$$

gives a multiplicative TC^0 approximation of f. □

In practice, TC^0 approximation functions will often need additional inputs. For example, to compute a TC^0 approximation of $\exp z$, it is not enough to have z (in binary) as input, as the output may be exponentially large; we will also require a bound $r \in \mathbf{L}$ (in unary) such that $|z| \le r$, or at least $\operatorname{Re} z \le r$. We will employ the following terminology.

For a function $f\colon D \to \mathbf{C}$ as above, and a property $P(z,r)$, we say that a TC^0 function $f_+(z,r,n)$ is an *additive approximation of $f(z)$ parametrized by r such that $P(z,r)$* if

$$P(z,r) \implies |f_+(z,r,n) - f(z)| \le 2^{-n}$$

for all $z \in D \cap \mathbf{Q}(i)$ and $r, n \in \mathbf{L}$; analogously for multiplicative approximation. We also require that for every $z \in D \cap \mathbf{Q}(i)$, there exists $r \in \mathbf{L}$ such that $P(z,r)$.

The following facts are useful for basic manipulation of multiplicative approximations.

Lemma 2.3 *Let $z, w \in \mathbf{C}$ and $\varepsilon, \delta \in \mathbf{R}_{\ge 0}$.*

(i) *If $|z-1| \le \varepsilon$ and $|w-1| \le \delta$, then $|zw-1| \le \varepsilon + \delta + \varepsilon\delta$.*

(ii) *If $|z^2 - 1| \le 2\varepsilon - \varepsilon^2$ and $\operatorname{Re} z \ge 0$, then $|z-1| \le \varepsilon$.*

(iii) *If $|z-1| \le \varepsilon/(1+\varepsilon)$, then $|z^{-1} - 1| \le \varepsilon$.*

(iv) *Let $z = x + iy$ and $w = u + iv$ with $x, y, u, v \in \mathbf{R}$. Assuming $x, y \ne 0$,*

$$\left|\frac{u}{x} - 1\right| \le \varepsilon \wedge \left|\frac{v}{y} - 1\right| \le \varepsilon \implies \left|\frac{w}{z} - 1\right| \le \varepsilon.$$

Proof:
(i): $|zw-1| \le |zw-w| + |w-1| \le |w|\varepsilon + \delta \le (1+\delta)\varepsilon + \delta$ using Lemma 2.1.
(ii): Put $r = |1-z|$. We have $|1+z| \ge 2 - r$ by Lemma 2.1, hence

$$2\varepsilon - \varepsilon^2 \ge \left|1 - z^2\right| = |1-z|\,|1+z| \ge r(2-r).$$

Thus, $(1-\varepsilon)^2 \le (1-r)^2$, i.e., $r \le \min\{\varepsilon, 2-\varepsilon\}$ or $r \ge \max\{\varepsilon, 2-\varepsilon\}$. Since $\operatorname{Re} z \ge 0$, we have $|1+z| \ge r$; thus, if $r \ge 2-\varepsilon$ and $r > \varepsilon$, we have $\left|1 - z^2\right| = r|1+z| > \varepsilon|1+z| \ge \varepsilon(2-\varepsilon)$, a contradiction. Hence the only possibility is $r \le \varepsilon$.
(iii): We have $|z| \ge 1 - \varepsilon/(1+\varepsilon) = 1/(1+\varepsilon)$, hence $|z^{-1} - 1| = |z-1|/|z| \le \varepsilon$.
(iv): $|w-z|^2 = |u-x|^2 + |v-y|^2 \le \varepsilon^2|x|^2 + \varepsilon^2|y|^2 = \varepsilon^2|z|^2$. ☐

3 Exponential and logarithm

In this section, which is the main part of the paper, we will construct functions exp and log on suitable subsets of $\mathbf{C}^{\mathfrak{M}}$, and verify their basic properties. Since especially the construction of log will be somewhat complicated, proceeding in several stages, we will need many technical lemmas along the way, which will be mixed with bits and pieces of the intended end results. To help the reader not lose track of what is going on, we start by collecting the most useful results and stating them in one place upfront.

Let us fix a model $\mathfrak{M} \vDash \mathsf{VTC}^0$ for the duration of this section. Put

$$\mathbf{R}_{\downarrow\mathbf{L}} = \{x \in \mathbf{R} : \exists n \in \mathbf{L}\; x \le n\} = \mathbf{R}_{\mathbf{L}} \cup \mathbf{R}_{<0}.$$

We are going to define functions

$$\exp\colon \mathbf{R}_{\downarrow\mathbf{L}} + i\mathbf{R} \to \mathbf{C}$$

(in Lemma 3.56, following up on Definition 3.3 and Lemmas 3.5 and 3.9) and

$$\log\colon \mathbf{C}_{\neq 0} \to \mathbf{C}_{\mathbf{L}}$$

(in Definition 3.34, following up on Definition 3.12, Lemmas 3.14, 3.19, and 3.21, and Definitions 3.27 and 3.24, and renamed to log in view of Lemma 3.58), as well as a constant $\pi \in \mathbf{R}_{>0}$ and the argument function $\arg\colon \mathbf{C}_{\neq 0} \to \mathbf{R}_{\mathbf{L}}$ (in Definition 3.38).

Theorem 3.1 *The functions* exp *and* log *have the following properties.*

(i) *For all* $z, w \in \operatorname{dom}(\exp)$, $\exp(z+w) = \exp z \exp w$, *and* $\exp \overline{z} = \overline{\exp z}$.

(ii) $\exp \restriction \mathbf{R}_{\mathbf{L}} + i\mathbf{R}$ *is a surjective group homomorphism* $\langle \mathbf{R}_{\mathbf{L}} + i\mathbf{R}, +, 0, - \rangle \to \langle \mathbf{C}_{\neq 0}, \cdot, 1, {}^{-1} \rangle$ *with kernel* $2\pi i\mathbf{Z}$.

(iii) $\exp z = 0$ *iff* $\operatorname{Re} z \in \mathbf{R}_{\downarrow\mathbf{L}} \smallsetminus \mathbf{R}_{\mathbf{L}}$.

(iv) log *maps* $\mathbf{C}_{\neq 0}$ *onto* $\mathbf{R}_{\mathbf{L}} + i(-\pi, \pi]$, *and it is a right inverse of* exp, *i.e.,* $\exp \log z = z$ *for all* $z \in \mathbf{C}_{\neq 0}$. *Also,* $\log \exp z = z$ *for all* $z \in \mathbf{R}_{\mathbf{L}} + i(-\pi, \pi]$.

(v) $\exp \restriction \mathbf{R}_{\mathbf{L}}$ *is an ordered group isomorphism* $\langle \mathbf{R}_{\mathbf{L}}, +, 0, -, < \rangle \to \langle \mathbf{R}_{>0}, \cdot, 1, {}^{-1}, < \rangle$ *whose inverse is* $\log \restriction \mathbf{R}_{>0}$.

(vi) exp *is continuous, and it is uniformly continuous on* $(-\infty, r] + i\mathbf{R}$ *for each* $r \in \mathbf{L}$; log *is continuous on* $\mathbf{C} \smallsetminus \mathbf{R}_{\leq 0}$ *and on* $\{z \neq 0 : \operatorname{Im} z \geq 0\}$, *and for each* $\varepsilon \in \mathbf{R}_{>0}$, *it is uniformly continuous on* $\bigl\{z : |z| \geq \varepsilon \wedge (\operatorname{Re} z \geq 0 \vee \operatorname{Im} z \geq 0 \vee \operatorname{Im} z \leq -\varepsilon)\bigr\}$.

(vii) $|\exp z| = \exp \operatorname{Re} z$ *for all* $z \in \operatorname{dom}(\exp)$, *and* $\log z = \log|z| + i \arg z$ *for all* $z \in \mathbf{C}_{\neq 0}$.

(viii) arg *maps the quadrant* $\{z \neq 0 : \operatorname{Re} z, \operatorname{Im} z \geq 0\}$ *to* $\bigl[0, \frac{\pi}{2}\bigr]$, $\{z \neq 0 : \operatorname{Re} z \leq 0, \operatorname{Im} z \geq 0\}$ *to* $\bigl[\frac{\pi}{2}, \pi\bigr]$, $\{z \neq 0 : \operatorname{Re} z \geq 0, \operatorname{Im} z \leq 0\}$ *to* $\bigl[-\frac{\pi}{2}, 0\bigr]$, *and* $\{z : \operatorname{Re} z \leq 0, \operatorname{Im} z < 0\}$ *to* $\bigl(-\pi, -\frac{\pi}{2}\bigr]$. *In each quadrant, it increases or decreases in tandem with* $\operatorname{Re} \operatorname{sgn} z$ *and* $\operatorname{Im} \operatorname{sgn} z$ *as determined in Lemma 3.40, where* $\operatorname{sgn} z = z/|z|$.

(ix) *If* $|z| \leq \frac{3}{2}$, *then* $\bigl|\exp z - (1+z)\bigr| \leq |z|^2$. *If* $|z| \leq \frac{1}{2}$, *then* $\bigl|\log(1+z) - z\bigr| \leq |z|^2$.

(x) *If* $z \in \mathbf{C}_{\mathbf{L}}$ *and* $n \in \mathbf{Z}_{\mathbf{L}}$, *then* $\exp nz = (\exp z)^n$.

(xi) *If* $z \in \mathbf{C}$ *and* $n \in \mathbf{L}_{>0}$ *is such that* $n \geq \max\bigl\{2|z|, |z|^2\bigr\}$, *then*

$$\left| \frac{\bigl(1 + \frac{z}{n}\bigr)^n}{\exp z} - 1 \right| \leq \frac{2|z|^2}{n}.$$

(xii) *For all* $x \in \mathbf{R}_{\downarrow\mathbf{L}}$, $\exp x \geq 1 + x$. *Consequently,* $\exp \restriction \mathbf{R}_{\downarrow\mathbf{L}}$ *is convex: for all* $x, y \in \mathbf{R}_{\downarrow\mathbf{L}}$ *and* $t \in [0,1]$,

$$(y - x) \exp x \leq \exp y - \exp x \leq (y - x) \exp y,$$
$$\exp\bigl((1-t)x + ty\bigr) \leq (1-t) \exp x + t \exp y.$$

(xiii) $\exp z$ *has* TC^0 *additive approximation* $E_+(z,r,n)$ *for* $z \in \mathbf{Q}_{\downarrow\mathbf{L}} + i\mathbf{Q}$, *parametrized by* $r \in \mathbf{L}$ *such that* $\operatorname{Re} z \le r$, *and* TC^0 *multiplicative approximation* $E_\times(z,r,n)$ *for* $z \in \mathbf{Q}_{\mathbf{L}} + i\mathbf{Q}$, *parametrized by* $r \in \mathbf{L}$ *such that* $|\operatorname{Re} z| \le r$. *For* $z \in \mathbf{Q}(i) \smallsetminus \{0\}$, $\log z$ *has* TC^0 *additive approximation* $L_+(z,n)$ *and* TC^0 *multiplicative approximation* $L_\times(z,n)$.

While Theorem 3.1 is for the most part a summary of various lemmas that appear separately throughout the course of Section 3, we will formally prove it at the end of the section.

We omit listing some useful properties that can be inferred from the above: in particular, (ii) and (iv) imply Lemma 3.43; we mention though that they also imply a variant of Lemma 3.37 (i) and (ii) with a perhaps clearer geometric meaning:

Corollary 3.2 *If* $z, w \in \mathbf{C}_{\neq 0}$ *satisfy* $\arg z + \arg w \in (-\pi, \pi]$, *then* $\log zw = \log z + \log w$. $\square$

Further facts of interest that will be proved in this section are the bounds on π in Proposition 3.44, bounds on $e = \exp 1$ in Lemma 3.54, and properties of the complex square root function in §3.5.

We should comment on the decision to put $\exp z = 0$ for $\operatorname{Re} z \in \mathbf{R}_{\downarrow\mathbf{L}} \smallsetminus \mathbf{R}_{\mathbf{L}}$, rather than leaving it undefined. This violates the basic property that $\exp z \neq 0$ for all z. However, it retains other fundamental properties of exp, in particular $\exp(z+w) = \exp z \exp w$, and the monotonicity of exp on the reals. Conceptually, it seems to be the right thing to do, as $|\exp z|$ drops down to 0 as $\operatorname{Re} z \to -\infty$ for $\operatorname{Re} z \in \mathbf{R}_{\mathbf{L}}$. (By the same reasoning, we could also define $\exp z = \infty$ when $\operatorname{Re} z > \mathbf{R}_{\mathbf{L}}$, but we prefer to keep functions finite.)

Perhaps the best technical reason for this definition stems from point (xiii). Recall that our overarching goal is to explore what is provable in the theory VTC^0, which cannot directly talk about $\mathbf{C}$-valued functions such as exp or log; from this viewpoint, the TC^0 approximations of these functions are more fundamental than the functions themselves, which are just figments of our imagination. Now, additive approximation $E_+(z,r,n)$ of $\exp z$ is most naturally presented with a parameter $r \in \mathbf{L}$ such that $\operatorname{Re} z \le r$ as indicated, as this is exactly what is needed to keep the approximation efficiently computable. However, there is no way for a TC^0 function to distinguish inputs z with $\operatorname{Re} z \in \mathbf{Q}_{\downarrow\mathbf{L}} \smallsetminus \mathbf{Q}_{\mathbf{L}}$ from those where $\operatorname{Re} z \in \mathbf{Q}_{\mathbf{L}}$ is merely very small; the approximating function is bound to output (approximately) 0 for both. Thus, the exponential function determined by $\lim_{n\to\infty} E_+(z,r,n)$ will be defined even for $\operatorname{Re} z \in \mathbf{Q}_{\downarrow\mathbf{L}} \smallsetminus \mathbf{Q}_{\mathbf{L}}$, assigning such z the value 0. We chose to make our official exponential function agree with this.

In any case, a skeptical reader is free to restrict the exp function to $\mathbf{R}_{\mathbf{L}} + i\mathbf{R}$.

3.1 Exponential

Our first task is relatively straightforward: define a function $\exp\colon \mathbf{C}_{\mathbf{L}} \to \mathbf{C}_{\neq 0}$ using the power series

$$\sum_n \frac{z^n}{n!},$$

and (among other basic properties) prove the homomorphism property

$$\exp(z+w) = \exp z \exp w$$

by means of the standard argument exploiting the binomial theorem.

We start by defining partial sums of this power series, which we will then use to define exp on $\mathbf{Q}_{\mathbf{L}}(i)$.

Definition 3.3 We define a function $e\colon \mathbf{Q}(i) \times \mathbf{L} \to \mathbf{Q}(i)$ by

$$e(z,n) = \sum_{j<n} \frac{z^j}{j!}.$$

Lemma 3.4 *$n! \geq 2\bigl(\frac{1}{4}(n+1)\bigr)^n$ for all $n \in \mathbf{L}$, $n \geq 1$.*

Proof: By induction on n. The statement holds for $n = 1$. If $n \geq 2$, the induction hypothesis for $m = \lfloor n/2 \rfloor$ gives

$$n! \geq m!\,(m+1)^{n-m} \geq 2\frac{(m+1)^n}{4^m} = 2\frac{(2m+2)^n}{4^m 2^n} \geq 2\frac{(n+1)^n}{4^n}.$$

□

Lemma 3.5 *If $z \in \mathbf{Q}_{\mathbf{L}}(i)$, then $\{e(z,n) : n \in \mathbf{L}\}$ is a Cauchy net. Thus, we can define a function $\exp_{\mathbf{Q}_{\mathbf{L}}(i)}\colon \mathbf{Q}_{\mathbf{L}}(i) \to \mathbf{C}$ by*

$$\exp_{\mathbf{Q}_{\mathbf{L}}(i)} z = \lim_{\substack{n\in\mathbf{L}\\ n\to\infty}} e(z,n).$$

Proof: Assume $|z| \leq r \in \mathbf{L}$. If $2r \leq n \leq m \in \mathbf{L}$, we have

$$\bigl|e(z,m) - e(z,n)\bigr| = \left|\sum_{j=n}^{m-1} \frac{z^j}{j!}\right| \leq \sum_{j=n}^{m-1} \frac{r^j}{j!} \leq \frac{r^n}{n!} \sum_{j<m-n} \left(\frac{r}{n}\right)^j \leq \frac{r^n}{n!} \sum_{j<m-n} 2^{-j} \leq 2\frac{r^n}{n!},$$

using Lemma 2.1 and $(n+j)! \geq n!\,n^j$. Thus, if $n, m \geq \max\{8r, t\}$, then

$$\bigl|e(z,m) - e(z,n)\bigr| \leq \left(\frac{4r}{n}\right)^n \leq 2^{-n} \leq 2^{-t}$$

by Lemma 3.4. □

We are going to extend the domain of $\exp_{\mathbf{Q}_{\mathbf{L}}(i)}$ first to $\mathbf{C}_{\mathbf{L}}$, and later to $\mathbf{R}_{\downarrow\mathbf{L}} + i\mathbf{R}$. Formally, we distinguish these functions by subscripts, but since they give the same values whenever they are defined, we may write just exp unless the distinction becomes important.

Lemma 3.6 *Let $z \in \mathbf{Q}(i)$ and $r \in \mathbf{Q}_{\mathbf{L}}$. If $|z| \leq r$, then $|\exp z| \leq \exp r$.*

Proof: For any $n \in \mathbf{L}$, we have

$$|e(z,n)| = \left|\sum_{j<n} \frac{z^j}{j!}\right| \leq \sum_{j<n} \frac{r^j}{j!} \leq \exp r$$

by Lemma 2.1. The result follows by taking the limit $n \to \infty$. □

Lemma 3.7 *If $z \in \overline{D}_{3/2}(0) \cap \mathbf{Q}(i)$, then*

$$\left|\exp z - (1+z)\right| \leq |z|^2.$$

Proof: For any $n \in \mathbf{L}$, $n \geq 2$,

$$\left|\frac{e(z,n)-(1+z)}{z^2}\right| = \left|\sum_{j=2}^{n-1} \frac{z^{j-2}}{j!}\right| \leq \sum_{j=2}^{n-1} \frac{3^{j-2}}{2^{j-2} j!} \leq \sum_{j=2}^{n-1} 2^{1-j} \leq 1$$

using Lemma 2.1 and $j! \geq 2 \cdot 3^{j-2}$ for $j \geq 2$, thus

$$\left|e(z,n) - (1+z)\right| \leq |z|^2.$$

Taking the limit, a similar inequality holds for $\exp z$. $\square$

Lemma 3.8 *For any $z, w \in \mathbf{Q_L}(i)$,*

$$\exp(z+w) = \exp z \exp w.$$

Proof: For any $n \in \mathbf{L}$, we have

$$e(z,n)e(w,n) = \sum_{j,k<n} \frac{z^j w^k}{j!\,k!},$$

while

$$e(z+w,2n) = \sum_{l<2n} \frac{(z+w)^l}{l!} = \sum_{l<2n} \sum_{j+k=l} \binom{l}{j} \frac{z^j w^k}{l!} = \sum_{j+k<2n} \frac{z^j w^k}{j!\,k!},$$

hence

$$e(z+w,2n) - e(z,n)e(w,n) = \sum_{j=n}^{2n-1} \frac{z^j}{j!} \sum_{k<2n-j} \frac{w^k}{k!} + \sum_{k=n}^{2n-1} \frac{w^k}{k!} \sum_{j<2n-k} \frac{z^j}{j!}.$$

Fix $r \in \mathbf{L}$ such that $|z|, |w| \leq r$. Then Lemma 2.1 gives

$$\left|e(z+w,2n) - e(z,n)e(w,n)\right| \leq 2 \sum_{j=n}^{2n-1} \frac{r^j}{j!} \sum_{k<2n-j} \frac{r^k}{k!} \leq 2\exp(r) \sum_{j=n}^{2n-1} \frac{r^j}{j!}.$$

Thus, for all $n \geq 8r$, we have

$$\left|e(z+w,2n) - e(z,n)e(w,n)\right| \leq 2^{1-n} \exp r$$

by the proof of Lemma 3.5. The result follows by taking the limit $n \to \infty$. $\square$

Lemma 3.9 *The restrictions $\exp_{\mathbf{Q_L}(i)} \restriction \overline{D}_r(0) \cap \mathbf{Q}(i)$ are uniformly continuous for all $r \in \mathbf{L}$. Thus, $\exp_{\mathbf{Q_L}(i)}$ has a unique extension to a continuous function $\exp_{\mathbf{C_L}} : \mathbf{C_L} \to \mathbf{C}$.*

Proof: Let $\delta \in \mathbf{Q}$, $0 < \delta \le 1$. Then any $z, w \in \overline{D}_r(0) \cap \mathbf{Q}(i)$ such that $|w - z| \le \delta$ satisfy

$$|\exp w - \exp z| = \bigl|\bigl(\exp(w - z) - 1\bigr) \exp z\bigr| \le (\delta + \delta^2) \exp r \le 2\delta \exp r$$

by Lemmas 3.6, 3.7, and 3.8, thus $\exp_{\mathbf{Q_L}(i)} \restriction \overline{D}_r(0) \cap \mathbf{Q}(i)$ is indeed uniformly continuous. It follows that it has a unique continuous extension $\exp_r \colon \overline{D}_r(0) \to \mathbf{C}$. Uniqueness ensures that $\exp_r = \exp_s \restriction \overline{D}_r(0)$ whenever $r \le s$, hence $\exp_{\mathbf{C_L}} = \bigcup_r \exp_r$ is a well-defined function $\mathbf{C_L} \to \mathbf{C}$, and it is continuous as its restrictions to all $\overline{D}_r(0)$ are continuous. Conversely, any continuous extension of $\exp_{\mathbf{Q_L}(i)}$ to $\mathbf{C_L}$ must coincide with $\exp_r$ on $\overline{D}_r(0)$ for each r, hence it equals $\exp_{\mathbf{C_L}}$. □

The main take-away from Section 3.1 is the next summary lemma.

Lemma 3.10

(i) *The function* $\exp_{\mathbf{C_L}}$ *is a group homomorphism* $\langle \mathbf{C_L}, +, 0, - \rangle \to \langle \mathbf{C}_{\neq 0}, \cdot, 1, {}^{-1} \rangle$ *commuting with* $\overline{z}$.

(ii) *The restriction* $\exp_{\mathbf{R_L}} = \exp_{\mathbf{C_L}} \restriction \mathbf{R_L}$ *is an embedding of ordered groups* $\langle \mathbf{R_L}, +, 0, -, < \rangle \to \langle \mathbf{R}_{>0}, \cdot, 1, {}^{-1}, < \rangle$.

(iii) *For all* $z \in \mathbf{C_L}$, $|\exp_{\mathbf{C_L}} z| = \exp_{\mathbf{R_L}} \operatorname{Re} z$.

(iv) *If* $z \in \overline{D}_{3/2}(0)$, *then* $\bigl|\exp z - (1 + z)\bigr| \le |z|^2$.

Proof:

(i): For any $w \in \mathbf{Q_L}(i)$, the set

$$H_w = \bigl\{z \in \mathbf{C_L} : \exp(z + w) = \exp z \exp w\bigr\}$$

is closed due to the continuity of exp, and includes $\mathbf{Q_L}(i)$ by Lemma 3.8. Since $\mathbf{Q_L}(i)$ is dense in $\mathbf{C_L}$, we see that $H_w = \mathbf{C_L}$, i.e.,

$$\exp(z + w) = \exp z \exp w \tag{1}$$

for all $z \in \mathbf{C_L}$ and $w \in \mathbf{Q_L}(i)$. Using the same density argument once more, $\mathbf{Q_L}(i) \subseteq H_w$ for each $w \in \mathbf{C_L}$ by (1) (with arguments swapped), hence $H_w = \mathbf{C_L}$, i.e., (1) holds for all $z, w \in \mathbf{C_L}$. This shows that exp is a group homomorphism as indicated in (i), provided that the codomain is right, i.e., $\exp z \neq 0$ for all $z \in \mathbf{C_L}$. This, too, follows from (1), as $\exp z \exp(-z) = \exp 0 = 1$.

We have $e(\overline{z}, n) = \overline{e(z, n)}$ for all $z \in \mathbf{Q_L}(i)$ and $n \in \mathbf{L}$, hence $\exp \overline{z} = \overline{\exp z}$ by taking limits. Using density of $\mathbf{Q_L}(i) \subseteq \mathbf{C_L}$ again, the same holds for all $z \in \mathbf{C_L}$.

(ii): Let $x \in \mathbf{R_L}$. Since $\overline{\exp x} = \exp x$ by (i), we have $\exp x \in \mathbf{R}$. If $x \in \mathbf{Q_L}(i)$, $x > 0$, then $e(x, n)$ is non-decreasing in n, hence $\exp x \ge e(x, 2) = 1 + x$. By density, $\exp x \ge 1 + x$ for all $x \in \mathbf{R_L}$, $x > 0$, hence $\exp x > 1$. Since $\exp x \exp(-x) = 1$ by (i), this ensures $\exp x > 0$ for all $x \in \mathbf{R_L}$, and it implies that exp is strictly increasing on $\mathbf{R_L}$: if $x < y$, we have

$$\exp(y) = \exp(y - x) \exp x > \exp x$$

as $\exp(y - x) > 1$ and $\exp x > 0$. In particular, $\exp_{\mathbf{R_L}}$ is injective, and it is an ordered group homomorphism.

(iii): $|\exp z|^2 = \exp z\, \overline{\exp z} = \exp(z + \overline{z}) = \exp(2 \operatorname{Re} z) = (\exp \operatorname{Re} z)^2$ using (i).

(iv): By Lemma 3.7 and the density of $\overline{D}_{3/2}(0) \cap \mathbf{Q}(i)$ in $\overline{D}_{3/2}(0)$. □

The main remaining problem now is to prove that $\exp_{\mathbf{C_L}}$ is *surjective* (onto $\mathbf{C}_{\neq 0}$); consequently, $\exp_{\mathbf{R_L}}$ is an ordered group isomorphism, and there is a constant π such that $\exp_{\mathbf{C_L}}$ is $2\pi i$-periodic, which will enable its extension to $\mathbf{R_L} + i\mathbf{R}$. Let us first mention a few failed approaches so that we understand that the problem is nontrivial.

Considering the real case for simplicity, the most obvious idea how to find for a given $x \in \mathbf{R}_{>0}$ a preimage $y \in \mathbf{R_L}$ such that $\exp y = x$ is to show, for any integer $n > 0$, that there is an integer m such that $\exp(m/n) \leq x \leq \exp\bigl((m+1)/n\bigr)$, using the monotonicity of exp. On closer inspection, this argument amounts to induction on m for the formula $\exp(m/n) \leq x$; thus, to make it work in VTC^0, we actually need to use rational approximations of exp rather than the function itself, and even so, it only works for $n \in \mathbf{L}$, which implies $m \in \mathbf{Z_L}$. (Note that binary number induction for TC^0 predicates implies VPV over VTC^0. Here, VPV is a theory of bounded arithmetic corresponding to polynomial-time functions, and as such it is generally assumed to be stronger than VTC^0; cf. [4].) Thus, we can only determine logarithmically many most significant bits of y, which is insufficient to construct it as an element of $\mathbf{R}$.

We could use binary search to determine y with precision 2^{-n} rather than n^{-1}, but this is an inherently sequential algorithm taking us outside TC^0; likewise for more sophisticated iterative methods such as Newton iteration, which parallelize better, but still need a non-constant number of sequential iterations. In [8], we formalized a form of the Lagrange inversion theorem, which can in principle be used to invert any function f given by power series, such as exp; however, the core argument in [8, Thm. 5.1] (or even the definition of the inverse series) only works when f is a constant-degree polynomial, as it relies on bounded sums with $n^{O(d)}$ terms, where $d = \deg f$.

We will solve the problem by constructing in an ad hoc way a function $\log\colon \mathbf{C}_{\neq 0} \to \mathbf{C_L}$, and proving its various properties, eventually showing $\exp \log z = z$. This will take us the next few subsections.

But before we leave, let us present some bounds on $\exp_{\mathbf{R_L}}$ that express its convexity.

Lemma 3.11

(i) *For all* $x \in \mathbf{R_L}$*,* $\exp x \geq 1 + x$.

(ii) *For all* $x, y \in \mathbf{R_L}$*,* $(y - x)\exp x \leq \exp y - \exp x \leq (y - x)\exp y$.

(iii) *For all* $x, y \in \mathbf{R_L}$ *and* $t \in [0, 1]$*,* $\exp\bigl((1 - t)x + ty\bigr) \leq (1 - t)\exp x + t\exp y$.

Proof:

(i): By density, it suffices to prove the result for $x \in \mathbf{Q_L}$. We have shown $\exp x \geq 1 + x$ for $x \geq 0$ in the proof of Lemma 3.10 (ii). Moreover, if $0 \leq x < 1$, then

$$e(x, n) = \sum_{j<n} \frac{x^j}{j!} \leq \sum_{j<n} x^j \leq \frac{1}{1 - x},$$

hence $\exp x \leq (1-x)^{-1}$, and $\exp(-x) \geq 1-x$. Thus, $\exp x \geq 1+x$ also holds when $-1 < x \leq 0$; if $x \geq -1$, then $\exp x \geq 0 \geq 1 + x$.

(ii): We have $\exp y - \exp x = \bigl(\exp(y-x)-1\bigr)\exp x \geq (y-x)\exp x$ by (i); the other inequality follows by swapping x and y.

(iii): Put $w = (1-t)x + ty$. We have $\exp w - \exp x \le (w-x)\exp w = t(y-x)\exp w$ by (ii), hence $\exp x \ge \bigl(1 - t(y-x)\bigr)\exp w$. Likewise, $\exp y - \exp w \ge (y-w)\exp w$ implies $\exp y \ge \bigl(1 + (1-t)(y-x)\bigr)\exp w$. Thus,

$$(1-t)\exp x + t\exp y \ge \bigl[(1-t)\bigl(1-t(y-x)\bigr) + t\bigl(1+(1-t)(y-x)\bigr)\bigr]\exp w = \exp w. \qquad \square$$

3.2 Logarithm near 1

We intend to construct a logarithm function which is a right inverse of exp, implying that exp is surjective. Defining log will be more complicated than exp, largely due to the fact that exp is entire, whereas log has a branching singularity at the origin. Thus, a power series will only give us log in a circular neighbourhood of 1: this will be the topic of the present subsection. We will then extend it to $\mathbf{C}_{\neq 0}$ (with a branch cut along the negative real axis) in several stages:

- Using the function $2^n\colon \mathbf{L} \to \mathbf{N}$, we extend log to $\mathbf{R}_{>0}$ (Section 3.3).
- Combining $\mathbf{R}_{>0}$ with the neighbourhood of 1, we extend log to a sector $\{x+iy : |y| < cx\}$ for a suitable c (Section 3.4).
- Using $\sqrt{z}$ (treated in Section 3.5), we can increase the angle of the sector. We iterate this a few times to cover $\mathbf{C}_{\neq 0}$ (Section 3.6).

We will rely on restricted forms of the identity $\log zw = \log z + \log w$ (which does not quite hold, due to the branch cut) to make sure that the successive extensions fit together well, and to eventually derive $\exp\log z = z$.

We start with the power series for log, or rather, for the function $-\log(1-z)$.

Definition 3.12 We define a function $\lambda\colon \mathbf{Q}(i) \times \mathbf{L} \to \mathbf{Q}(i)$ by

$$\lambda(z,n) = \sum_{j=1}^{n} \frac{z^j}{j}.$$

We write $x <^* y$ if $x \le y - h^{-1}$ for some $h \in \mathbf{L}_{>0}$, and we put $D^*_r(z_0) = \{z \in \mathbf{C} : |z - z_0| <^* r\}$, $(a,b)^* = \{x \in \mathbf{R} : a <^* x <^* b\}$, $[a,b)^* = \{x \in \mathbf{R} : a \le x <^* b\}$, etc.

Lemma 3.13 *If $h \in \mathbf{L}_{>0}$, then $(1-h^{-1})^h \le \frac{1}{2}$.*

Proof: $h^h = \sum_{j\le h} \binom{h}{j}(h-1)^j \ge (h-1)^h + h(h-1)^{h-1} \ge 2(h-1)^h$. $\square$

Lemma 3.14 *If $z \in D^*_1(0) \cap \mathbf{Q}(i)$, then $\{\lambda(z,n) : n \in \mathbf{L}\}$ is a Cauchy net. Thus, we can define a function $\Lambda\colon D^*_1(0) \cap \mathbf{Q}(i) \to \mathbf{C}$ by*

$$\Lambda(z) = \lim_{\substack{n\in\mathbf{L}\\ n\to\infty}} \lambda(z,n).$$

Proof: Assume $|z| \le 1 - h^{-1}$, where $h \in \mathbf{L}$, and let $n \le m \in \mathbf{L}$. Then

$$\bigl|\lambda(z,m) - \lambda(z,n)\bigr| = \Bigl|\sum_{j=n+1}^{m} \frac{z^j}{j}\Bigr| \le \sum_{j=n+1}^{m} \frac{(1-h^{-1})^j}{j} \le \frac{(1-h^{-1})^{n+1}}{n+1} \sum_{j<m-n} (1-h^{-1})^j$$
$$\le \frac{h}{n+1}(1-h^{-1})^{n+1} \le 2^{-t}$$

if $n+1 \ge ht$, using Lemmas 2.1 and 3.13. $\square$

Lemma 3.15 *If $z \in \overline{D}_{1/2}(0) \cap \mathbf{Q}(i)$, then*

$$|\Lambda(z) - z| \le |z|^2.$$

Proof: For any $n \in \mathbf{L}$, $n \ge 2$,

$$\left|\frac{\lambda(z,n) - z}{z^2}\right| = \left|\sum_{j=2}^{n-1} \frac{z^{j-2}}{j}\right| \le \sum_{j=2}^{n-1} \frac{1}{2^{j-2}j} \le \sum_{j=2}^{n-1} 2^{1-j} \le 1$$

using Lemma 2.1, which gives the result by taking the limit $n \to \infty$. $\square$

We are now heading to prove the identity $\Lambda(z) + \Lambda(w) = \Lambda(z + w - zw)$, which will yield $\log(z) + \log(w) = \log(zw)$; this is the most technical part of the construction of log. We will need the next lemma as an ingredient in the proof; it effectively means that $\nabla^n f = 0$ for any polynomial f of degree $< n$ (expressed as a linear combination of the falling factorials $x^{\underline{h}}$, $h < n$, rather than the usual monomials x^h), where $(\nabla f)(x) = f(x) - f(x-1)$ is the backwards difference operator.

Lemma 3.16 *For all $h < n \in \mathbf{L}$ and $x \in \mathbf{Q}$,*

$$\sum_{k \le n} \binom{n}{k} (-1)^k (x-k)^{\underline{h}} = 0,$$

where $x^{\underline{h}} = \prod_{j<h}(x-j)$.

Proof: Fix $x \in \mathbf{Q}$ and $m \in \mathbf{L}_{>0}$; we will prove

$$\sum_{k \le m+h} \binom{m+h}{k} (-1)^k (x+h-k)^{\underline{h}} = 0 \tag{2}$$

by induction on $h \in \mathbf{L}$. For $h = 0$, we have

$$\sum_{k \le m} \binom{m}{k} (-1)^k (x-k)^{\underline{0}} = \sum_{k \le m} \binom{m}{k} (-1)^k = (1-1)^m = 0.$$

Assuming (2) holds for h, and writing $m' = m + h$, $x' = x + h$, we obtain

$$\begin{aligned}
&\sum_{k \le m'+1} \binom{m'+1}{k} (-1)^k (x'+1-k)^{\underline{h+1}} \\
&\quad = \sum_{k \le m'} \binom{m'}{k} (-1)^k (x'+1-k)^{\underline{h+1}} + \sum_{k \le m'} \binom{m'}{k} (-1)^{k+1} (x'-k)^{\underline{h+1}} \\
&\quad = \sum_{k \le m'} \binom{m'}{k} (-1)^k (x'+1-k)(x'-k)^{\underline{h}} - \sum_{k \le m'} \binom{m'}{k} (-1)^k (x'-k)^{\underline{h}} (x'-k-h) \\
&\quad = (h+1) \sum_{k \le m'} \binom{m'}{k} (-1)^k (x'-k)^{\underline{h}} = 0
\end{aligned}$$

using $\binom{m'+1}{k} = \binom{m'}{k} + \binom{m'}{k-1}$ and the induction hypothesis. □

Lemma 3.17 *Let $r, s \in \mathbf{Q}_{>0}$ be such that $(1+r)(1+s) <^* 2$. Then*

$$\Lambda(z) + \Lambda(w) = \Lambda(z + w - zw)$$

for all $z \in \overline{D}_r(0) \cap \mathbf{Q}(i)$ and $w \in \overline{D}_s(0) \cap \mathbf{Q}(i)$.

Proof: Since $|z + w - zw| \le r + s + rs <^* 1$ by Lemma 2.1, $\Lambda(z + w - zw)$ is defined. For any $n \in \mathbf{L}_{>0}$, we have

$$\begin{aligned}
&\lambda(z, n) + \lambda(w, n) - \lambda(z + w - zw, n) \\
&\qquad = \sum_{j=1}^{n} \frac{z^j}{j} + \sum_{k=1}^{n} \frac{w^k}{k} - \sum_{\substack{j,k,l \\ 0 < j+k+l \le n}} \binom{j+k+l}{j, k, l} \frac{(-1)^l z^{j+l} w^{k+l}}{j+k+l} \\
&\qquad = - \sum_{\substack{j,k,l \\ 0 < j+l, k+l \\ j+k+l \le n}} \binom{j+k+l}{j, k, l} \frac{(-1)^l z^{j+l} w^{k+l}}{j+k+l}.
\end{aligned}$$

We claim that

$$\sum_{\substack{j,k,l \\ 0 < j+l, k+l \le n}} \binom{j+k+l}{j, k, l} \frac{(-1)^l z^{j+l} w^{k+l}}{j+k+l} = \sum_{a,b=1}^{n} z^a w^b \sum_{l \le a,b} \binom{a+b-l}{a-l, b-l, l} \frac{(-1)^l}{a+b-l} = 0 :$$

indeed, if w.l.o.g. $a \le b$, Lemma 3.16 gives

$$\begin{aligned}
\sum_{l \le a,b} \binom{a+b-l}{a-l, b-l, l} \frac{(-1)^l}{a+b-l} &= \sum_{l \le a} \frac{(a+b-1-l)!}{(a-l)!\,(b-l)!\,l!} (-1)^l \\
&= \frac{1}{a!} \sum_{l \le a} \binom{a}{l} (-1)^l (a+b-1-l)^{\underline{a-1}} = 0.
\end{aligned}$$

Thus,

$$\lambda(z,n)+\lambda(w,n)-\lambda(z+w-zw,n)=\sum_{\substack{j,k,l\\ j+l,k+l\le n<j+k+l}}\binom{j+k+l}{j,k,l}\frac{(-1)^l z^{j+l}w^{k+l}}{j+k+l}.$$

By Lemma 2.1,

$$\begin{aligned}\left|\lambda(z,n)+\lambda(w,n)-\lambda(z+w-zw,n)\right| &\le \sum_{\substack{j,k,l\\ j+l,k+l\le n<j+k+l}}\binom{j+k+l}{j,k,l}\frac{r^{j+l}s^{k+l}}{j+k+l}\\ &\le \frac{1}{n+1}\sum_{\substack{j,k,l\\ n<j+k+l\le 2n}}\binom{j+k+l}{j,k,l}r^{j+l}s^{k+l}\\ &=\frac{1}{n+1}\sum_{a=n+1}^{2n}(r+s+rs)^a\\ &\le \frac{(r+s+rs)^{n+1}}{(n+1)(1-r-s-rs)}.\end{aligned}$$

By assumption, we can fix $h\in\mathbf{L}$ such that $r+s+rs\le 1-h^{-1}$. Then for all $n,t\in\mathbf{L}$,

$$n+1\ge ht \implies \left|\lambda(z,n)+\lambda(w,n)-\lambda(z+w-zw,n)\right|\le\frac{h}{n+1}(1-h^{-1})^{n+1}\le 2^{-t}$$

using Lemma 3.13. The result follows by taking the limit $n\to\infty$. □

Lemma 3.18 *Let $h\in\mathbf{L}_{>0}$ and $r\in\mathbf{Q}_{>0}$. Then for all $z,w\in\overline{D}_{1-h^{-1}}(0)\cap\mathbf{Q}(i)$,*

$$|z-w|\le r \implies |\Lambda(z)-\Lambda(w)|\le hr.$$

Proof: For any $n\in\mathbf{L}$, we have

$$\begin{aligned}|\lambda(z,n)-\lambda(w,n)| &= \left|\sum_{j=1}^{n}\frac{z^j-w^j}{j}\right| = \left|(z-w)\sum_{j=1}^{n}\frac{1}{j}\sum_{k<j}z^k w^{j-1-k}\right|\\ &\le r\sum_{j=1}^{n}(1-h^{-1})^{j-1}\le hr.\end{aligned}$$

The result follows by taking the limit $n\to\infty$. □

The next lemma (and definition) is the main result of Section 3.2.

Lemma 3.19 *There is a unique continuous function*

$$\log_D\colon D_1^*(1)\to\mathbf{C}$$

such that $\log_D z=-\Lambda(1-z)$ for all $z\in D_1^*(1)\cap\mathbf{Q}(i)$. It satisfies

$$\left|\log_D(1+z)-z\right|\le|z|^2 \tag{3}$$

for $z \in \overline{D}_{1/2}(0)$. *If* $r, s \in \mathbf{Q}_{>0}$ *are such that* $(1+r)(1+s) <^* 2$, *then*

$$\log_D zw = \log_D z + \log_D w \tag{4}$$

for all $z \in \overline{D}_r(1)$ *and* $w \in \overline{D}_s(1)$. *In particular,* (4) *holds for all* $z, w \in \overline{D}_{2/5}(1)$.

Proof: As in the proof of Lemma 3.9, the existence and uniqueness of $\log_D$ follows from the uniform continuity of $\Lambda \restriction \overline{D}_{1-h^{-1}}(0) \cap \mathbf{Q}(i)$ for every $h \in \mathbf{L}_{>0}$, which was proved in Lemma 3.18. Properties (3) and (4) for $z, w \in \mathbf{Q}(i)$ follow from Lemmas 3.15 and 3.17; this implies the general case using the density of $\mathbf{Q}(i)$ in $\mathbf{C}$, similarly to the proof of Lemma 3.10. $\square$

As in the case of exp, we will define several versions of log on various domains, distinguished by subscripts. (The D in $\log_D$ refers to the disk $D_1^*(1)$.) Again, we will sometimes drop the subscript if it can be inferred from the context, but we have to be more careful than before, because the variants of log do not a priori agree on their common domains (though we will eventually prove they do, in Lemma 3.58).

3.3 Real logarithm

We now start extending $\log_D$ to further domains, first to $\mathbf{R}_{>0}$. The idea is simple: using the function $2^n \colon \mathbf{L} \to \mathbf{N}$ (or rather, $\mathbf{Z_L} \to \mathbf{Q}$), we can write any $x \in \mathbf{R}_{>0}$ as $x = 2^n x'$ with $n \in \mathbf{Z_L}$ and $x' \in \left[\frac{1}{2}, 1\right]$, and put $\log_{\mathbf{R}} x = \log_D x' + n \log 2$ for a suitably defined $\log 2$. We will actually ensure this defining identity to hold for x' from a larger interval; the resulting interval overlap will assist us in proving that $\log_{\mathbf{R}}$ is well behaved, such as that it satisfies the identity $\log_{\mathbf{R}} xy = \log_{\mathbf{R}} x + \log_{\mathbf{R}} y$. We begin with a definition of $\ell_2 = \log 2$.

Lemma 3.20 *The constant* $\ell_2 = -\log_D \frac{1}{2} = \Lambda\left(\frac{1}{2}\right)$ *satisfies*

$$\log_D 2x = \log_D x + \ell_2$$

for all $x \in \left(\frac{1}{3}, \frac{3}{4}\right)^*$.

Proof: First, if $x \in \left(\frac{1}{3}, \frac{2}{3}\right)^*$, we have

$$\log_D 2x + \log_D \tfrac{1}{2} = \log_D x$$

by eq. (4) in Lemma 3.19 with $r = |1-2x| <^* \frac{1}{3}$ and $s = \frac{1}{2}$. Next, if $x \in \left[\frac{1}{2}, \frac{3}{4}\right)^*$, let $y = \frac{2}{3} - h^{-1}$ for sufficiently large $h \in \mathbf{L}$. Then

$$\log_D 2x + \log_D y = \log_D 2xy = \log_D x + \log_D 2y = \log_D x + \log_D y + \ell_2 \colon$$

the first equality follows from (4) with $r = 2x - 1 <^* \frac{1}{2}$ and $s = 1 - y = \frac{1}{3} + h^{-1}$; we can choose h such that $(1+r)(1+s) <^* 2$. The second equality follows from (4) with $r = 1 - x \leq \frac{1}{2}$ and $s = 2y - 1 <^* \frac{1}{3}$. $\square$

Lemma 3.21 *There is a unique continuous function* $\log_{\mathbf{R}} \colon \mathbf{R}_{>0} \to \mathbf{R}_{\mathbf{L}}$ *such that*

$$\log_{\mathbf{R}} 2^n x = \log_D x + n\ell_2$$

for all $n \in \mathbf{Z}_{\mathbf{L}}$ *and* $x \in \left(\frac{1}{3}, \frac{3}{2}\right)^*$.

Proof: Every $x \in \mathbf{R}_{>0}$ can be written as $2^n x'$ for some $n \in \mathbf{Z}_{\mathbf{L}}$ and $x' \in \left[\frac{1}{2}, 1\right]$. Since $\lambda(z, n) \in \mathbf{Q}$ for $z \in \mathbf{Q}$, Λ maps $D_1^*(0) \cap \mathbf{Q}$ to $\mathbf{R}$, hence $\log_D$ maps $D_1^*(1) \cap \mathbf{R}$ to $\mathbf{R}$. Moreover, Lemma 3.19 (eq. (3)) implies that $\log_D$ maps $\left[\frac{1}{2}, \frac{3}{2}\right]$ to $\left[-\frac{3}{4}, \frac{3}{4}\right]$. Thus, $\log_D x' + n\ell_2 \in \mathbf{R}_{\mathbf{L}}$.

Assume $2^n x = 2^m y$ for some $n, m \in \mathbf{Z}_{\mathbf{L}}$ and $x, y \in \left(\frac{1}{3}, \frac{3}{2}\right)^*$, $x < y$. Then $2^{n-m} = y/x \in \left(1, \frac{9}{2}\right)$, hence $n = m + 1$, $y = 2x$, and $x \in \left(\frac{1}{3}, \frac{3}{4}\right)^*$, or $n = m + 2$, $y = 4x$, and $x \in \left(\frac{1}{3}, \frac{3}{8}\right)^*$. Thus,

$$\log_D x + n\ell_2 = \log_D y + m\ell_2$$

using Lemma 3.20.

The continuity of $\log_D$ ensures that $\log_{\mathbf{R}}$ is continuous on $\left(\frac{1}{3}2^n, \frac{3}{2}2^n\right)^*$ for each $n \in \mathbf{Z}_{\mathbf{L}}$. These open sets cover $\mathbf{R}_{>0}$, hence $\log_{\mathbf{R}}$ is continuous. $\square$

While we eventually want to show that $\log_{\mathbf{R}}$ is an inverse of $\exp_{\mathbf{R}_{\mathbf{L}}}$, we will be content for now with proving that it is an ordered group embedding $\langle \mathbf{R}_{>0}, \cdot, < \rangle \to \langle \mathbf{R}_{\mathbf{L}}, +, < \rangle$.

Lemma 3.22 *The function* $\log_{\mathbf{R}}$ *is strictly increasing (hence injective).*

Proof: We first show that $\log_D$ is strictly increasing on $\left[\frac{1}{2}, 1\right]$. Let $\frac{1}{2} \le x < y \le 1$, and consider $u = x/y \in \left[\frac{1}{2}, 1\right)$. We have $\log_D u \le (u-1) + (u-1)^2 = u(u-1) < 0$ by Lemma 3.19 (eq. (3)), thus

$$\log_D x = \log_D u + \log_D y < \log_D y$$

by (4), as long as $u >^* \frac{2}{3}$: then $r = |1 - y| \le \frac{1}{2}$ and $s = 1 - u <^* \frac{1}{3}$, thus $(1 + r)(1 + s) <^* 2$. It follows that $\log_D$ is strictly increasing on $\left[\frac{1}{2}, \frac{3}{4}\right)^*$ and on $\left(\frac{2}{3}, 1\right]^*$, hence on $\left[\frac{1}{2}, 1\right]$.

Now, let $x, y \in \mathbf{R}_{>0}$, and assume $x < y$. Write $x = 2^n x'$ and $y = 2^m y'$ with $n, m \in \mathbf{Z}_{\mathbf{L}}$ and $x', y' \in \left(\frac{1}{2}, 1\right]$. The previous part ensures that $\log_{\mathbf{R}}$ is strictly increasing on $[2^{n-1}, 2^n]$, hence $\log_{\mathbf{R}} x < \log_{\mathbf{R}} y$ if $m = n$. If $m > n$, we have

$$\log_{\mathbf{R}} y > (m-1)\ell_2 \ge n\ell_2 \ge \log_{\mathbf{R}} x$$

as $\log_D$ maps $\left(\frac{1}{2}, 1\right]$ to $(-\ell_2, 0]$. $\square$

Lemma 3.23 *For all* $x, y \in \mathbf{R}_{>0}$,

$$\log_{\mathbf{R}} xy = \log_{\mathbf{R}} x + \log_{\mathbf{R}} y.$$

Proof: Write $x = 2^n x'$ and $y = 2^m y'$, where $n, m \in \mathbf{Z}_{\mathbf{L}}$ and $x', y' \in \left[\frac{3}{5}, \frac{6}{5}\right] \subseteq \left(\frac{1}{3}, \frac{3}{2}\right)^*$. Then $xy = 2^{n+m} x'y'$, where $x'y' \in \left[\frac{9}{25}, \frac{36}{25}\right] \subseteq \left(\frac{1}{3}, \frac{3}{2}\right)^*$. It follows that

$$\log_{\mathbf{R}} xy = (n+m)\ell_2 + \log_D x'y' = n\ell_2 + \log_D x' + m\ell_2 + \log_D y' = \log_{\mathbf{R}} x + \log_{\mathbf{R}} y$$

using (4), as $|1 - x'|, |1 - y'| \le \frac{2}{5}$. $\square$

3.4 Logarithm in a sector

The next extension of log is to an angular sector by means of $\log z = \log_{\mathbf{R}}|z| + \log_D\bigl(z/|z|\bigr)$, as long as $z/|z|$ is close enough to 1.

Definition 3.24 We define the *complex sign* function $\operatorname{sgn}\colon \mathbf{C}_{\neq 0} \to \bigl\{z : |z| = 1\bigr\}$ by $\operatorname{sgn} z = z/|z|$. We consider the sector

$$S = \bigl\{z \in \mathbf{C}_{\neq 0} : |\operatorname{sgn} z - 1| <^* 1\bigr\}.$$

We define a continuous function $\log_S\colon S \to \mathbf{C_L}$ by

$$\log_S z = \log_{\mathbf{R}}|z| + \log_D \operatorname{sgn} z.$$

Let us clarify the geometry of S:

Lemma 3.25 *Let $z = x + iy \in \mathbf{C}_{\neq 0}$. Then*

$$z \in S \iff \frac{x}{|z|} >^* \frac{1}{2} \iff x > 0 \wedge \frac{|y|}{|z|} <^* \frac{\sqrt{3}}{2} \iff x > 0 \wedge \frac{|y|}{x} <^* \sqrt{3}.$$

Proof: We have $z \in S$ iff $|\operatorname{sgn} z - 1|^2 <^* 1$, where

$$|\operatorname{sgn} z - 1|^2 = \frac{\bigl(z - |z|\bigr)\bigl(\overline{z} - |z|\bigr)}{|z|^2} = \frac{2|z|^2 - (z + \overline{z})|z|}{|z|^2} = 2\left(1 - \frac{x}{|z|}\right),$$

which proves the first equivalence. The rest follows easily, using $x^2 + y^2 = |z|^2$. ☐

Basic properties of $\log_S$ are easy to establish by combining the properties of $\log_D$ and $\log_{\mathbf{R}}$:

Lemma 3.26

(i) *If $z, w \in S$ and $\bigl(1 + |\operatorname{sgn} z - 1|\bigr)\bigl(1 + |\operatorname{sgn} w - 1|\bigr) <^* 2$, then*

$$\log_S zw = \log_S z + \log_S w.$$

In particular, this holds if $z = x + iy$ and $w = u + iv$ satisfy $|y/z|, |v/w| \le \frac{2}{5}$.

(ii) *If $z = x + iy \in S$ satisfies $|y/z| \le \frac{2}{5}$, then $\log_S z^{-1} = -\log_S z$.*

(iii) *For any $x \in \mathbf{R}_{>0}$, $\log_S x = \log_{\mathbf{R}} x$.*

(iv) *If $z \in \overline{D}_{2/5}(1)$, then $\log_S z = \log_D z$.*

Proof:

(i): We have $\operatorname{sgn} zw = \operatorname{sgn} z \operatorname{sgn} w$, hence the identity follows from eq. (4) in Lemma 3.19 and Lemma 3.23.

If $|y/z| \le 0.4$, then $x^2/|z|^2 \ge 1 - 0.4^2 = 0.84$, hence $x/|z| \ge 0.916$, and $|\operatorname{sgn} z - 1|^2 = 2\bigl(1 - x/|z|\bigr) \le 0.168$, thus $|\operatorname{sgn} z - 1| \le 0.41$. Likewise, $|v/w| \le 0.4$ implies $|\operatorname{sgn} w - 1| \le 0.41$, hence $\bigl(1 + |\operatorname{sgn} z - 1|\bigr)\bigl(1 + |\operatorname{sgn} w - 1|\bigr) \le 1.41^2 <^* 2$.

(ii): Write $z^{-1} = u + iv$. Since $z^{-1} = \overline{z}/|z|^2$, we have $v/|z^{-1}| = -y/|z|$, hence $\log_S z + \log_S z^{-1} = 0$ by (i).

(iii) is immediate, as $\operatorname{sgn} x = 1$ for $x \in \mathbf{R}_{>0}$.

(iv): Assume $|z-1| \leq \frac{2}{5}$. The triangle inequality (Lemma 2.1) implies $|z| \in \left[\frac{3}{5}, \frac{7}{5}\right] \subseteq \left(\frac{1}{3}, \frac{3}{2}\right)^*$, thus

$$\log_S z = \log_{\mathbf{R}}|z| + \log_D \operatorname{sgn} z = \log_D|z| + \log_D \operatorname{sgn} z,$$

and $\big||z| - 1\big| \leq \frac{2}{5}$. Moreover,

$$\frac{2}{5} \geq |z-1| = \left|\frac{z}{|z|}\left(|z| - \frac{\overline{z}}{|z|}\right)\right| = \left||z| - \frac{\overline{z}}{|z|}\right| \geq \frac{|y|}{|z|},$$

hence $|\operatorname{sgn} z - 1| \leq 0.41$ by the proof of (i). Thus,

$$\log_D|z| + \log_D \operatorname{sgn} z = \log_D z$$

by (4). □

3.5 Complex square root

The idea for our final extension of log is to widen the domain of $\log_S$ by several iterations of $\log z = 2 \log \sqrt{z}$ (each of which doubles the angle of the sector) until it covers all of $\mathbf{C}_{\neq 0}$. To do that, we need first to define carefully the complex square root function with the right branch cut, and establish its properties.

Definition 3.27 We define the *lopsided sign* function $\operatorname{sgn}^+ \colon \mathbf{R} \to \{-1, 1\}$ by

$$\operatorname{sgn}^+ y = \begin{cases} 1 & \text{if } y \geq 0, \\ -1 & \text{if } y < 0, \end{cases}$$

and the *complex square root* function $\sqrt{} \colon \mathbf{C} \to \mathbf{C}$ for $z = x + iy$ by

$$\sqrt{z} = \sqrt{\frac{|z| + x}{2}} + i\sqrt{\frac{|z| - x}{2}} \operatorname{sgn}^+ y.$$

Lemma 3.28

(i) *For all* $z \in \mathbf{C}$, $\left(\sqrt{z}\right)^2 = z$ *and* $\operatorname{sgn}^+ \operatorname{Im} \sqrt{z} = \operatorname{sgn}^+ \operatorname{Im} z$.

(ii) *For any* $z \in \mathbf{C} \smallsetminus \mathbf{R}_{<0}$, $\sqrt{\overline{z}} = \overline{\sqrt{z}}$.

(iii) *The restrictions* $\sqrt{} \restriction \mathbf{C} \smallsetminus \mathbf{R}_{<0}$ *and* $\sqrt{} \restriction \{z : \operatorname{Im} z \geq 0\}$ *are continuous.*

Proof:

(i): Write $z = x + iy$ and $\sqrt{z} = u + iv$. We have $u^2 - v^2 = x$ and

$$2uv = 2\sqrt{\frac{|z|^2 - x^2}{4}} \operatorname{sgn}^+ y = |y| \operatorname{sgn}^+ y = y,$$

thus $(u+iv)^2 = z$. Clearly, $\operatorname{sgn}^+ v = \operatorname{sgn}^+ y$ if $v \neq 0$; otherwise, $y = v = 0$.

(ii): For $z \in \mathbf{R}_{\geq 0}$, $\sqrt{z} \in \mathbf{R}$; for $z \notin \mathbf{R}$, the only difference between $\sqrt{z}$ and $\sqrt{\bar{z}}$ is that $\operatorname{sgn}^+ y$ is negated.

(iii): Being a composition of continuous functions, $\sqrt{} \restriction \{z : \operatorname{Im} z \geq 0\}$ is continuous. Thus, in view of (ii), $\sqrt{} \restriction \{z \notin \mathbf{R}_{<0} : \operatorname{Im} z \leq 0\}$ is continuous, which we can glue with $\sqrt{} \restriction \{z \notin \mathbf{R}_{<0} : \operatorname{Im} z \geq 0\}$ to get the continuity of $\sqrt{} \restriction \mathbf{C} \smallsetminus \mathbf{R}_{<0}$. $\square$

The next lemma elucidates how we can use $\sqrt{}$ to enlarge the defining sector of log.

Lemma 3.29 *Let $z \in \mathbf{C}$ and $w = \sqrt{z}$.*

(i) $\operatorname{Re} w \geq 0$, *with strict inequality if $z \notin \mathbf{R}_{\leq 0}$.*

(ii) *If* $\operatorname{Re} z \geq 0$, *then* $|\operatorname{Im} w| \leq \operatorname{Re} w$, *with strict inequality if* $\operatorname{Re} z > 0$.

(iii) *If* $|\operatorname{Im} z| \leq \operatorname{Re} z$, *then* $|\operatorname{Im} w| \leq \frac{2}{5}|w|$.

Proof: (i) and (ii) are immediate from the definition.

(iii): Write $z = x + iy$ and $w = u + iv$. We have $x \geq 0$ and $2x^2 \geq |z|^2$, hence $x \geq \frac{7}{10}|z|$. It follows that $v^2 = \frac{1}{2}\bigl(|z| - x\bigr) \leq \frac{3}{20}|z| = \frac{3}{20}|w|^2$, thus $|v| \leq \frac{2}{5}|w|$. $\square$

As we already mentioned, a crucial property of log we need to show is $\log zw = \log z + \log w$ under suitable restrictions on z, w. Extending this identity from $\log_S$ to full log will require multiplicativity of the square root function, thus let us establish some convenient conditions under which the latter holds.

Lemma 3.30 *If $z, w \in \mathbf{C}$ are such that* $\operatorname{Re} z \geq 0$ *and* $\operatorname{Re} w > 0$, *then* $\sqrt{zw} = \sqrt{z}\sqrt{w}$.

Proof: Since $(\sqrt{z}\sqrt{w})^2 = zw$, we have $\sqrt{z}\sqrt{w} = \pm\sqrt{zw}$; we only need to check that the sign is correct. Write $\sqrt{z} = x + iy$, $\sqrt{w} = u + iv$. We have $x \geq |y|$ and $u > |v|$ by Lemma 3.29, hence $\operatorname{Re}\bigl(\sqrt{z}\sqrt{w}\bigr) = xu - yv > 0$ (unless $x = y = 0$, thus $z = 0$), which means, in view of Lemma 3.29 (i), that $\sqrt{zw} \neq -\sqrt{z}\sqrt{w}$. Thus, $\sqrt{zw} = \sqrt{z}\sqrt{w}$ as required. $\square$

We can, in fact, formulate a comprehensive criterion for multiplicativity of $\sqrt{}$. (One can check that the sufficient condition below is also necessary up to exchanging z and w, though we will not need this.)

Lemma 3.31 *Let $z, w \in \mathbf{C}$ be such that* $\operatorname{sgn}^+ \operatorname{Im} zw \in \{\operatorname{sgn}^+ \operatorname{Im} z, \operatorname{sgn}^+ \operatorname{Im} w\}$ *and* $z \notin \mathbf{R}_{<0}$. *Then* $\sqrt{zw} = \sqrt{z}\sqrt{w}$.

Proof: Write $\sqrt{z} = x + iy$, $\sqrt{w} = u + iv$. Assume first that $\operatorname{sgn}^+ \operatorname{Im} z \neq \operatorname{sgn}^+ \operatorname{Im} w$; say, $\operatorname{Im} z \geq 0 > \operatorname{Im} w$. Then $y \geq 0 > v$ by Lemma 3.28, and $x \geq 0$, $u > 0$ by Lemma 3.29, hence $\operatorname{Re}\bigl(\sqrt{z}\sqrt{w}\bigr) = xu - yv > 0$ unless $x = y = 0$ (in which case $z = 0 = zw$). Thus, $\sqrt{zw} = \sqrt{z}\sqrt{w}$ using Lemma 3.29.

Next, assume $\operatorname{Im} z, \operatorname{Im} w, \operatorname{Im}(zw) < 0$. Then $x, u > 0 > y, v$ by Lemmas 3.28 and 3.29, thus $\operatorname{Im}\bigl(\sqrt{z}\sqrt{w}\bigr) = xv + yu < 0$, which implies $\sqrt{zw} = \sqrt{z}\sqrt{w}$ using Lemma 3.28.

Finally, if $\operatorname{Im} z, \operatorname{Im} w, \operatorname{Im} zw \geq 0$, we have $x, u, y, v \geq 0$, hence $\operatorname{Im}\bigl(\sqrt{z}\sqrt{w}\bigr) = xv + yu \geq 0$. If the inequality is strict, we get $\sqrt{zw} = \sqrt{z}\sqrt{w}$ using Lemma 3.28 again. Otherwise $xv = yu = 0$:

thus, $x = 0$ (in which case either $z = 0 = zw$ or $z \in \mathbf{R}_{<0}$, but the latter is ruled out), or $u = v = 0$ (in which case $w = 0 = zw$), or $y = v = 0$ (in which case $z, w, zw \in \mathbf{R}_{\geq 0}$). $\square$

Corollary 3.32 *If* $z \in \mathbf{C} \smallsetminus \mathbf{R}_{<0}$, *then* $\sqrt{z^{-1}} = \left(\sqrt{z}\right)^{-1}$.

Proof: $\operatorname{Im} z$ and $\operatorname{Im} z^{-1}$ have opposite signs. $\square$

Remark 3.33 We can restate Lemma 3.31 in the following symmetric form: if $z_0, z_1, z_2 \in \mathbf{C}$ are such that $z_0 z_1 z_2 = 1$, then $\sqrt{z_0}\sqrt{z_1}\sqrt{z_2} = 1$, unless $\operatorname{sgn}^+ z_0 = \operatorname{sgn}^+ z_1 = \operatorname{sgn}^+ z_2$ and at most one z_j is in $\mathbf{R}_{>0}$. Lemma 3.37 (ii) below can also be stated like this.

3.6 Full complex logarithm

In this section, we are going to finish the definition of log (and, eventually, exp), and prove the remaining desired properties of log and exp, such as the right inverse property $\exp \log z = z$.

Definition 3.34 We put $\sqrt[4]{z} = \sqrt{\sqrt{z}}$, $\sqrt[8]{z} = \sqrt{\sqrt[4]{z}}$, and define $\log_{\mathbf{C}} \colon \mathbf{C}_{\neq 0} \to \mathbf{C}_{\mathbf{L}}$ by

$$\log_{\mathbf{C}} z = 8 \log_S \sqrt[8]{z}.$$

Note that $\sqrt[8]{z} \in S$ by Lemmas 3.29 and 3.25.

In fact, we have even $\sqrt[4]{z} \in S$ for all $z \neq 0$, hence already $4 \log_S \sqrt[4]{z}$ would define log on all of $\mathbf{C}_{\neq 0}$. The purpose of the extra iteration of $\sqrt{}$ is to facilitate our proof of $\log zw = \log z + \log w$ below.

We start with a few basic properties that follow either directly from the definition, or from properties of $\log_S$ and $\sqrt{}$.

Lemma 3.35 *The restrictions* $\log_{\mathbf{C}} \restriction \mathbf{C} \smallsetminus \mathbf{R}_{<0}$ *and* $\log_{\mathbf{C}} \restriction \{z : \operatorname{Im} z \geq 0\}$ *are continuous.*

Proof: This follows from Lemma 3.28 (iii) and the continuity of $\log_S$. $\square$

Lemma 3.36 *If* $z \in \mathbf{C}_{\neq 0}$ *and* $|\operatorname{Im} z| \leq \operatorname{Re} z$, *then* $\log_{\mathbf{C}} z = \log_S z$.

Consequently, $\log_{\mathbf{C}} z = \log_{\mathbf{R}} z$ *for* $z \in \mathbf{R}_{>0}$, *and* $\log_{\mathbf{C}} z = \log_D z$ *for* $z \in \overline{D}_{2/5}(1)$.

Proof: By Lemma 3.29, $w = \sqrt{z}$ satisfies $|\operatorname{Im} w| \leq \frac{2}{5}|w|$, hence $\log_S z = 2 \log_S w$ by Lemma 3.26. Iterating this argument, we obtain $\log_S z = 8 \log_S \sqrt[8]{z} = \log_{\mathbf{C}} z$. The rest follows by Lemma 3.26 (iii) and (iv). $\square$

We will improve Lemma 3.36 in Lemma 3.58.

Lemma 3.37

(i) *If* $z, w \in \mathbf{C}$ *are such that* $\operatorname{Re} z \geq 0$ *and* $\operatorname{Re} w > 0$, *then*

$$\log_{\mathbf{C}} zw = \log_{\mathbf{C}} z + \log_{\mathbf{C}} w. \tag{5}$$

(ii) *If* $z, w \in \mathbf{C}_{\neq 0}$ *satisfy* $\operatorname{sgn}^+ \operatorname{Im} zw \in \{\operatorname{sgn}^+ \operatorname{Im} z, \operatorname{sgn}^+ \operatorname{Im} w\}$ *and* $z \notin \mathbf{R}_{<0}$, *then* (5) *holds.*

(iii) *For all* $z \in \mathbf{C}_{\neq 0}$, $\log_{\mathbf{C}} z = 2\log_{\mathbf{C}} \sqrt{z}$.

(iv) *If* $z \in \mathbf{C} \smallsetminus \mathbf{R}_{\leq 0}$, *then* $\log_{\mathbf{C}} z^{-1} = -\log_{\mathbf{C}} z$ *and* $\log_{\mathbf{C}} \overline{z} = \overline{\log_{\mathbf{C}} z}$.

(v) *If* $|z| = 1$, *then* $\log_{\mathbf{C}} z \in i\mathbf{R}_{\mathbf{L}}$.

Proof:

(ii): The assumption implies $\sqrt{zw} = \sqrt{z}\sqrt{w}$ by Lemma 3.30. Moreover, $\operatorname{sgn}^+ \operatorname{Im}\sqrt{z} = \operatorname{sgn}^+ \operatorname{Im} z$ and $\sqrt{z} \notin \mathbf{R}_{<0}$, and similarly for w and zw, hence the original assumptions continue to hold with $\sqrt{z}$, $\sqrt{w}$ in place of z, w; thus, we can iterate the argument, eventually obtaining $\sqrt[8]{zw} = \sqrt[8]{z}\sqrt[8]{w}$. By Lemma 3.29, $\bigl|\operatorname{Im}\sqrt[8]{z}\bigr| \leq \frac{2}{5}\bigl|\sqrt[8]{z}\bigr|$, and similarly for $\sqrt[8]{w}$, hence

$$\log_S \sqrt[8]{z} + \log_S \sqrt[8]{w} = \log_S\bigl(\sqrt[8]{z}\sqrt[8]{w}\bigr) = \log_S \sqrt[8]{zw}$$

by Lemma 3.26. Multiplying by 8 yields (5).

(iii) follows from (ii) using Lemma 3.28 (i).

The proofs of (i) and the first identity in (iv) are similar to (ii), using Lemma 3.30 and Corollary 3.32 in place of Lemma 3.31.

In order to prove $\log_{\mathbf{C}} \overline{z} = \overline{\log_{\mathbf{C}} z}$ for $z \notin \mathbf{R}_{\leq 0}$, we first observe that $\lambda(\overline{z}, n) = \overline{\lambda(z, n)}$ for all $z \in \mathbf{Q}(i)$ and $n \in \mathbf{L}$, hence $\Lambda(\overline{z}) = \overline{\Lambda(z)}$ for $z \in D_1^*(0) \cap \mathbf{Q}(i)$, and $\log_D \overline{z} = \overline{\log_D z}$ for all $z \in D_1^*(1)$ by density. Since $\log_{\mathbf{R}}$ is real and $\operatorname{sgn}\overline{z} = \overline{\operatorname{sgn} z}$, we obtain $\log_S \overline{z} = \overline{\log_S z}$ for all $z \in S$. This implies $\log_{\mathbf{C}} \overline{z} = \overline{\log_{\mathbf{C}} z}$ for all $z \in \mathbf{C} \smallsetminus \mathbf{R}_{\leq 0}$ using Lemma 3.28 (ii).

(v): If $z \neq -1$, we have $\overline{\log_{\mathbf{C}} z} = \log_{\mathbf{C}} \overline{z} = \log_{\mathbf{C}} z^{-1} = -\log_{\mathbf{C}} z$, hence $\log_{\mathbf{C}} z$ is purely imaginary. The case $z = -1$ follows using (iii). $\square$

We now make a short detour: we define the argument function and establish its monotonicity properties. Besides being useful in its own right, our immediate goal here is to prove that $\log_{\mathbf{C}}$ is injective (which will be instrumental in deriving $\exp\log z = z$ from $\log\exp z = z$): the injectivity of $\log_{\mathbf{R}}$ ensures that $\operatorname{Re}\log_{\mathbf{C}} z = \log_{\mathbf{R}}|z|$ distinguishes numbers with different absolute values, and arg will give us a handle on numbers with the same absolute value. It will also help us establish the image of $\log_{\mathbf{C}}$.

Definition 3.38 If $z \in \mathbf{C}_{\neq 0}$, we define $\arg z = \operatorname{Im}\log_{\mathbf{C}} z$. Let $\pi = \arg(-1)$.

Lemma 3.39 *For any* $z \in \mathbf{C}_{\neq 0}$, $\arg z = \arg\operatorname{sgn} z$, *and* $\log_{\mathbf{C}} z = \log_{\mathbf{R}}|z| + i\arg z$.

Proof: We have $\log_{\mathbf{C}} z = \log_{\mathbf{R}}|z| + \log_{\mathbf{C}}\operatorname{sgn} z$ by Lemma 3.37 (ii), which implies $\operatorname{Im}\log_{\mathbf{C}} z = \operatorname{Im}\log_{\mathbf{C}}\operatorname{sgn} z$, and $\operatorname{Re}\log_{\mathbf{C}} z = \log_{\mathbf{R}}|z|$ using Lemma 3.37 (v). $\square$

Lemma 3.40 *Let* $z, w \in \mathbf{C}_{\neq 0}$.

(i) *If* $z \notin \mathbf{R}_{<0}$, *then* $\arg z^{-1} = \arg\overline{z} = -\arg z$.

(ii) *If* $\operatorname{Re} z \geq 0$ *or* $\operatorname{Im} z < 0$, *then* $\arg iz = \arg z + \frac{\pi}{2}$.

(iii) *If* $\operatorname{Im} z \geq 0$ *and* $z \notin \mathbf{R}_{>0}$, *then* $\arg z > 0$.

(iv) *If* $\operatorname{Re} z, \operatorname{Re} w \geq 0$, *then* $\arg z < \arg w$ *iff* $\operatorname{Im}\operatorname{sgn} z < \operatorname{Im}\operatorname{sgn} w$.

(v) *If* $\operatorname{Im} z, \operatorname{Im} w \geq 0$, *then* $\arg z < \arg w$ *iff* $\operatorname{Re}\operatorname{sgn} z > \operatorname{Re}\operatorname{sgn} w$.

(vi) $\arg z = \arg w$ *iff* $\operatorname{sgn} z = \operatorname{sgn} w$.

Proof:
(i) is immediate from 3.37 (iv).

(ii): We observe that $\arg i = \frac{\pi}{2}$ by Lemma 3.37 (iii), and apply Lemma 3.37 (ii): we have $\operatorname{Im} i > 0$ and $i \notin \mathbf{R}_{<0}$; if $\operatorname{Im} z < 0$, then $\operatorname{sgn}^+ \operatorname{Im} iz \in \{1, -1\}$ trivially, and if $\operatorname{Re} z \geq 0$, then $\operatorname{sgn}^+ \operatorname{Im} iz = 1$.

(iii): We may assume $|z| = 1$. Then $i \arg z = \log_{\mathbf{C}} z = 8 \log_S w = 8 \log_D w$, where $w = \sqrt[8]{z} = u + iv$ satisfies $0 < v \leq \frac{2}{5}$ by Lemma 3.28 (i) and Lemma 3.29, thus $|w - 1| \leq 0.41$ by the proof of Lemma 3.26 (i), whence $\operatorname{Im} \log_D w \geq v - |w-1|^2 = v + 2u - 2$ using Lemma 3.19. Since $v \geq \frac{5}{2} v^2$, we have $(2-v)^2 = 4 - 4v + v^2 \leq 4 - 9v^2 < 4u^2$, thus $2 - v < 2u$, i.e., $v + 2u - 2 > 0$.

(iv): We may assume $|z| = |w| = 1$. Write $z = x + iy$ and $w = u + iv$, thus $x, u \geq 0$.

If $v > y \geq 0$, then $x^2 = 1 - y^2 > 1 - v^2 = u^2$, thus $x > u \geq 0$, and $\operatorname{Im} w\overline{z} = xv - yu > 0$. It follows that

$$\arg w - \arg z = \arg w + \arg \overline{z} = \arg w\overline{z} > 0$$

using (i), (iii), and Lemma 3.37 (i).

If $0 \geq v > y$, then $\arg w = -\arg \overline{w} > -\arg \overline{z} = \arg z$ using the previous part (with z and w swapped) and (i).

If $v > 0 > y$, then $\arg w > \arg 1 > \arg z$ by the previous two cases. This completes the proof of the right-to-left implication in (iv).

If $y > v$, then $\arg z > \arg w$ by what we have already proved. If $y = v$, then $x^2 = u^2$, thus $x = u$, i.e., $z = w$ and $\arg z = \arg w$.

(v): We have $z = iz'$, $w = iw'$ for some z', w', which satisfy $\operatorname{Re} z', \operatorname{Re} w' \geq 0$, $\operatorname{Im}\operatorname{sgn} z' = -\operatorname{Re}\operatorname{sgn} z$, $\operatorname{Im}\operatorname{sgn} w' = -\operatorname{Re}\operatorname{sgn} w$, and $\arg z < \arg w$ iff $\arg z' < \arg w'$ by (ii), hence the result follows from (iv).

(vi): We have $\operatorname{sgn}^+ \arg z = \operatorname{sgn}^+ \operatorname{Im} z$ by (iii) and (i). Thus, if $\arg z = \arg w$, then either $\operatorname{Im} z, \operatorname{Im} w \geq 0$, in which case $\operatorname{sgn} z = \operatorname{sgn} w$ by (v), or $\operatorname{Im} z, \operatorname{Im} w < 0$, which reduces to the previous case by (i). $\square$

Corollary 3.41 *The function* $\log_{\mathbf{C}}$ *is injective.*

Proof: If $\log_{\mathbf{C}} z = \log_{\mathbf{C}} w$, then $\log_{\mathbf{R}} |z| = \log_{\mathbf{R}} |w|$ and $\arg z = \arg w$ by Lemma 3.39. The former implies $|z| = |w|$ by Lemma 3.10, while the latter implies $\operatorname{sgn} z = \operatorname{sgn} w$ by Lemma 3.40. Thus, $z = w$. $\square$

Corollary 3.42 *For any* $z \in \mathbf{C}_{\neq 0}$, $\arg z \in (-\pi, \pi]$ *and* $\log_{\mathbf{C}} z \in \mathbf{R}_{\mathbf{L}} + i(-\pi, \pi]$.

Proof: If $\operatorname{Im} z \geq 0$, we have $0 \leq \arg z \leq \pi$ by Lemma 3.40 (v). If $\operatorname{Im} z < 0$, then $0 < \arg \overline{z} = -\arg z < \pi$ using Lemma 3.40 (i). $\square$

Let us prove a yet another version of eq. (5) in Lemma 3.37, this time indicating exactly how much it may be off in cases where it does not hold.

Lemma 3.43 *For all $z, w \in \mathbf{C}_{\neq 0}$,*

$$\log_{\mathbf{C}} z + \log_{\mathbf{C}} w - \log_{\mathbf{C}} zw \in \{-2\pi i, 0, 2\pi i\}.$$

Proof: We first observe that $\log_{\mathbf{C}}(-z) = \log_{\mathbf{C}} z + \pi i$ when $\operatorname{Im} z < 0$ or $z \in \mathbf{R}_{>0}$ by Lemma 3.37 (ii), hence

$$\log_{\mathbf{C}}(-z) = \log_{\mathbf{C}} z \pm \pi i$$

for all $z \in \mathbf{C}_{\neq 0}$. Now, given $z, w \in \mathbf{C}_{\neq 0}$, let $z' = \pm z$ and $w' = \pm w$ be such that $\operatorname{Re} z' > 0$, or $\operatorname{Re} z' = 0$ and $\operatorname{Im} z' > 0$, and similarly for w'. Then

$$\log_{\mathbf{C}} z' + \log_{\mathbf{C}} w' = \log_{\mathbf{C}} z'w'$$

by Lemma 3.37 (i) (unless $\operatorname{Re} z' = \operatorname{Re} w' = 0$, i.e., $z', w' \in i\mathbf{R}_{>0}$, in which case the identity holds as well). Since 0 or 2 of z', w', $z'w'$ are negated as compared to z, w, zw (resp.), $\log_{\mathbf{C}} z + \log_{\mathbf{C}} w - \log_{\mathbf{C}} zw$ is a sum of 0 or 2 terms of the form $\pm\pi i$, which gives the result. $\Box$

One application is to estimate the value of π, which we indicate below (without actually carrying out the computation with standard rationals in the proof). The same argument can establish in VTC^0 all true inequalities of the form $q < \pi < r$ where $q, r \in \mathbb{Q}$ are standard.

Proposition 3.44 $3.1 < \pi < 3.2$.

Proof: Let $z = 1 + \frac{1}{100}i$. We have $\left|\log_{\mathbf{C}} z - \frac{1}{100}i\right| \leq \frac{1}{10000}$ by Lemmas 3.36 and 3.19, hence $\arg z \in [0.0099, 0.0101]$. One can check $\operatorname{Im} z^n > 0$ for $n = 1, \dots, 314$, thus $\log_{\mathbf{C}} z^{314} = 314 \log_{\mathbf{C}} z$ by repeated use of Lemma 3.37 (ii), which implies $\pi \geq 314 \arg z \geq 3.1086$ by Corollary 3.42. On the other hand, $\operatorname{Im} z^{315} < 0$, thus $\arg z^{315} < 0$ by Lemma 3.40; in view of Lemma 3.43 and Corollary 3.42, this means $-\pi < \log_{\mathbf{C}} z^{315} = 315 \arg z - 2\pi$, thus $\pi < 315 \arg z \leq 3.1815$. $\Box$

We now come to the crucial Cauchy functional equation for $\log\exp z$.

Lemma 3.45 *If $z \in \mathbf{R}_{\mathbf{L}} + i(-1,1)$, then $\operatorname{Re} \exp_{\mathbf{C}_{\mathbf{L}}} z > 0$. Consequently,*

$$\log_{\mathbf{C}} \exp_{\mathbf{C}_{\mathbf{L}}}(z + w) = \log_{\mathbf{C}} \exp_{\mathbf{C}_{\mathbf{L}}} z + \log_{\mathbf{C}} \exp_{\mathbf{C}_{\mathbf{L}}} w \tag{6}$$

for all $z, w \in \mathbf{R}_{\mathbf{L}} + i(-1,1)$.

Proof: Let $z = x + iy$ with $x \in \mathbf{R}_{\mathbf{L}}$ and $y \in (-1,1)$. We have $\left|\exp iy - (1 + iy)\right| \leq y^2$ by Lemma 3.10, hence $|\operatorname{Re} \exp iy - 1| \leq y^2 < 1$. Thus, $\operatorname{Re} \exp z = \exp x \operatorname{Re} \exp iy > 0$.

Assuming the same holds for w, we have

$$\log\exp(z + w) = \log(\exp z \exp w) = \log\exp z + \log\exp w$$

by Lemmas 3.10 and 3.37. $\Box$

We are heading towards a proof of $\log \exp z = z$ when z is sufficiently small. To this end, we intend to use the identity $\log \exp 2^{-n} z = 2^{-n} \log \exp z$ for $n \in \mathbf{L}$. This appears to follow "by induction on n" from (6), but there is an obstacle to formalizing this idea: z, $\exp z$, and $\log \exp z$ are elements of the completion $\mathbf{C}^{\mathfrak{M}}$, which is too big to be definable in $\mathfrak{M}$, hence we cannot use induction directly. Instead, we need to argue about Gaussian rational approximations of $\exp z$ and $\log \exp z$ for $z \in \mathbf{Q_L}(i)$; moreover, we need to make sure these approximations are computable by TC^0 functions so that the induction formula has the right complexity for VTC^0. On a more fundamental level, we need such approximations so that the facts we prove about exp, log, and other functions $\mathbf{C} \to \mathbf{C}$ can be transferred back to the language of VTC^0. This is the goal of the next lemma.

Lemma 3.46 *We can construct* TC^0 *functions* $E_{\mathbf{C_L}}(z,r,n)$, $SR_{\mathbf{R}}(x,n)$, $A_\times(z,n)$, $A_+(z,n)$, $SR_{\mathbf{C}}(z,n)$, $L_D(z,r,n)$, $L_{\mathbf{R}}(x,n)$, $L_{\mathbf{C}}(z,n)$, *and* $LE(z,r,n)$ *with the following properties.*

(i) $\mathrm{E}_{\mathbf{C_L}}(z,r,n)$ *is a multiplicative approximation of* $\exp_{\mathbf{C_L}} z$ *for* $z \in \mathbf{Q_L}(i)$, *parametrized by* $r \in \mathbf{L}$ *such that* $|z| \le r$.

(ii) $SR_{\mathbf{R}}(x,n)$ *is a multiplicative approximation of* $\sqrt{x}$ *for* $x \in \mathbf{Q}_{>0}$.

(iii) $A_\times(z,n)$ *and* $A_+(z,n)$ *are multiplicative and additive (respectively) approximations of* $|z| \in \mathbf{R}$ *for* $z \in \mathbf{Q}(i)$.

(iv) $SR_{\mathbf{C}}(z,n)$ *is a multiplicative approximation of* $\sqrt{z}$ *for* $z \in \mathbf{Q}(i) \smallsetminus \{0\}$.

(v) $L_D(z,r,n)$ *is an additive approximation of* $\log_D z$ *for* $z \in D_1^*(1) \cap \mathbf{Q}(i)$, *parametrized by* $r \in \mathbf{L}$ *such that* $|z-1| \le 1 - r^{-1}$.

(vi) $L_{\mathbf{R}}(x,n)$ *is an additive approximation of* $\log_{\mathbf{R}} x$ *for* $x \in \mathbf{Q}_{>0}$.

(vii) $L_{\mathbf{C}}(z,n)$ *is an additive approximation of* $\log_{\mathbf{C}} z$ *for* $z \in \mathbf{Q}(i) \smallsetminus \{0\}$.

(viii) $LE(z,r,n)$ *is an additive approximation of* $\log_{\mathbf{C}} \exp_{\mathbf{C_L}} z$ *for* $z \in \mathbf{Q_L}(i)$ *with* $|\mathrm{Im}\, z| < 1$, *parametrized by* $r \in \mathbf{L}$ *such that* $|z| \le r$.

Proof sketch: We employ the $e(z,n)$ function to construct $E_{\mathbf{C_L}}(z,r,n)$. The results of [8] give $SR_{\mathbf{R}}(x,n)$, which we use to construct $A_\times$, A_+, and $SR_{\mathbf{C}}(z,n)$. We define $L_D(z,r,n)$ using the $\lambda(z,n)$ function, combine it with the integer length function to get $L_{\mathbf{R}}(x,n)$, and we construct $L_{\mathbf{C}}(z,n)$ from L_D, $L_{\mathbf{R}}$, and $SR_{\mathbf{C}}$. Finally, we compose $E_{\mathbf{C_L}}$ and $L_{\mathbf{C}}$ to get $LE(z,r,n)$.

The tedious but mostly unenlightening details have been moved to the appendix: see Lemma A.1. □

Lemma 3.47 *For all* $z \in \mathbf{R_L} + i(-1,1)$ *and* $n \in \mathbf{L}$,

$$\log_{\mathbf{C}} \exp_{\mathbf{C_L}} 2^{-n} z = 2^{-n} \log_{\mathbf{C}} \exp_{\mathbf{C_L}} z.$$

Proof: In view of Lemmas 3.45 and 3.35, both sides are continuous in z (for fixed n), hence it suffices to prove the result for $z \in \mathbf{Q_L}(i)$ by density. Fix $z \in \mathbf{Q}(i)$ and $r \in \mathbf{L}$ such that $|z| \le r$ and $|\operatorname{Im} z| < 1$, and $t \in \mathbf{L}$; we will prove the TC^0 formula

$$\big|LE(2^{-n}z, r, t) - 2^{-n}LE(z, r, t)\big| \le 3 \cdot 2^{-t} \tag{7}$$

by induction on $n \in \mathbf{L}$. The statement for $n = 0$ is trivial. Assuming (7) holds for n, we have

$$\big|\log\exp 2^{-n}z - 2^{-n}LE(z, r, t)\big| \le 4 \cdot 2^{-t}$$

by Lemma 3.46. Since $\log\exp 2^{-n}z = 2\log\exp 2^{-(n+1)}z$ by Lemma 3.45,

$$\big|\log\exp 2^{-(n+1)}z - 2^{-(n+1)}LE(z, r, t)\big| \le 2 \cdot 2^{-t},$$

hence

$$\big|LE(2^{-(n+1)}z, r, t) - 2^{-(n+1)}LE(z, r, t)\big| \le 3 \cdot 2^{-t}$$

by Lemma 3.46.

In view of Lemma 3.46, (7) implies

$$\big|\log\exp 2^{-n}z - 2^{-n}\log\exp z\big| \le 4 \cdot 2^{-t} + 2^{-t-n} \le 5 \cdot 2^{-t}.$$

Since $t \in \mathbf{L}$ is arbitrary, we obtain $\log\exp 2^{-n}z = 2^{-n}\log\exp z$. □

In the real world, all continuous solutions of Cauchy's functional equation are linear. Armed with Lemma 3.47, we use a similar argument to derive $\log\exp z = z$ from the asymptotic estimate $\log\exp z = z + O(z^2)$ for small z.

Lemma 3.48 *For all $z \in \mathbf{R_L} + i(-1, 1)$, $\log_{\mathbf{C}}\exp_{\mathbf{C_L}} z = z$.*

Proof: For any $n \in \mathbf{L}$, we have

$$\log\exp z - z = 2^n\big(\log\exp 2^{-n}z - 2^{-n}z\big)$$

by Lemma 3.47. Assume $|z| \le r$. If $2^n \ge 4r$, then

$$\big|\exp 2^{-n}z - (1 + 2^{-n}z)\big| \le 2^{-2n}r^2 \le \tfrac{1}{4}2^{-n}r$$

by Lemma 3.10 (iv), hence

$$\big|\exp 2^{-n}z - 1\big| \le \tfrac{5}{4}2^{-n}r \le \tfrac{5}{16} < \tfrac{2}{5},$$

whence

$$\big|\log\exp 2^{-n}z - (\exp 2^{-n}z - 1)\big| \le |\exp 2^{-n}z - 1|^2 \le \tfrac{25}{16}2^{-2n}r^2$$

by Lemmas 3.36 and 3.19. Consequently,

$$\big|\log\exp 2^{-n}z - 2^{-n}z\big| \le \tfrac{25}{16}2^{-2n}r^2 + 2^{-2n}r^2 = \tfrac{41}{16}2^{-2n}r^2,$$

and

$$|\log\exp z - z| \le \tfrac{41}{16}2^{-n}r^2.$$

Since $n \in \mathbf{L}$ can be arbitrarily large, this implies $\log\exp z = z$. □

Corollary 3.49 *For all $z \in \mathbf{R_L} + i(-\pi, \pi]$, $\log_{\mathbf{C}} \exp_{\mathbf{C_L}} z = z$.*

Proof: Using Proposition 3.44, we have $w = \frac{1}{4}z \in \mathbf{R_L} + i(-1,1)$, hence

$$\log \exp z = \log\bigl((\exp w)^4\bigr) = 4 \log \exp w + 2\pi i\, n = z + 2\pi i\, n$$

for some $n \in \{-3, \dots, 3\}$ by Lemmas 3.10, 3.43, and 3.48. Since both $\log \exp z$ and z are in $\mathbf{R_L} + i(-\pi, \pi]$ due to Corollary 3.42, the only possibility is $n = 0$. □

We have everything ready to derive the crucial right inverse property:

Corollary 3.50 *For all $z \in \mathbf{C}_{\neq 0}$, $\exp_{\mathbf{C_L}} \log_{\mathbf{C}} z = z$.*

Proof: We have $\log_{\mathbf{C}} z \in \mathbf{R_L} + i(-\pi, \pi]$ by Corollary 3.42, hence

$$\log_{\mathbf{C}} \exp_{\mathbf{C_L}} \log_{\mathbf{C}} z = \log_{\mathbf{C}} z$$

by Corollary 3.49, and $\exp_{\mathbf{C_L}} \log_{\mathbf{C}} z = z$ by Corollary 3.41. □

A useful property to know is that we can compute powers by means of exp and log, namely $z^n = \exp(n \log z)$. It follows "by induction on n" from Corollary 3.50, but again, this takes a bit of work to formalize, as we have to carry out the induction argument using TC^0 approximations. In Section 4, we will use this property to justify the definition of complex exponentiation via $z^w = \exp(w \log z)$.

Lemma 3.51 *$\{z : \exp_{\mathbf{C_L}} z \in \mathbf{Q}(i)\}$ is dense in $\mathbf{C_L}$.*

Proof: For any $z \in \mathbf{C_L}$ and $0 < \delta \le \frac{4}{5}$, the image of $D_\delta(z)$ under exp includes

$$\{\exp z \exp w : w \in D_\delta(0)\} \supseteq \{w \exp z : \log w \in D_\delta(0)\} \supseteq \{w \exp z : w \in D_{\delta/2}(1)\}$$

using Lemma 3.10, Corollary 3.50, and Lemmas 3.19 and 3.36. □

Lemma 3.52 *If $z \in \mathbf{C_L}$ and $n \in \mathbf{Z_L}$, then $\exp_{\mathbf{C_L}} nz = (\exp_{\mathbf{C_L}} z)^n$. In particular, we have $\exp_{\mathbf{C_L}}(n \log_{\mathbf{C}} w) = w^n$ for all $w \in \mathbf{C}_{\neq 0}$.*

Proof: Without loss of generality, fix $n > 0$. In view of Lemma 3.51, we may assume $w := \exp z \in \mathbf{Q}(i)$ as both sides are continuous in z. For any $t \in \mathbf{L}$ such that $2^t \ge 8n + 42$, fix $z' \in \mathbf{Q}(i)$ and $r \in \mathbf{L}$ such that $|z' - z| \le 2^{-t}$ and $n|z'| \le r$; we will prove

$$\left| \frac{E_{\mathbf{C_L}}(mz', r, t)}{w^m} - 1 \right| \le (6m+1)2^{-t} \tag{8}$$

by induction on $m \le n$. The statement holds for $m = 0$. For the induction step, we have

$$\begin{aligned}
\left| \frac{\exp mz'}{E_{\mathbf{C_L}}(mz', r, t)} - 1 \right| &\le \frac{1}{2^t - 1} \le 2^{-t} + 2 \cdot 2^{-2t}, \\
\left| \frac{\exp((m+1)z')}{w^{m+1}} \frac{w^m}{\exp mz'} - 1 \right| &= \left| \frac{\exp z'}{w} - 1 \right| = \bigl|\exp(z' - z) - 1\bigr| \le 2^{-t} + 2^{-2t}, \\
\left| \frac{E_{\mathbf{C_L}}((m+1)z', r, t)}{\exp((m+1)z')} - 1 \right| &\le 2^{-t}
\end{aligned}$$

by Lemma 3.46 (i), Lemma 2.3 (iii), and Lemma 3.10, hence assuming (8) for $m < n$,

$$\left|\frac{\exp mz'}{w^m} - 1\right| \le (6m+2)2^{-t} + (6m+3)2^{-2t} + (12m+2)2^{-3t} \le (6m+3)2^{-t},$$

$$\left|\frac{\exp((m+1)z')}{w^{m+1}} - 1\right| \le (6m+4)2^{-t} + (6m+4)2^{-2t} + (6m+3)2^{-3t} \le (6m+5)2^{-t},$$

$$\left|\frac{E_{\mathbf{C_L}}((m+1)z', r, t)}{w^{m+1}} - 1\right| \le (6m+6)2^{-t} + (6m+5)2^{-2t} \le (6m+7)2^{-t}$$

using Lemma 2.3 (i).

By the first part of the induction step, (8) for $m = n$ gives

$$\left|\frac{\exp nz'}{w^n} - 1\right| \le (6n+3)2^{-t}.$$

Since

$$\left|\frac{\exp nz}{\exp nz'} - 1\right| = \left|\exp\bigl(n(z - z')\bigr) - 1\right| \le n2^{-t} + n^2 2^{-2t},$$

Lemma 2.3 (i) implies

$$\left|\frac{\exp nz}{w^n} - 1\right| \le (7n+3)2^{-t} + (7n^2+3n)2^{-2t} + (6n^3+3n^2)2^{-3t} \le 8n2^{-t}.$$

Since $t \in \mathbf{L}$ can be arbitrarily large, we obtain $\exp nz = w^n$. $\square$

Apart from its intrinsic value, we have a few applications for Lemma 3.52: it enables us to extend the definition of exp to $\mathbf{R_L} + i\mathbf{R}$ by exploiting its $2\pi i$-periodicity, and it implies numerical bounds on e based on the approximation $\bigl(1 + \frac{1}{n}\bigr)^n$. We start with the latter.

Definition 3.53 Let $e = \exp 1$.

Lemma 3.54 *Let $n \in \mathbf{L}$, $n > 0$.*

(i) $\bigl(1 + \frac{1}{n}\bigr)^n \le e \le \bigl(1 + \frac{1}{n}\bigr)^{n+1}$.

(ii) $2^n \le \exp n \le 4^n$.

(iii) $2.7 < e < 2.8$.

Proof:

(i): We have $1 + \frac{1}{n} \le \exp\frac{1}{n}$ by Lemma 3.11, thus $\bigl(1 + \frac{1}{n}\bigr)^n \le \exp 1 = e$ by Lemma 3.52 and the monotonicity of x^n. Likewise, Lemma 3.11 gives $1 - \frac{1}{n+1} \le \exp\bigl(-\frac{1}{n+1}\bigr)$, thus $\bigl(1 + \frac{1}{n}\bigr) = \bigl(1 - \frac{1}{n+1}\bigr)^{-1} \ge \exp\frac{1}{n+1}$, which implies $\bigl(1 + \frac{1}{n}\bigr)^{n+1} \ge e$.

(ii) follows from $2 = (1+1)^1 \le e \le (1+1)^2 = 4$ and Lemma 3.52.

(iii): One can check that $2.7048 < 1.01^{100} \le e \le 1.01^{101} < 2.7319$. $\square$

We can generalize Lemma 3.54 (i) to a form of the alternative definition

$$\exp z = \lim_{n\to\infty} \left(1 + \frac{z}{n}\right)^n.$$

Notice that we could not have actually used this expression to *define* exp, as it has relative error proportional to n^{-1}, hence it only determines logarithmically many most significant bits of $\exp z$ rather than its precise value.

Proposition 3.55 *If $z \in \mathbf{C}$ and $n \in \mathbf{L}_{>0}$ are such that $n \geq \max\{2|z|, |z|^2\}$, then*

$$\left| \frac{\left(1 + \frac{z}{n}\right)^n}{\exp_{\mathbf{C_L}} z} - 1 \right| \leq \frac{2|z|^2}{n}.$$

Proof: Let $w = n \log\left(1 + \frac{z}{n}\right) - z$. We have $|w| \leq \frac{1}{n}|z|^2 \leq 1$ by Lemma 3.19, hence $|\exp w - 1| \leq |w| + |w|^2 \leq 2|w|$ by Lemma 3.10, and

$$\left(1 + \frac{z}{n}\right)^n = \exp\left(n \log\left(1 + \frac{z}{n}\right)\right) = \exp(z + w) = \exp z \exp w$$

by Lemma 3.52. □

We now define our final extension of exp; since it will not be modified any further, it will not carry any subscript. Recall that $\mathbf{R}_{\downarrow\mathbf{L}} = \{x \in \mathbf{R} : \exists n \in \mathbf{L}\, x \leq n\} = \mathbf{R_L} \cup \mathbf{R}_{<0}$.

Lemma 3.56 *There is a unique function* $\exp\colon \mathbf{R}_{\downarrow\mathbf{L}} + i\mathbf{R} \to \mathbf{C}$ *such that*

$$\exp(z + 2\pi i n) = \exp_{\mathbf{C_L}} z$$

for all $z \in \mathbf{C_L}$ and $n \in \mathbf{Z}$, and $\exp z = 0$ when $\operatorname{Re} z \notin \mathbf{R_L}$. It satisfies

$$\exp(z + w) = \exp z \exp w \tag{9}$$

for all $z, w \in \mathbf{R}_{\downarrow\mathbf{L}} + i\mathbf{R}$. For each $r \in \mathbf{L}$, exp *is uniformly continuous on $(-\infty, r] + i\mathbf{R}$.*

Proof: Any $z \in \mathbf{R_L} + i\mathbf{R}$ can be written as $z' + 2\pi i n$ for $n \in \mathbf{Z}$ and $z' \in \mathbf{R_L} + i(-\pi, \pi] \subseteq \mathbf{C_L}$; on the other hand, if $z + 2\pi i n = z' + 2\pi i n'$, where $z, z' \in \mathbf{C_L}$ and $n, n' \in \mathbf{Z}$, we have $n - n' \in \mathbf{Z_L}$, thus

$$\exp_{\mathbf{C_L}} z' = \exp_{\mathbf{C_L}}\left(2\pi i(n - n')\right) \exp_{\mathbf{C_L}} z = (-1)^{2(n-n')} \exp_{\mathbf{C_L}} z = \exp_{\mathbf{C_L}} z$$

using Lemmas 3.10 and 3.52 (note that $\log_{\mathbf{C}}(-1) = \pi i$ by Lemma 3.39). This shows the existence and uniqueness of exp.

If $\operatorname{Re} z \notin \mathbf{R_L}$ or $\operatorname{Re} w \notin \mathbf{R_L}$, then the same holds for $z + w$, hence both sides of (9) equal 0. Otherwise, (9) follows from Lemma 3.10.

If $\operatorname{Re} z, \operatorname{Re} w \leq r$ and $|w - z| \leq 1$, we have

$$|\exp w - \exp z| = |\exp z||\exp_{\mathbf{C_L}}(w - z) - 1| \leq 2 \exp_{\mathbf{R_L}}(r)|w - z|$$

by (9) and Lemma 3.10 (iv), using that $|\exp_{\mathbf{C_L}} z| = \exp_{\mathbf{R_L}} \operatorname{Re} z \leq \exp_{\mathbf{R_L}} r$ by Lemma 3.10 (iii) and (ii) (if $\operatorname{Re} z \notin \mathbf{R_L}$, this bound holds trivially). □

We also extend our TC^0 approximation to exp. Notice that we cannot define a multiplicative approximation of exp by a TC^0 formula on a domain with real part crossing the $\mathbf{R_L}$ boundary, as this would give us a TC^0 definition of $\mathbf{Q_L}$ inside $\mathbf{Q}$, and therefore of $\mathbf{L}$ inside $\mathbf{N}$, contradicting induction.

Lemma 3.57 *There are* TC^0 *functions* $E_\times(z,r,n)$ *and* $E_+(z,r,n)$ *with the following properties.*

(i) $E_\times(z,r,n)$ *is a multiplicative approximation of* $\exp z$ *for* $z\in\mathbf{Q_L}+i\mathbf{Q}$*, parametrized by* $r\in\mathbf{L}$ *such that* $|\operatorname{Re} z|\le r$*.*

(ii) $E_+(z,r,n)$ *is an additive approximation of* $\exp z$ *for* $z\in\mathbf{Q_{\downarrow L}}+i\mathbf{Q}$*, parametrized by* $r\in\mathbf{L}$ *such that* $\operatorname{Re} z\le r$*.*

Proof sketch: We use $L_{\mathbf{C}}(-1,\dots)$ to compute $P\approx\pi$, and $N\in\mathbf{Z}$ close to $\frac{1}{2\pi}\operatorname{Im} z$. Then we define $E_\times(z,r,n)$ as $E_{\mathbf{C_L}}(z-2PNi,\dots)$. For $E_+(z,r,n)$, we use $E_\times(z,\dots)$ if $\operatorname{Re} z$ is not too negative, and 0 otherwise. Details are again presented in Lemma A.1 in the appendix. □

By Lemma 3.36, $\log_{\mathbf{R}}\subseteq\log_{\mathbf{C}}$, but we do not know yet whether $\log_{\mathbf{C}}$ extends $\log_D$ and $\log_S$ on the entirety of their domains. Let us remedy this now; since this establishes that all our $\log_X$ functions agree whenever they are defined, it justifies that we officially rename $\log_{\mathbf{C}}$ to just log.

Lemma 3.58 $\log_D\subseteq\log_{\mathbf{C}}$ *and* $\log_S\subseteq\log_{\mathbf{C}}$*.*

Proof: It is enough to prove the claim for $\log_D$: then for all $z\in S$,

$$\log_S z=\log_{\mathbf{R}}|z|+\log_D\operatorname{sgn} z=\log_{\mathbf{C}}|z|+\log_{\mathbf{C}}\operatorname{sgn} z=\log_{\mathbf{C}} z$$

using Lemma 3.37. Moreover, by the continuity of $\log_{\mathbf{C}}$ and $\log_D$, it suffices to show that $\log_{\mathbf{C}}$ agrees with $\log_D$ on $\mathbf{Q}(i)$.

Thus, let $z\in\mathbf{Q}(i)\cap\overline{D}_{1-h^{-1}}(0)$, where $h\in\mathbf{L}$, $h\ge 2$; we will show $\log_D(1+z)=\log_{\mathbf{C}}(1+z)$. Put $n=2h^2$. For each $j<n$, $\left|\frac{j}{n}z\right|\le 1-h^{-1}$, thus $\left|1+\frac{j}{n}z\right|\ge h^{-1}$, and

$$\left|\frac{1+\frac{j+1}{n}z}{1+\frac{j}{n}z}-1\right|=\left|\frac{z}{n+jz}\right|\le\frac{h}{n}|z|\le\frac{h}{n}=\frac{1}{2h}.$$

Since $(2-h^{-1})\bigl(1+(2h)^{-1}\bigr)=2-(2h^2)^{-1}<^* 2$ and $(2h)^{-1}\le\frac{2}{5}$, we obtain

$$\begin{aligned}\log_D\bigl(1+\tfrac{j+1}{n}z\bigr)-\log_D\bigl(1+\tfrac{j}{n}z\bigr)&=\log_D\left(1+\frac{z}{n+jz}\right)\\&=\log_{\mathbf{C}}\left(1+\frac{z}{n+jz}\right)\\&=\log_{\mathbf{C}}\bigl(1+\tfrac{j+1}{n}z\bigr)-\log_{\mathbf{C}}\bigl(1+\tfrac{j}{n}z\bigr)\end{aligned}$$

using Lemmas 3.19, 3.36, and 3.37, thus

$$\log_D\bigl(1+\tfrac{j+1}{n}z\bigr)-\log_{\mathbf{C}}\bigl(1+\tfrac{j+1}{n}z\bigr)=\log_D\bigl(1+\tfrac{j}{n}z\bigr)-\log_{\mathbf{C}}\bigl(1+\tfrac{j}{n}z\bigr).\tag{10}$$

Fix $t \in \mathbf{L}$; we will prove

$$\bigl|L_D\bigl(1 + \tfrac{j}{n}z, h, t\bigr) - L_{\mathbf{C}}\bigl(1 + \tfrac{j}{n}z, t\bigr)\bigr| \le (4j+2)2^{-t} \tag{11}$$

by induction on $j \le n$. Since $\log_D 1 = 0 = \log_{\mathbf{C}} 1$, the base case $j = 0$ follows immediately from Lemma 3.46. Assuming (11) holds for some $j < n$, Lemma 3.46 and (10) give

$$\begin{aligned}
\bigl|\log_D\bigl(1 + \tfrac{j+1}{n}z\bigr) - \log_{\mathbf{C}}\bigl(1 + \tfrac{j+1}{n}z\bigr)\bigr| &= \bigl|\log_D\bigl(1 + \tfrac{j}{n}z\bigr) - \log_{\mathbf{C}}\bigl(1 + \tfrac{j}{n}z\bigr)\bigr| \\
&\le (4j+4)2^{-t}, \\
\bigl|L_D\bigl(1 + \tfrac{j+1}{n}z, h, t\bigr) - L_{\mathbf{C}}\bigl(1 + \tfrac{j+1}{n}z, t\bigr)\bigr| &\le (4j+6)2^{-t}.
\end{aligned}$$

Taking (11) for $j = n$, Lemma 3.46 implies

$$\bigl|\log_D(1+z) - \log_{\mathbf{C}}(1+z)\bigr| \le (4n+4)2^{-t}.$$

Since $t \in \mathbf{L}$ can be chosen arbitrarily large, we obtain $\log_D(1+z) = \log_{\mathbf{C}}(1+z)$. □

To tie up one more loose end, Lemma 3.56 gives a useful result on uniform continuity of exp, but for log, we only have the rather unsatisfactory Lemma 3.18. Let us state a better result for the sake of completeness.

Lemma 3.59 *For every $\varepsilon \in \mathbf{R}_{>0}$,* log *is uniformly continuous on*

$$\bigl\{z \in \mathbf{C} : |z| \ge \varepsilon \wedge (\operatorname{Re} z \ge 0 \vee \operatorname{Im} z \ge 0 \vee \operatorname{Im} z \le -\varepsilon)\bigr\}.$$

Proof: We claim that if z, w belong to the indicated set, then for all $0 < \delta \le 1$,

$$|z - w| \le \frac{\varepsilon}{2}\delta \implies |\log z - \log w| \le \delta.$$

First, we observe

$$\left|\frac{w}{z} - 1\right| = \frac{|z-w|}{|z|} \le \frac{\varepsilon\delta/2}{\varepsilon} \le \frac{\delta}{2}, \qquad \left|\log\frac{w}{z}\right| \le \delta,$$

using Lemma 3.19. Thus, it suffices to show

$$\log z + \log\frac{w}{z} = \log w. \tag{12}$$

If $\operatorname{Re} z \ge 0$, then (12) is true by Lemma 3.37 (i), as $\operatorname{Re}(w/z) > 0$; if $\operatorname{Re} w \ge 0$, we may swap z and w, noting that $\log(z/w) = -\log(w/z)$ by Lemma 3.37 (iv). Thus, it remains to consider the case $\operatorname{Re} z, \operatorname{Re} w < 0$. Then either $\operatorname{Im} z, \operatorname{Im} w \ge 0$, or $\operatorname{Im} z, \operatorname{Im} w \le -\varepsilon$: we cannot have, say, $\operatorname{Im} z \ge 0$ and $\operatorname{Im} w \le -\varepsilon$, as $|z - w| < \varepsilon$.

Assume $\operatorname{Im} z, \operatorname{Im} w \ge 0$. Then $\operatorname{sgn}^+\bigl(z\frac{w}{z}\bigr) = \operatorname{sgn}^+ z$, hence (12) follows from Lemma 3.37 (ii), unless $z \in \mathbf{R}_{<0}$. Again, we may swap z and w if necessary, obtaining (12) unless $w \in \mathbf{R}_{<0}$ as well; but if $z, w \in \mathbf{R}_{<0}$ and $w/z \in \mathbf{R}_{>0}$, then (12) is also true.

If $\operatorname{Im} z, \operatorname{Im} w \le -\varepsilon$, we obtain (12) by applying the previous part to $\overline{z}, \overline{w}$ in place of z, w, using Lemma 3.37 (iv). □

Proof of Theorem 3.1: We refer to item numbers from the statement of Theorem 3.1.

Lemmas 3.10 and 3.56 ensure that (i) and (iii) hold (by definition), and that exp is a group homomorphism $\langle \mathbf{R_L} + i\mathbf{R}, +\rangle \to \langle \mathbf{C}_{\neq 0}, \cdot\rangle$ whose kernel includes $2\pi i\mathbf{Z}$. By Corollary 3.42, log maps $\mathbf{C}_{\neq 0}$ to $\mathbf{R_L} + i(-\pi, \pi]$, and $\exp \log z = z$ by Corollary 3.50, which also implies that $\exp\colon \mathbf{R_L} + i\mathbf{R} \to \mathbf{C}_{\neq 0}$ is surjective, and log is injective. Conversely, $\log \exp z = z$ for $z \in \mathbf{R_L} + i(-\pi, \pi]$ by Corollary 3.49, hence $\log\colon \mathbf{C}_{\neq 0} \to \mathbf{R_L} + i(-\pi, \pi]$ is surjective, and exp is injective on $\mathbf{R_L} + i(-\pi, \pi]$, which implies the kernel of exp is *exactly* $2\pi i\mathbf{Z}$: if $\exp(z) = 1$, we may write $z = w + 2\pi i\, n$ for some $n \in \mathbf{Z}$ and $w \in \mathbf{R_L} + i(-\pi, \pi]$; then $\exp w = 1$, hence $w = 0$. This gives (ii) and (iv).

(v) follows from Lemma 3.10 and (iv), using the fact that $\log \restriction \mathbf{R}_{>0}$ is real-valued due to Lemma 3.36. (vi) is stated in Lemmas 3.56, 3.35, and 3.59. (vii) follows from Lemmas 3.10 and 3.39.

(viii) follows from Lemma 3.40: e.g., if $z_0, z_1 \in \mathbf{C}_{\neq 0}$ are such that $\operatorname{Re} z_j \geq 0 \geq \operatorname{Im} z_j$, then $\arg z_0 < \arg z_1$ iff $\operatorname{Re} \operatorname{sgn} z_0 < \operatorname{Re} \operatorname{sgn} z_1$ iff $\operatorname{Im} \operatorname{sgn} z_0 < \operatorname{Im} \operatorname{sgn} z_1$ by Lemma 3.40 (i), (iv), and (v); in particular, $-\frac{\pi}{2} = \arg(-i) \leq \arg z_j \leq \arg 1 = 0$.

(ix) follows from Lemmas 3.10, 3.19, and 3.58; (x) is Lemma 3.52, (xi) is Proposition 3.55, and (xii) is Lemma 3.11 (with trivial extension to $\mathbf{R}_{\downarrow\mathbf{L}}$).

(xiii): Lemmas 3.46 and 3.57 (proved in Lemma A.1) give E_+, $E_\times$, and L_+ (called $L_\mathbf{C}$ there). The existence of $L_\times$ follows from Lemma 2.3: we only need to exhibit a TC^0 function $h\colon \mathbf{Q}(i) \smallsetminus \{0\} \to \mathbf{L}$ such that $|\log z| \geq 2^{-h(z)}$ for all $z \neq 0, 1$. If $0 < |z - 1| \leq \frac{1}{2}$, we have $|\log z| \geq |z - 1| - |z - 1|^2 \geq |z - 1|^2$ by (ix), hence it suffices to put $h(z) = \left\| \left\lceil |z - 1|^{-2} \right\rceil \right\|$ using integer division and the length function. We claim that if $|z - 1| \geq \frac{1}{2}$, then $|\log z| > \frac{1}{3}$, hence we can just take $h(z) = 2$: indeed, if $|\log z| \leq \frac{1}{3}$, then

$$|z - 1| = |\exp \log z - 1| \leq |\log z| + |\log z|^2 \leq \tfrac{4}{9} < \tfrac{1}{2}$$

by (iv) and (ix). □

4 Complex powers and iterated multiplication

Having completed our treatment of exp and log, we come to applications. The first one is a definition of powering. We have so far defined the powering function z^n for $z \in \mathbf{C}_{\neq 0}$ and $n \in \mathbf{Z_L}$ (and for $z = 0$ and $n \in \mathbf{L}$); we can now extend it to all exponents in $\mathbf{C_L}$.

Definition 4.1 If $z \in \mathbf{C}_{\neq 0}$ and $w \in \mathbf{C_L}$, let $z^w = \exp(w \log z)$.

Notice that this definition provides an alternative notation for exponentiation: $e^w = \exp w$. We will use this notation also when $\operatorname{Re} w \in \mathbf{R}_{\downarrow\mathbf{L}} \smallsetminus \mathbf{R_L}$ (even though we did not bother to define z^w in such circumstances).

Proposition 4.2 *Let $z, z' \in \mathbf{C}_{\neq 0}$ and $w, w' \in \mathbf{C_L}$.*

(i) *If $w \in \mathbf{Z_L}$, then z^w agrees with the previous definition. In particular, $z^0 = 1$ and $z^1 = z$.*

(ii) *$z^{w+w'} = z^w z^{w'}$ and $z^{-w} = 1/z^w$.*

(iii) *If* $\arg z + \arg z' \in (-\pi, \pi]$, *then* $(zz')^w = z^w z'^w$.

(iv) *If* $\operatorname{Im}(w \log z) \in (-\pi, \pi]$, *then* $(z^w)^{w'} = z^{ww'}$. *In particular, this holds when* $w \in (-1, 1]$, *or when* $z \in \mathbf{R}_{>0}$ *and* $w \in \mathbf{R}_{\mathbf{L}}$.

Proof:

(i) and (ii) follow from Theorem 3.1 (i), (iv), and (x).

(iii) follows from Corollary 3.2.

(iv): If $\operatorname{Im}(w \log z) \in (-\pi, \pi]$, then $\log z^w = w \log z$ by Theorem 3.1 (iv), thus $(z^w)^{w'} = \exp(w' w \log z) = z^{ww'}$. If $w \in \mathbf{R}_{\mathbf{L}}$, then $\operatorname{Im}(w \log z) = w \arg z$, which is in $(-\pi, \pi]$ if $w \in (-1, 1]$ or $\arg z = 0$. □

The usefulness of the general definition of z^w is limited, as $\log z$ is conceptually a multivalued function (only defined up to integer multiples of $2\pi i$), thus z^w should be only defined up to multiplying by integer powers of $\exp(2\pi i w)$; this explains why Proposition 4.2 (iii) and (iv) hold only under unsightly side conditions. The definition is better-behaved for:

- $w \in \mathbf{Z}_{\mathbf{L}}$, when it is independent of the branch of log, as $\exp(2\pi i w) = 1$; in this case, it coincides with the previous definition using iterated multiplication.
- $z \in \mathbf{R}_{>0}$, in which case the choice of the branch $\log z \in \mathbf{R}$ is canonical.

Another interesting case is $w = 1/n$, $n \in \mathbf{L}_{>0}$:

Definition 4.3 If $z \in \mathbf{C}_{\neq 0}$ and $n \in \mathbf{L}_{>0}$, let $\sqrt[n]{z} = z^{1/n}$. We also put $\sqrt[n]{0} = 0$.

Proposition 4.4 *Let* $z, z' \in \mathbf{C}$, $n, m \in \mathbf{L}_{>0}$, *and* $w \in \mathbf{C}_{\mathbf{L}}$.

(i) $\sqrt[1]{z} = z$ *and* $\sqrt[2]{z} = \sqrt{z}$.

(ii) $(\sqrt[n]{z})^w = z^{w/n}$. *In particular,* $(\sqrt[n]{z})^n = z$ *and* $\sqrt[m]{\sqrt[n]{z}} = \sqrt[nm]{z}$.

(iii) *If* $zz' = 0$ *or* $\arg z + \arg z' \in (-\pi, \pi]$, *then* $\sqrt[n]{zz'} = \sqrt[n]{z}\,\sqrt[n]{z'}$.

Proof: (ii) and (iii) follow from Proposition 4.2. (i): $\sqrt[1]{z} = z$ is clear, and

$$\sqrt{z} = \exp \log \sqrt{z} = \exp\bigl(\tfrac{1}{2} \log z\bigr) = \sqrt[2]{z}$$

by Lemma 3.37 (iii). □

The second application we promised in Section 2 is an extension of the definition of iterated multiplication $\prod_{j<n} z_j$ to coded sequences $\langle z_j : j < n \rangle$ of Gaussian rationals $z_j \in \mathbf{Q}(i)$. Basically, we want to put

$$\prod_{j<n} z_j = \exp\Bigl(\sum_{j<n} \log z_j\Bigr),$$

but we cannot do this directly as $\log z_j \notin \mathbf{Q}(i)$ in general, hence the sum is meaningless. We can use an approximation $L_+(z_j, t)$ instead of $\log z_j$, but then we have another problem—how to determine the exact result. For this reason, we first define $\prod_{j<n} z_j$ for Gaussian *integers* $z_j \in \mathbf{Z}[i]$, in which case we can round a sufficiently good approximation to an exact result.

Definition 4.5 We put $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor$ for $x \in \mathbf{R}$, and $\lfloor z \rceil = \lfloor \operatorname{Re} z \rceil + i \lfloor \operatorname{Im} z \rceil$ for $z \in \mathbf{C}$.

If $\langle z_j : j < n \rangle$ is a sequence of Gaussian integers $z_j = x_j + iy_j$, $x_j, y_j \in \mathbf{Z}$, we define

$$\prod_{j<n} z_j = \begin{cases} 0, & \text{if } z_j = 0 \text{ for some } j < n, \\ \left\lfloor E_\times \left(\sum_{j<n} L_+(z_j, t), r, t \right) \right\rceil, & \text{otherwise,} \end{cases}$$

where $r = 1 + \sum_j \big\| |x_j| + |y_j| \big\|$ and $t = r + 3 + \|n\|$.

If $\langle z_j : j < n \rangle$ is a sequence of Gaussian rationals $z_j = w_j / x_j$, where $w_j \in \mathbf{Z}[i]$ and $x_j \in \mathbf{Z}_{>0}$, we define

$$\prod_{j<n} z_j = \frac{\prod_{j<n} w_j}{\prod_{j<n} x_j}.$$

Observe that $\prod_{j<n} z_j$ is defined by a TC^0 function, and $\prod_{j<0} z_j = 1$, as $|E_\times(0, r, t) - 1| < \frac{1}{2}$.

Theorem 4.6 *For any sequence $\langle z_j : j \le n \rangle$ of Gaussian rationals,*

$$\prod_{j<n+1} z_j = z_n \prod_{j<n} z_j.$$

Proof: It suffices to prove the result for $z_j \in \mathbf{Z}[i] \smallsetminus \{0\}$. Let $z_j = x_j + iy_j$, $r_j = \big\| |x_j| + |y_j| \big\|$, $r = 1 + \sum_{j \le n} r_j$, and $t = r + 3 + \|n + 1\|$ as in the definition of $\prod_{j<n+1} z_j$; notice that $1 \le |z_j| \le |x_j| + |y_j| \le 2^{r_j}$, hence $0 \le \operatorname{Re} \log(z_j) \le r_j$ using Theorem 3.1 (vii) and Lemma 3.54. Thus,

$$\Big| \operatorname{Re} \sum_{j<m} L_+(z_j, t) \Big| \le \sum_{j<m} r_j + m 2^{-t} \le r$$

for all $m \le n + 1$, which ensures that the usage of $E_\times$ in the definition of $\prod_{j<n+1} z_j$ is sound, and more generally, that it makes sense to define

$$w_m = E_\times \Big(\sum_{j<m} L_+(z_j, t), r, t \Big), \qquad m \le n + 1.$$

We will prove

$$m > 0 \implies \lfloor w_m \rceil = z_{m-1} \lfloor w_{m-1} \rceil, \tag{13}$$

$$|\lfloor w_m \rceil| \le 2^{\sum_{j<m} r_j}, \tag{14}$$

$$\left| \frac{w_m}{\lfloor w_m \rceil} - 1 \right| \le (4m + 1) 2^{-t} \tag{15}$$

for all $m \le n + 1$ by induction on m. For $m = 0$, $|w_0 - 1| \le 2^{-t} < \frac{1}{2}$, thus $\lfloor w_0 \rceil = 1$, which gives the claim. Assume (13)–(15) hold for $m \le n$, we will prove them for $m + 1$. We have

$$\left| \frac{\exp \sum_{j<m} L_+(z_j, t)}{\lfloor w_m \rceil} - 1 \right| \le (4m + 2) 2^{-t} + O(m 2^{-2t})$$

by (15), the properties of $E_\times$, and Lemma 2.3, while $|L_+(z_m, t) - \log(z_m)| \le 2^{-t}$ gives

$$\left| \frac{\exp L_+(z_m, t)}{z_m} - 1 \right| = \big| \exp\big(L_+(z_m, t) - \log z_m \big) - 1 \big| \le 2^{-t} + O(2^{-2t}),$$

using Theorem 3.1 (ix). Thus,

$$\left|\frac{\exp \sum_{j\le m} L_+(z_j,t)}{z_m\lfloor w_m\rceil} - 1\right| \le (4m+3)2^{-t} + O(m2^{-2t}),$$
$$\left|\frac{w_{m+1}}{z_m\lfloor w_m\rceil} - 1\right| \le (4m+4)2^{-t} + O(m2^{-2t}) \le (4m+5)2^{-t},$$

using again Lemma 2.3 and the approximation property of $E_\times$. Since (14) and $|z_m| \le 2^{r_m}$ imply

$$\left|z_m\lfloor w_m\rceil\right| \le 2^{\sum_{j\le m} r_j} \le 2^{r-1},$$

we obtain

$$\left|w_{m+1} - z_m\lfloor w_m\rceil\right| \le (4n+5)2^{r-1-t} \le 2^{r+1+\|n+1\|-t} \le 2^{-2},$$

thus, in view of $z_m\lfloor w_m\rceil \in \mathbf{Z}[i]$,

$$\lfloor w_{m+1}\rceil = z_m\lfloor w_m\rceil.$$

This gives (13), (14), and (15) for $m+1$.

Now, (13) for $m = n+1$ shows

$$\prod_{j<n+1} z_j = \lfloor w_{n+1}\rceil = z_n\lfloor w_n\rceil.$$

Moreover, putting $r' = 1 + \sum_{j<n} r_j$, $t' = r' + 3 + \|n\|$, and

$$w'_m = E_\times\Big(\sum_{j<m} L_+(z_j,t'), r', t'\Big), \qquad m \le n,$$

the same argument as above shows

$$\lfloor w'_0\rceil = 1, \qquad \forall 0 < m \le n\ \lfloor w'_m\rceil = z_{m-1}\lfloor w'_{m-1}\rceil,$$

which implies $\lfloor w_m\rceil = \lfloor w'_m\rceil$ by induction on $m \le n$. Thus,

$$\lfloor w_n\rceil = \lfloor w'_n\rceil = \prod_{j<n} z_j,$$

completing the proof. □

5 Trigonometric and hyperbolic functions

Armed with complex exponential and logarithm, we can easily define trigonometric and hyperbolic functions and their inverses in the usual way. We present the definitions and a few basic properties below, mostly to indicate the effects of our setup with (possibly) $\mathbf{L} \ne \mathbf{N}$ on domains of the functions, but we will skip many routine details (which are generally easy to verify using Theorem 3.1); since we deal with 24 functions here, we cannot afford to give each the same level of attention we spent on exp and log.

Definition 5.1 We introduce the following functions, where we write $x = \operatorname{Re} z$:

$$
\begin{aligned}
\sinh\colon \mathbf{R_L} + i\mathbf{R} &\to \mathbf{C}, & \sinh z &= \tfrac{1}{2}\big(e^{z} - e^{-z}\big),\\
\sin\colon \mathbf{R} + i\mathbf{R_L} &\to \mathbf{C}, & \sin z &= \tfrac{1}{i}\sinh iz,\\
\cosh\colon \mathbf{R_L} + i\mathbf{R} &\to \mathbf{C}, & \cosh z &= \tfrac{1}{2}\big(e^{z} + e^{-z}\big),\\
\cos\colon \mathbf{R} + i\mathbf{R_L} &\to \mathbf{C}, & \cos z &= \cosh iz,\\
\tanh\colon \mathbf{C} \smallsetminus i\pi\big(\tfrac{1}{2} + \mathbf{Z}\big) &\to \mathbf{C}, & \tanh z &= \begin{cases} \dfrac{\sinh z}{\cosh z}, & x \in \mathbf{R_L} \\ \operatorname{sgn} x, & x \notin \mathbf{R_L} \end{cases} = \begin{cases} \dfrac{1 - e^{-2z}}{1 + e^{-2z}}, & x \geq 0, \\ \dfrac{e^{2z} - 1}{e^{2z} + 1}, & x \leq 0, \end{cases}\\
\tan\colon \mathbf{C} \smallsetminus \pi\big(\tfrac{1}{2} + \mathbf{Z}\big) &\to \mathbf{C}, & \tan z &= \tfrac{1}{i}\tanh iz,\\
\coth\colon \mathbf{C} \smallsetminus i\pi\mathbf{Z} &\to \mathbf{C}, & \coth z &= \begin{cases} \dfrac{\cosh z}{\sinh z}, & x \in \mathbf{R_L} \\ \operatorname{sgn} x, & x \notin \mathbf{R_L} \end{cases} = \begin{cases} \dfrac{1 + e^{-2z}}{1 - e^{-2z}}, & x \geq 0, \\ \dfrac{e^{2z} + 1}{e^{2z} - 1}, & x \leq 0, \end{cases}\\
\cot\colon \mathbf{C} \smallsetminus \pi\mathbf{Z} &\to \mathbf{C}, & \cot z &= i\coth iz,\\
\operatorname{sech}\colon \mathbf{C} \smallsetminus i\pi\big(\tfrac{1}{2} + \mathbf{Z}\big) &\to \mathbf{C}, & \operatorname{sech} z &= \begin{cases} \dfrac{1}{\cosh z}, & x \in \mathbf{R_L} \\ 0, & x \notin \mathbf{R_L} \end{cases} = \begin{cases} \dfrac{2e^{-z}}{1 + e^{-2z}}, & x \geq 0, \\ \dfrac{2e^{z}}{e^{2z} + 1}, & x \leq 0, \end{cases}\\
\sec\colon \mathbf{C} \smallsetminus \pi\big(\tfrac{1}{2} + \mathbf{Z}\big) &\to \mathbf{C}, & \sec z &= \operatorname{sech} iz,\\
\operatorname{csch}\colon \mathbf{C} \smallsetminus i\pi\mathbf{Z} &\to \mathbf{C}, & \operatorname{csch} z &= \begin{cases} \dfrac{1}{\sinh z}, & x \in \mathbf{R_L} \\ 0, & x \notin \mathbf{R_L} \end{cases} = \begin{cases} \dfrac{2e^{-z}}{1 - e^{-2z}}, & x \geq 0, \\ \dfrac{2e^{z}}{e^{2z} - 1}, & x \leq 0, \end{cases}\\
\csc\colon \mathbf{C} \smallsetminus \pi\mathbf{Z} &\to \mathbf{C}, & \csc z &= i\operatorname{csch} iz.
\end{aligned}
$$

Definition 5.2 A function f is *p-periodic* if $f(z + pn) = f(z)$ for all $z \in \operatorname{dom}(f)$ and $n \in \mathbf{Z}$, and *p-antiperiodic* if $f(z + pn) = (-1)^n f(z)$ for all $z \in \operatorname{dom}(f)$ and $n \in \mathbf{Z}$ (which implies it is $2p$-periodic).

Proposition 5.3 *Each of the 12 functions f from Definition 5.1 satisfies $f(\overline{z}) = \overline{f(z)}$, whence f maps $\mathbf{R} \cap \operatorname{dom}(f)$ to $\mathbf{R}$. The functions* sin, cos, sec, *and* csc *are π-antiperiodic;* sinh, cosh, sech, *and* csch *are πi-antiperiodic;* tan *and* cot *are π-periodic;* tanh *and* coth *are πi-periodic. The functions* cos, cosh, sec, *and* sech *are even, while the remaining 8 functions are odd.*

Proof: Straightforward consequence of $\exp \overline{z} = \overline{\exp z}$ and the πi-antiperiodicity of exp, which follow from Theorem 3.1. □

We now turn to inverse trigonometric and hyperbolic functions. Similar to log, these functions are multivalued, and it is a somewhat arbitrary decision how to choose their branch cuts;

we will define them in such a way that they extend the most natural choices of inverse *real* trigonometric and hyperbolic functions.

Definition 5.4 We introduce the functions below:

$$
\begin{aligned}
\operatorname{arsinh}\colon \mathbf{C} &\to \mathbf{R_L} + i\big[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big], & \operatorname{arsinh} z &= \log\big(z + \sqrt{z^2+1}\big),\\
\arcsin\colon \mathbf{C} &\to \big[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big] + i\mathbf{R_L}, & \arcsin z &= \tfrac{1}{i} \operatorname{arsinh} iz,\\
\operatorname{arcosh}\colon \mathbf{C} &\to \mathbf{R}_{\mathbf{L},\geq 0} + i(-\pi, \pi], & \operatorname{arcosh} z &= \log\big(z + \sqrt{z+1}\sqrt{z-1}\big),\\
\arccos\colon \mathbf{C} &\to [0, \pi] + i\mathbf{R_L}, & \arccos z &= \tfrac{\pi}{2} - \arcsin z,\\
\operatorname{artanh}\colon \mathbf{C} \smallsetminus \{\pm 1\} &\to \mathbf{R_L} + i\big(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big], & \operatorname{artanh} z &= \tfrac{1}{2} \log\big(\tfrac{1+z}{1-z}\big),\\
\arctan\colon \mathbf{C} \smallsetminus \{\pm i\} &\to \big(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big] + i\mathbf{R_L}, & \arctan z &= \tfrac{1}{i} \operatorname{artanh} iz,\\
\operatorname{arcoth}\colon \mathbf{C} \smallsetminus \{\pm 1\} &\to \mathbf{R_L} + i\big(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big], & \operatorname{arcoth} z &= \tfrac{1}{2} \log\big(\tfrac{z+1}{z-1}\big),\\
\operatorname{arccot}\colon \mathbf{C} \smallsetminus \{\pm i\} &\to [0, \pi) + i\mathbf{R_L}, & \operatorname{arccot} z &= \tfrac{\pi}{2} - \arctan z,\\
\operatorname{arsech}\colon \mathbf{C}_{\neq 0} &\to \mathbf{R}_{\mathbf{L},\geq 0} + i(-\pi, \pi], & \operatorname{arsech} z &= \operatorname{arcosh} z^{-1},\\
\operatorname{arcsec}\colon \mathbf{C}_{\neq 0} &\to [0, \pi] + i\mathbf{R_L}, & \operatorname{arcsec} z &= \arccos z^{-1},\\
\operatorname{arcsch}\colon \mathbf{C}_{\neq 0} &\to \mathbf{R_L} + i\big[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big], & \operatorname{arcsch} z &= \operatorname{arsinh} z^{-1},\\
\operatorname{arccsc}\colon \mathbf{C}_{\neq 0} &\to \big[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big] + i\mathbf{R_L}, & \operatorname{arccsc} z &= \arcsin z^{-1}.
\end{aligned}
$$

To see that the indicated codomains of these functions are valid, we need the following:

Lemma 5.5 *For all* $z \in \mathbf{C}$, $\operatorname{Re}\big(z + \sqrt{z^2+1}\big) \geq 0$ *and* $\big|z + \sqrt{z+1}\sqrt{z-1}\big| \geq 1$.

Proof: Putting $w_\pm = \sqrt{z^2+1} \pm z$ for $\pm \in \{+,-\}$, we have $w_+ w_- = 1$, i.e., $w_- = \overline{w_+}/|w_+|^2$. We obtain $\operatorname{sgn}^+ \operatorname{Re} w_+ = \operatorname{sgn}^+ \operatorname{Re} w_- = \operatorname{sgn}^+ \operatorname{Re}(w_+ + w_-) = \operatorname{sgn}^+ \operatorname{Re} \sqrt{z^2+1} = 1$, using Lemma 3.29.

Observe that if z_0 and z_1 belong to the same quadrant, then $|z_0 + z_1| \geq |z_0 - z_1|$: writing $z_j = x_j + iy_j$, we have $|z_0 + z_1|^2 = (x_0 + x_1)^2 + (y_0 + y_1)^2 \geq (x_0 - x_1)^2 + (y_0 - y_1)^2 = |z_0 - z_1|^2$ as $x_0 x_1 + y_0 y_1 \geq 0$.

Lemmas 3.28 and 3.29 give $\operatorname{Re} \sqrt{z \pm 1} \geq 0$ and $\operatorname{sgn}^+ \operatorname{Im} \sqrt{z \pm 1} = \operatorname{sgn}^+ \operatorname{Im} z$, hence

$$\big|\sqrt{z+1} + \sqrt{z-1}\big| \geq \big|\sqrt{z+1} - \sqrt{z-1}\big|$$

by the observation above. Since $\big(\sqrt{z+1} \pm \sqrt{z-1}\big)^2 = 2z \pm 2\sqrt{z+1}\sqrt{z-1}$, we obtain

$$\big|z + \sqrt{z+1}\sqrt{z-1}\big| \geq \big|z - \sqrt{z+1}\sqrt{z-1}\big|.$$

In view of $\big(z + \sqrt{z+1}\sqrt{z-1}\big)\big(z - \sqrt{z+1}\sqrt{z-1}\big) = 1$, this shows $\big|z + \sqrt{z+1}\sqrt{z-1}\big| \geq 1$. □

The functions as presented in Definition 5.4 are not quite surjective. Their precise ranges as well as the complete structure of preimages of trigonometric and hyperbolic functions in the complex and real cases are described below.

Proposition 5.6 *Let* $f\colon \operatorname{dom}(f) \to \operatorname{cod}(f)$ *be a hyperbolic or trigonometric function from Definition 5.1,* $g\colon \operatorname{dom}(g) \to \operatorname{cod}(g)$ *the corresponding function from Definition 5.4, and* $B(g)$, $X(g)$, $\operatorname{dom}_{\mathbf{R}}(g)$, $\operatorname{im}_{\mathbf{R}}(g)$ *the corresponding sets in Table 1. Let* $\operatorname{dom}_{\mathbf{R}}(f) = \operatorname{dom}(f) \cap \mathbf{R}$ *if* f *is trigonometric, and* $\operatorname{dom}_{\mathbf{R}}(f) = \operatorname{dom}(f) \cap \mathbf{R_L}$ *if it is hyperbolic.*

g	$B(g)$	$X(g)$	$\mathrm{dom}_{\mathbf{R}}(g)$	$\mathrm{im}_{\mathbf{R}}(g)$	$f^{-1}(z)$
arsinh	$\pm i(1,\infty)$	$\pm\big(\mathbf{R}_{\mathbf{L},<0} + i\frac{\pi}{2}\big)$	$\mathbf{R}$	$\mathbf{R}_{\mathbf{L}}$	$w + 2\pi i\mathbf{Z}$ $\pi i - w + 2\pi i\mathbf{Z}$
arcsin	$\pm(1,\infty)$	$\pm\big(\frac{\pi}{2} + i\mathbf{R}_{\mathbf{L},>0}\big)$	$[-1,1]$	$\big[-\frac{\pi}{2},\frac{\pi}{2}\big]$	$w + 2\pi\mathbf{Z}$ $\pi - w + 2\pi\mathbf{Z}$
arcosh	$(-\infty,1)$	$i(-\pi,0)$	$[1,\infty)$	$\mathbf{R}_{\mathbf{L},\geq 0}$	$\pm w + 2\pi i\mathbf{Z}$
arccos	$\pm(1,\infty)$	$(\pi + i\mathbf{R}_{\mathbf{L},>0})$ $\cup\, i\mathbf{R}_{\mathbf{L},<0}$	$[-1,1]$	$[0,\pi]$	$\pm w + 2\pi\mathbf{Z}$
artanh	$\pm[1,\infty)$	$i\frac{\pi}{2}$	$(-1,1)$	$\mathbf{R}_{\mathbf{L}}$	$w + \pi i\mathbf{Z}$
arctan	$\pm i[1,\infty)$	$\frac{\pi}{2}$	$\mathbf{R}$	$\big(-\frac{\pi}{2},\frac{\pi}{2}\big)$	$w + \pi\mathbf{Z}$
arcoth	$[-1,1]$	0	$\pm(1,\infty)$	$\mathbf{R}_{\mathbf{L},\neq 0}$	$w + \pi i\mathbf{Z}$
arccot	$\pm i[1,\infty)$	0	$\mathbf{R}$	$(0,\pi)$	$w + \pi\mathbf{Z}$
arsech	$(-\infty,0]$ $\cup\,(1,\infty)$	$i(-\pi,0) \cup \big\{i\frac{\pi}{2}\big\}$	$(0,1]$	$\mathbf{R}_{\mathbf{L},\geq 0}$	$\pm w + 2\pi i\mathbf{Z}$
arcsec	$(-1,1)$	$(\pi + i\mathbf{R}_{\mathbf{L},>0})$ $\cup\, i\mathbf{R}_{\mathbf{L},<0} \cup \big\{\frac{\pi}{2}\big\}$	$\pm[1,\infty)$	$[0,\pi] \setminus \big\{\frac{\pi}{2}\big\}$	$\pm w + 2\pi\mathbf{Z}$
arcsch	$i(-1,1)$	$\pm\big(\mathbf{R}_{\mathbf{L},<0} + i\frac{\pi}{2}\big)$ $\cup\,\{0\}$	$\mathbf{R}_{\neq 0}$	$\mathbf{R}_{\mathbf{L},\neq 0}$	$w + 2\pi i\mathbf{Z}$ $\pi i - w + 2\pi i\mathbf{Z}$
arccsc	$(-1,1)$	$\pm\big(\frac{\pi}{2} + i\mathbf{R}_{\mathbf{L},>0}\big)$ $\cup\,\{0\}$	$\pm[1,\infty)$	$\big[-\frac{\pi}{2},\frac{\pi}{2}\big] \setminus \{0\}$	$w + 2\pi\mathbf{Z}$ $\pi - w + 2\pi\mathbf{Z}$

Table 1: Properties of inverse hyperbolic and trigonometric functions (see Proposition 5.6)

(i) *The function g is continuous in $\mathbf{C} \setminus B(g)$.*

(ii) *The image of g is $\mathrm{cod}(g) \setminus X(g)$. We have $f(g(z)) = z$ for all $z \in \mathrm{dom}(g)$, and $g(f(z)) = z$ for all $z \in \mathrm{cod}(g) \setminus X(g)$.*

(iii) *f maps $\mathrm{dom}_{\mathbf{R}}(f)$ onto $\mathrm{dom}_{\mathbf{R}}(g)$, and g maps $\mathrm{dom}_{\mathbf{R}}(g)$ onto $\mathrm{im}_{\mathbf{R}}(g)$.*

(iv) *If $g(z) = w$, then $f^{-1}(z)$ is the set described in the last column of Table 1.*

Proof: Left to the reader. $\square$

Using Theorem 3.1, it is routine to prove all standard trigonometric identities. The following is just an example.

Proposition 5.7 *For all $z, w \in \mathbf{R} + i\mathbf{R_L}$,*

$$\sin^2 z + \cos^2 z = 1, \tag{16}$$

$$\sin(z+w) = \sin z \cos w + \cos z \sin w. \tag{17}$$

Proof:

$$\begin{aligned}
\sin z \cos w + \cos z \sin w &= \frac{(e^{iz} - e^{-iz})(e^{iw} + e^{-iw}) + (e^{iz} + e^{-iz})(e^{iw} - e^{-iw})}{4i} \\
&= \frac{2e^{iz}e^{iw} - 2e^{-iz}e^{-iw}}{4i} \\
&= \frac{e^{i(z+w)} - e^{-i(z+w)}}{2i} = \sin(z+w).
\end{aligned}$$

We leave (16) to the reader. □

In order to work with the functions introduced in this section in inductive arguments and other reasoning within VTC^0, we need their TC^0 approximations. We start with the inverse functions which are relatively straightforward to approximate.

Proposition 5.8 *Each of the 12 functions $g(z)$ from Definition 5.4 has additive and multiplicative TC^0 approximations for $z \in \mathbf{Q}(i) \cap \operatorname{dom}(g)$.*

Proof: We only sketch the arguments, leaving details to the reader. Let us start with additive approximations.

For $\operatorname{artanh} z$, we can just take $\frac{1}{2}L_+\bigl(\frac{1+z}{1-z}, n\bigr)$; similarly for $\operatorname{arcoth} z$.

Using an additive approximation for $\sqrt{z}$ (which exists by Lemmas 3.46 and 2.2), we can compute an additive approximation to $z+\sqrt{z^2+1}$. In view of $\bigl(z+\sqrt{z^2+1}\bigr)\bigl(z-\sqrt{z^2+1}\bigr) = -1$, we can bound the value of $z+\sqrt{z^2+1}$ away from 0 by a TC^0 function of z, hence we can compute a multiplicative approximation of $z+\sqrt{z^2+1}$ using Lemma 2.2. Plugging it into L_+, we obtain an additive approximation of $\operatorname{arsinh} z$. A similar argument applies to $\operatorname{arcosh} z$: we apply L_+ to a multiplicative approximation of $z+\sqrt{z+1}\sqrt{z-1}$, making sure that its $\operatorname{sgn}^+ \operatorname{Im}$ is correct[4] so that we do not inadvertently cross the branch cut of log.

The remaining functions reduce to these four, either directly, or using an additive approximation for $\frac{\pi}{2}$ such as $\operatorname{Im} L_+(i, n)$.

In order to construct multiplicative approximations using Lemma 2.2, it suffices to bound $g(z)$ away from 0 (except for the at most one z where $g(z)$ is exactly 0). Let f be the hyperbolic or trigonometric function whose inverse g is. Since $f(g(z)) = z$, $g(z)$ is close to 0 only if z is in the f-image of a small neighbourhood of 0. If f is sinh, sin, tanh, or tan, then $g(z) = 0$ only if $z = 0$, and Theorem 3.1 (ix) implies that there is a constant $c > 0$ such that $|f(w) - w| \le c|w|^2$ for $|w| \le c$. Thus, $|g(z)| \ge \min\{c_1|z|, c_2\}$ for some constants $c_1, c_2 > 0$. If f is coth, cot, csch, or csc, then likewise $|g(z)| \ge \min\{c_1|z|^{-1}, c_2\}$ (here, $g(z)$ is never 0).

[4] We have $\operatorname{sgn}^+ \operatorname{Im}\bigl(z+\sqrt{z+1}\sqrt{z-1}\bigr) = \operatorname{sgn}^+ \operatorname{Im} z$ by a similar argument as in Lemma 5.5; if $\operatorname{sgn}^+ \operatorname{Im}$ of the computed multiplicative approximation is wrong, we adjust its imaginary part slightly by moving across the real axis, which can only improve the accuracy of the approximation. This issue does not arise for arsinh as $\operatorname{Re}\bigl(z+\sqrt{z^2+1}\bigr) \ge 0$ by Lemma 5.5.

For cosh, we can use the definitions of $\exp_{\mathbf{Q_L}(i)}$ and $\exp_{\mathbf{C_L}}$ to prove there is a constant $c > 0$ such that $\left|e^w - (1 + w + \frac{1}{2}w^2)\right| \le c|w|^3$ for $|w| \le c$, thus $\left|\cosh w - (1 + \frac{1}{2}w^2)\right| \le c|w|^3$, and $|\operatorname{arcosh} z| \ge \min\{c_1|z-1|^{1/2}, c_2\}$ for some constants $c_1, c_2 > 0$. Similarly for arccos, arsech, and arcsec. □

We now turn to approximation of hyperbolic and trigonometric functions. Many of these functions run into rough spots (singularities or zeros) near integer multiples of π, $i\pi$, $\frac{\pi}{2}$, or $i\frac{\pi}{2}$, hence we will need to parameterize their approximations to bound them away from the problematic points. Let us introduce some notation to this end.

Definition 5.9 For any $z \in \mathbf{C}$ and $\alpha \in \mathbf{C}_{\ne 0}$, we put

$$\operatorname{dist}(z, \alpha\mathbf{Z}) = \min\bigl\{|z - \alpha n| : n \in \mathbf{Z}\bigr\} = \bigl|z - \alpha\lfloor \operatorname{Re}(z/\alpha)\rceil\bigr|,$$

$$\operatorname{dist}(z, \alpha\mathbf{Z}_{\ne 0}) = \min\bigl\{|z - \alpha n| : n \in \mathbf{Z}_{\ne 0}\bigr\} = \begin{cases} \min\bigl\{|z-\alpha|, |z+\alpha|\bigr\}, & |\operatorname{Re}(z/\alpha)| \le \frac{1}{2}, \\ \operatorname{dist}(z, \alpha\mathbf{Z}), & \text{otherwise.} \end{cases}$$

(The expressions on the right-hand side exhibit that the minima exist.) More generally, if $\beta \in \mathbf{C}$, let $\operatorname{dist}(z, \beta + \alpha\mathbf{Z}) = \operatorname{dist}(z - \beta, \alpha\mathbf{Z})$.

Lemma 5.10 *For any $\alpha \in \mathbf{Q}(i) \smallsetminus \{0\}$ and $\beta \in \mathbf{Q}(i)$, there are additive* TC^0 *approximations $D_{\pi(\beta+\alpha\mathbf{Z})}(z)$ of $\operatorname{dist}\bigl(z, \pi(\beta + \alpha\mathbf{Z})\bigr)$, and $D_{\pi\alpha\mathbf{Z}_{\ne 0}}(z)$ of $\operatorname{dist}(z, \pi\alpha\mathbf{Z}_{\ne 0})$, for $z \in \mathbf{Q}(i)$.*

Proof: Similarly to Lemma A.1 (ix), let $m \in \mathbf{L}$ be such that $2^{m-c} \ge |\operatorname{Re} z| + |\operatorname{Im} z| + 1$ for a suitable constant c (depending on α, β), and put

$$\begin{aligned} P &= \operatorname{Im} L_+(-1, n+m), \\ N &= \left\lfloor \operatorname{Re}\left(\alpha^{-1}\left(\frac{z}{P} - \beta\right)\right)\right\rceil, \\ D_{\pi(\beta+\alpha\mathbf{Z})}(z, n) &= \min\bigl\{A_+\bigl(z - P(\beta + \alpha(N+k)), n+1\bigr) : k \in \{-1, 0, 1\}\bigr\}. \end{aligned}$$

Write $N' = \bigl\lfloor \operatorname{Re}\bigl(\alpha^{-1}\bigl(\frac{z}{\pi} - \beta\bigr)\bigr)\bigr\rceil$ so that $\operatorname{dist}\bigl(z, \pi(\beta + \alpha\mathbf{Z})\bigr) = |z - \pi(\beta + \alpha N')|$. Since $|P - \pi| \le 2^{-(n+m)}$, we have

$$\left|\operatorname{Re}\left(\alpha^{-1}\left(\frac{z}{P} - \beta\right)\right) - \operatorname{Re}\left(\alpha^{-1}\left(\frac{z}{\pi} - \beta\right)\right)\right| = \left|\operatorname{Re}\frac{(P-\pi)z}{\alpha\pi P}\right| \le 1$$

as long as $2^c|\alpha|\pi^2 \ge 1$ or so. Thus, $N - N' \in \{-1, 0, 1\}$. Moreover, for $k \in \{-1, 0, 1\}$,

$$\bigl|\beta + \alpha(N+k)\bigr| \le |\beta| + |\alpha|\left(\left|\alpha^{-1}\left(\frac{z}{\pi} - \beta\right)\right| + \frac{5}{2}\right) \le 2|\beta| + \frac{5}{2}|\alpha| + \left|\frac{z}{\pi}\right| \le 2^{m-1}$$

assuming $2^{c-2} \ge 2|\beta| + \frac{5}{2}|\alpha|$, hence

$$\begin{aligned} \bigl|A_+\bigl(z - P(\beta + \alpha(N+k)), n+1\bigr) - |z - \pi(\beta + \alpha(N+k))|\bigr| \\ \le 2^{-(n+1)} + |P - \pi|\bigl|\beta + \alpha(N+k)\bigr| \\ \le 2^{-(n+1)} + 2^{-(n+m)}2^{m-1} = 2^{-n}. \end{aligned}$$

Consequently, $\bigl|\operatorname{dist}(z, \pi(\beta + \alpha\mathbf{Z})) - D_{\pi(\beta+\alpha\mathbf{Z})}(z, n)\bigr| \le 2^{-n}$.

The argument for $\operatorname{dist}(z, \pi\alpha\mathbf{Z}_{\ne 0})$ is similar. □

f	additive parameter	multiplicative parameter
sinh	$\lvert\operatorname{Re} z\rvert \le r$	$z \notin i\mathbf{Q}$ or $D_{\pi i\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$
sin	$\lvert\operatorname{Im} z\rvert \le r$	$z \notin \mathbf{Q}$ or $D_{\pi\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$
cosh	$\lvert\operatorname{Re} z\rvert \le r$	$z \notin i\mathbf{Q}$ or $D_{\pi i(\frac12+\mathbf{Z})}(z, r+1) \ge 2^{-r}$
cos	$\lvert\operatorname{Im} z\rvert \le r$	$z \notin \mathbf{Q}$ or $D_{\pi(\frac12+\mathbf{Z})}(z, r+1) \ge 2^{-r}$
tanh	$z \notin i\mathbf{Q}$ or $D_{\pi i(\frac12+\mathbf{Z})}(z, r+1) \ge 2^{-r}$	$z \notin i\mathbf{Q}$ or $D_{\frac{\pi}{2} i\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$
tan	$z \notin \mathbf{Q}$ or $D_{\pi(\frac12+\mathbf{Z})}(z, r+1) \ge 2^{-r}$	$z \notin \mathbf{Q}$ or $D_{\frac{\pi}{2}\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$
coth	$z \notin i\mathbf{Q}$ or $D_{\pi i\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$	$z \notin i\mathbf{Q}$ or $D_{\frac{\pi}{2} i\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$
cot	$z \notin \mathbf{Q}$ or $D_{\pi\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$	$z \notin \mathbf{Q}$ or $D_{\frac{\pi}{2}\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$
sech	$z \notin i\mathbf{Q}$ or $D_{\pi i(\frac12+\mathbf{Z})}(z, r+1) \ge 2^{-r}$	$\lvert\operatorname{Re} z\rvert \le r$
sec	$z \notin \mathbf{Q}$ or $D_{\pi(\frac12+\mathbf{Z})}(z, r+1) \ge 2^{-r}$	$\lvert\operatorname{Im} z\rvert \le r$
csch	$z \notin i\mathbf{Q}$ or $D_{\pi i\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$	$\lvert\operatorname{Re} z\rvert \le r$
csc	$z \notin \mathbf{Q}$ or $D_{\pi\mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$	$\lvert\operatorname{Im} z\rvert \le r$

Table 2: TC^0 approximation of hyperbolic and trigonometric functions

The reader may wonder why here and below, we work with the distance of z to *nonzero* integer multiples of π (πi, $\pi/2$, ...) rather than *all* integer multiplies. The reason is simply that the distance to the zero multiple is trivial to estimate, being $|z|$, thus we do not need a parameter to bound it. In the same vein, if we are given a $z \in \mathbf{Q}(i) \smallsetminus \mathbf{Q}$, a suitable lower bound on $\operatorname{dist}(z, \pi\mathbf{Z})$ is given by $|\operatorname{Im} z|$; thus, we only need a parameter to bound $\operatorname{dist}(z, \pi\mathbf{Z})$ when $z \in \mathbf{Q}$ (similarly for other configurations such as $\pi i\mathbf{Z}$). However, the actual arguments below are a bit more complicated, as we really need to bound values of $f(z)$ rather than the distance of z to zeros or poles of f. Let us also consider that a priori it is possible that $\pi \in \mathbf{Q}$ (we will discuss this in more detail below).

Proposition 5.11 *If f is any of the 12 functions from Definition 5.1, then f has an additive* TC^0 *approximation $F_+(z, r, n)$ and a multiplicative* TC^0 *approximation $F_\times(z, r, n)$, parametrized by $r \in \mathbf{L}$ that satisfies the conditions specified in Table 2 (the parameter of $F_\times$ is subject to conditions from both the additive and multiplicative columns). The additive approximation is defined for all $z \in \mathbf{Q}(i) \cap \operatorname{dom}(f)$, while the multiplicative approximation excludes $z \ne 0$ such that $f(z) = 0$, if any.*

Proof: An additive approximation of $\sinh z$ is given by $\frac12\bigl(E_+(z, r, n) - E_+(-z, r, n)\bigr)$. We can construct a multiplicative approximation using Lemma 2.2—it suffices to bound $\sinh z$ away from 0 by a TC^0 function of $z = x + iy$ and r. If, say, $|x| \ge \frac{1}{4}$, then

$$|\sinh z| \ge \frac{\bigl||e^z| - |e^{-z}|\bigr|}{2} = \frac{e^{|x|} - e^{-|x|}}{2} \ge \frac{e^{1/4} - e^{-1/4}}{2} > 0.$$

Write $y = \pi N + y_0$ and $z = \pi i N + z_0$, where $N \in \mathbf{Z}$ and $|y_0| \le \frac{\pi}{2}$. (Note that we cannot directly compute N, y_0, or z_0.) We have

$$|\operatorname{Im} \sinh z| = \frac{e^x + e^{-x}}{2} \sin|y_0| \ge \sin|y_0|.$$

Since $\sin t = \operatorname{Im} e^{it}$ is increasing on $\bigl[0, \frac{\pi}{2}\bigr]$ by Theorem 3.1 (viii), $|\operatorname{Im} \sinh z| \ge \sin \frac{1}{4} > 0$ if, say, $|y_0| \ge \frac{1}{4}$.

In the remaining case, we have $|z_0| = \operatorname{dist}(z, \pi i \mathbf{Z}) \le \frac{1}{2}$. Theorem 3.1 (ix) easily implies $|\sinh z_0 - z_0| \le |z_0|^2$, thus $|\sinh z| = |\sinh z_0| \ge \frac{1}{2}|z_0|$. Now, if $x \ne 0$, then $|z_0| \ge |x| > 0$, while if $x = 0$ and $N = 0$, then $|z_0| = |y| > 0$ (unless $z = 0$, in which case $\sinh z = 0$). Finally, if $x = 0$ and $N \ne 0$, then our assumption $D_{\pi i \mathbf{Z}_{\ne 0}}(z, r+1) \ge 2^{-r}$ on the parameter r implies $|z_0| \ge 2^{-(r+1)}$. Thus, all in all, if $z \ne 0$, we can lower bound $|\sinh z|$ by a constant or one of $\frac{1}{2}|x|$, $\frac{1}{2}|y|$, or $2^{-(r+2)}$.

The arguments for sin, cosh, and cos are similar.

In view of Lemma 2.3 (iii), the reciprocal of a suitable multiplicative approximation of $\cosh z$ gives a multiplicative approximation of $\operatorname{sech} z$; by Lemma 2.2, this also gives an additive approximation with the same parametrization. For additive approximation, we can get rid of the $|\operatorname{Re} z| \le r$ condition on r by observing that if $|\operatorname{Re} z| \ge n$ (including the case $\operatorname{Re} z \notin \mathbf{R}_\mathbf{L}$), then $|\operatorname{sech} z| \le 2^{-n}$, hence we can take 0 for the approximation; otherwise, we can use the original approximation with $\max\{r, n\}$ in place of r. A similar argument applies to sec, csch, and csc.

A multiplicative approximation of $\tanh z$ can be computed by dividing multiplicative approximations of $\sinh z$ and $\cosh z$. We get rid of the $|\operatorname{Re} z| \le r$ condition in the same way as for sech: if $|\operatorname{Re} z| \le n$, we proceed with $\max\{r, n\}$ in place of r, otherwise $\operatorname{sgn} \operatorname{Re} z$ can serve as approximation (since this is ± 1 rather than 0, it works as a multiplicative approximation as well as additive, unlike the case of sech). For additive approximation, we can relax the condition on r near $\pi i \mathbf{Z}$: if $D_{\pi i \mathbf{Z}}(z, n+2) \le 2^{-(n+1)}$, then $|\tanh z| \le 2^{-n}$, hence we can approximate it with 0; otherwise, we can proceed with $\max\{r, n+1\}$ in place of r. Thus, for $z \in i\mathbf{Q}$, we only need to assume $D_{\pi i (\frac{1}{2} + \mathbf{Z})}(z, r+1) \ge 2^{-r}$ rather than $D_{\frac{\pi}{2} i \mathbf{Z}}(z, r+1) \ge 2^{-r}$. Again, the arguments for tan, coth, and cot are analogous. $\square$

In the standard model, the picture becomes much simpler: multiplicative approximations are defined on full domains as $f(z) = 0$ with $z \ne 0$ is impossible (i.e., π is irrational and $\mathbf{L} = \mathbf{N}$), and more importantly, we do not need the $D_{\dots}(z, r+1) \ge 2^{-r}$ conditions on the parameters, as we can *compute* $r \in \mathbf{L}$ with these properties from z alone. The reason is that π has a finite *irrationality measure*: i.e., there is a constant μ such that

$$\left| \frac{p}{q} - \pi \right| \ge \frac{1}{q^\mu}$$

for all but finitely many pairs $\langle p,q\rangle \in \mathbb{Z}^2_{>0}$, which ensures that

$$\operatorname{dist}\left(\frac{p}{q},\pi\mathbb{Z}_{\neq 0}\right) = N\left|\frac{p}{qN}-\pi\right| \geq \frac{N}{(qN)^\mu} \approx \frac{1}{q}\left(\frac{\pi}{p}\right)^{\mu-1},$$

where $N \in \mathbb{Z}_{>0}$ is the integer closest to $p/(q\pi)$. This was originally proved by Mahler [15]; the current best bound $\mu \leq 7.1032\dots$ is due to Zeilberger and Zudilin [27]. We do not know whether VTC^0 can prove that π has a finite irrationality measure, or even the simpler and more fundamental property that π is irrational.

In fact, it turns out that the latter seemingly weaker property would be sufficient. First, observe that in the argument above, we do not quite need the finiteness of the irrationality measure: it would be enough if π has a finite "quasipolynomial irrationality measure", i.e., a constant ν such that

$$\left|\frac{p}{q}-\pi\right| = \Omega\big(2^{-(\log q)^\nu}\big).$$

Below, "VTC^0 proves …" means, more precisely, "… holds for all models of VTC^0".

Proposition 5.12 *If* VTC^0 *proves that* $\pi \notin \mathbf{Q}$*, then there is a constant* ν *such that* VTC^0 *proves*

$$\forall p,q \in \mathbf{Z}_{\geq 2}\ \left|\frac{p}{q}-\pi\right| \geq 2^{-\|q\|^\nu},$$

and consequently, that there is a TC^0*-computable lower bound on* $\operatorname{dist}(z,\pi\mathbf{Z}_{\neq 0})$.

Proof: The irrationality of π is equivalent to

$$\forall p,q \in \mathbf{Z}_{>0}\ \exists n \in \mathbf{L}\ \left|\frac{p}{q}-P(n)\right| \geq 2^{1-n},$$

where $P(n) = \operatorname{Im} L_+(-1,n)$ is an additive TC^0 approximation of π. This is a $\forall\exists\Sigma^B_0$ statement in the language of VTC^0, thus if it is provable in VTC^0, then VTC^0 proves

$$\forall p,q \in \mathbf{Z}_{>0}\ \exists n \leq \big(\|p\|+\|q\|\big)^c\ \left|\frac{p}{q}-P(n)\right| \geq 2^{1-n}$$

for some constant c by Parikh's theorem, which implies

$$\forall p,q \in \mathbf{Z}_{>0}\ \left|\frac{p}{q}-\pi\right| \geq 2^{-(\|p\|+\|q\|)^c}.$$

Now, if $p \geq 4q$, then $\left|\frac{p}{q}-\pi\right| \geq 4-\pi \geq \frac{1}{2}$; otherwise, $\|p\| \leq \|q\|+2$. This allows the bound to be restated in terms of q alone, using a possibly larger constant $\nu > c$. □

Question 5.13 *Does* VTC^0 *prove that* π *is irrational?*

There are some fairly elementary proofs of the irrationality of π, in particular the proof of Niven [17]. This proof can be formalized in $\mathsf{I\Delta_0}+\mathsf{EXP}$ with no difficulty, but it essentially relies on the totality of exponentiation, and it is unclear how to prove the result in any weaker theory.

We observe that VTC^0 easily proves that *some* reals are irrational: e.g., the irrationality of $\sqrt{2} \in \mathbf{R}$ follows in the usual way from the fact that any $u \in \mathbf{N}$ can be written uniquely as $2^n v$ with $n \in \mathbf{L}$ and odd $v \in \mathbf{N}$.

6 Conclusion

Even though it has taken us some effort, we have successfully formalized in VTC^0 the construction of complex exp and log as well as other elementary analytic functions, and we have shown that they share basic properties enjoyed by the prototypes of these functions in the real world, adjusted in expected ways to an environment where integer exponentiation is not necessarily total. We also managed to extend the definition of iterated multiplication to Gaussian rationals. We may consider these results as further evidence that VTC^0 is a robust and somewhat unexpectedly powerful theory.

This is not to say that no problems remain. We already identified one missing fundamental piece of the puzzle, namely Question 5.13: can VTC^0 prove that π is irrational? In view of Proposition 5.12, this is really asking for a feasible proof that π has a certain Diophantine inapproximability property a little weaker than finiteness of irrationality measure.

This paper is a modest start of investigation of analytic functions in models of VTC^0, and it opens various possibilities of how it could be extended. We treated the elementary analytic functions which are an important but small group of functions; there are many other functions of interest ("special functions") that might deserve similar attention, such as $\Gamma(z)$, $\zeta(z)$, Bessel functions, the error function, elliptic functions, etc. [1, 18]. An intriguing problem is whether we can formulate in VTC^0 some form of a general theory of analytic functions, i.e., basic results of complex analysis. Can VTC^0 understand differentiation and integration (or even simple differential equations such as Pfaffian chains)? We leave these open-ended questions for possible future work.

Acknowledgements

I am grateful to the anonymous referees for many helpful suggestions to improve the presentation of the paper.

The research was supported by the Czech Academy of Sciences (RVO 67985840) and GA ČR project 23-04825S.

A Detailed construction of TC^0 approximations

Here are the full proofs of Lemmas 3.46 and 3.57.

Lemma A.1 *We can construct* TC^0 *functions* $E_{\mathbf{C_L}}(z,r,n)$, $SR_{\mathbf{R}}(x,n)$, $A_\times(z,n)$, $A_+(z,n)$, $SR_{\mathbf{C}}(z,n)$, $L_D(z,r,n)$, $L_{\mathbf{R}}(x,n)$, $L_{\mathbf{C}}(z,n)$, $LE(z,r,n)$, $E_\times(z,r,n)$, *and* $E_+(z,r,n)$ *with the following properties.*

(i) $\mathrm{E}_{\mathbf{C_L}}(z,r,n)$ *is a multiplicative approximation of* $\exp_{\mathbf{C_L}} z$ *for* $z \in \mathbf{Q_L}(i)$, *parametrized by* $r \in \mathbf{L}$ *such that* $|z| \le r$.

(ii) $SR_{\mathbf{R}}(x,n)$ *is a multiplicative approximation of* $\sqrt{x}$ *for* $x \in \mathbf{Q}_{>0}$.

(iii) $A_\times(z,n)$ *and* $A_+(z,n)$ *are multiplicative and additive (respectively) approximations of* $|z| \in \mathbf{R}$ *for* $z \in \mathbf{Q}(i)$.

(iv) $SR_{\mathbf{C}}(z,n)$ *is a multiplicative approximation of* $\sqrt{z}$ *for* $z \in \mathbf{Q}(i) \smallsetminus \{0\}$.

(v) $L_D(z,r,n)$ *is an additive approximation of* $\log_D z$ *for* $z \in D_1^*(1) \cap \mathbf{Q}(i)$, *parametrized by* $r \in \mathbf{L}$ *such that* $|z-1| \le 1 - r^{-1}$.

(vi) $L_{\mathbf{R}}(x,n)$ *is an additive approximation of* $\log_{\mathbf{R}} x$ *for* $x \in \mathbf{Q}_{>0}$.

(vii) $L_{\mathbf{C}}(z,n)$ *is an additive approximation of* $\log_{\mathbf{C}} z$ *for* $z \in \mathbf{Q}(i) \smallsetminus \{0\}$.

(viii) $LE(z,r,n)$ *is an additive approximation of* $\log_{\mathbf{C}} \exp_{\mathbf{C_L}} z$ *for* $z \in \mathbf{Q_L}(i)$ *with* $|\operatorname{Im} z| < 1$, *parametrized by* $r \in \mathbf{L}$ *such that* $|z| \le r$.

(ix) $E_\times(z,r,n)$ *is a multiplicative approximation of* $\exp z$ *for* $z \in \mathbf{Q_L} + i\mathbf{Q}$, *parametrized by* $r \in \mathbf{L}$ *such that* $|\operatorname{Re} z| \le r$.

(x) $E_+(z,r,n)$ *is an additive approximation of* $\exp z$ *for* $z \in \mathbf{Q}_{\downarrow\mathbf{L}} + i\mathbf{Q}$, *parametrized by* $r \in \mathbf{L}$ *such that* $\operatorname{Re} z \le r$.

Proof:

(i): We know that $\bigl|e(z,\max\{8r,n\}) - \exp z\bigr| \le 2^{-n}$ from the proof of Lemma 3.5, hence

$$\left|\frac{e(z,\max\{8r,n\})}{\exp z} - 1\right| \le 2^{-n}|\exp(-z)| \le 2^{-n}\exp r$$

using Lemmas 3.6 and 3.8. Thus, the crude bound

$$\exp r \le 2^{-8r} + e(r,8r) \le 2^{-8r} + \sum_{j<8r} r^j \le r^{8r} \le 2^{8r^2}$$

shows that it suffices to take $E_{\mathbf{C_L}}(z,r,n) = e(z, n+8r^2)$.

(ii): In view of [8, Thm. 6.8], the existence of $SR_{\mathbf{R}}$ is a consequence of [8, Prop. 3.7]. An explicit description can be given as follows. Let $x \in \mathbf{Q}_{>0}$. Similarly to the proof of Lemma 2.2, we can compute $m \in \mathbf{Z_L}$ (in unary) such that $\frac{2}{5} \le 2^{-2m}x \le \frac{8}{5}$ by a TC^0 function. Putting $u = 1 - 2^{-2m}x$, we apply [8, Thm. 5.5] to the polynomial $h(y) = -y^2 + y - \frac{u}{4}$ (writing y instead of x for the indeterminate to avoid clash with our x), whose root is $y = \frac{1}{2}\bigl(1 - \sqrt{1-u}\bigr)$, i.e., $\sqrt{x} = 2^m(1-2y)$. Let α, b_j, and y_N be as in [8, Thm. 5.5]. Since $\alpha = |u| \le \frac{3}{5}$, we obtain

$$|y - y_N| \le \frac{5}{2}\left(\frac{3}{5}\right)^N,$$

where

$$y_N = \sum_{j=1}^N b_j \left(\frac{u}{4}\right)^N = \sum_{j=1}^N \binom{2(j-1)}{j-1}\frac{1}{j}\left(\frac{u}{4}\right)^j.$$

Since $(1-2y)^2 \ge \frac{2}{5}$, we have $|1-2y| \ge \frac{5}{8}$, hence

$$\left|\frac{2^m(1-2y_N)}{\sqrt{x}} - 1\right| = \left|\frac{2(y-y_N)}{1-2y}\right| \le 8\left(\frac{3}{5}\right)^N.$$

Thus, we may take $SR_{\mathbf{R}}(x,n) = 2^m(1-2y_{2(n+3)})$.

(iii): We can put $A_\times(z,n) = SR_{\mathbf{R}}(x^2+y^2,n)$ and $A_+(z,n) = A_\times(z,n+m)$, where $z = x+iy$, and $m \in \mathbf{L}$ is such that $2^m \geq |x|+|y|$.

(iv): Write $z = x+iy$, and assume first $x \geq 0$. Note that

$$\sqrt{z} = \sqrt{\frac{|z|+x}{2}} + i\frac{y}{2\sqrt{\frac{|z|+x}{2}}}$$

as $y = \operatorname{Im}\bigl((\sqrt{z})^2\bigr) = 2\operatorname{Re}\sqrt{z}\operatorname{Im}\sqrt{z}$. Put

$$\begin{aligned} r &= A_\times(z,n+1), \\ u &= SR_{\mathbf{R}}\bigl(\tfrac{1}{2}(r+x),n+1\bigr), \\ SR_{\mathbf{C}}(z,n) &= u + i\frac{y}{2u}. \end{aligned}$$

We have

$$\left|\frac{\frac{1}{2}(r+x)}{\frac{1}{2}(|z|+x)} - 1\right| = \left|\frac{r-|z|}{|z|+x}\right| = \frac{|z|}{|z|+x}\left|\frac{r}{|z|}-1\right| \leq 2^{-(n+1)}.$$

Put $n' = n+2$ and $\varepsilon = 2^{-n'} + 2^{-2n'}$. Since

$$2\varepsilon - \varepsilon^2 = 2\cdot 2^{-n'} + 2^{-2n'} - 2\cdot 2^{-3n'} - 2^{-4n'} \geq 2\cdot 2^{-n'} = 2^{-(n+1)},$$

Lemma 2.3 implies

$$\begin{aligned} &\left|\frac{\sqrt{\frac{1}{2}(r+x)}}{\sqrt{\frac{1}{2}(|z|+x)}} - 1\right| \leq \varepsilon, \\ &\left|\frac{u}{\sqrt{\frac{1}{2}(|z|+x)}} - 1\right| \leq 2^{-(n+1)} + \varepsilon + 2^{-(n+1)}\varepsilon \\ &\qquad = 3\cdot 2^{-n'} + 3\cdot 2^{-2n'} + 2\cdot 2^{-3n'} \leq 4\cdot 2^{-n'} = 2^{-n}. \end{aligned}$$

If $y = 0$, we are done. Otherwise,

$$(1+2^{-n})(3\cdot 2^{-n'} + 3\cdot 2^{-2n'} + 2\cdot 2^{-3n'}) = 3\cdot 2^{-n'} + 15\cdot 2^{-2n'} + 14\cdot 2^{-3n'} + 8\cdot 2^{-4n'} \leq 2^{-n}$$

as long as $n' \geq 4$, i.e., $n \geq 2$; thus,

$$\left|\frac{y/2u}{y\Big/2\sqrt{\frac{1}{2}(|z|+x)}} - 1\right| = \left|\frac{\sqrt{\frac{1}{2}(|z|+x)}}{u} - 1\right| \leq 2^{-n}$$

by Lemma 2.3 (iii), and

$$\left|\frac{SR_{\mathbf{C}}(z,n)}{\sqrt{z}} - 1\right| \leq 2^{-n}$$

by Lemma 2.3 (iv).

If $\operatorname{Re} z < 0$, we may take $SR_{\mathbf{C}}(z,n) = iSR_{\mathbf{C}}(-z,n)\operatorname{sgn}^+ y$.

(v): By the proof of Lemma 3.14, $L_D(z,r,n) = -\lambda(1-z,nr)$ works.

(vi): Given $x \in \mathbf{Q}_{>0}$, we can compute $m \in \mathbf{Z}_{\mathbf{L}}$ such that $2^m \geq x > 2^{m-1}$ as in (ii). Put $x' = 2^{-m}x \in \left(\frac{1}{2}, 1\right]$, so that

$$\log_{\mathbf{R}} x = \log_D x' + m\ell_2 = \log_D x' - m\log_D \tfrac{1}{2}.$$

Thus, it suffices to take $L_{\mathbf{R}}(x,n) = L_D(x',2,n+1) - mL_D\left(\frac{1}{2},2,n+|m|\right)$.

(vii): Let $z \in \mathbf{Q}(i) \smallsetminus \{0\}$. We have

$$\log_{\mathbf{C}} z = 8\log_S \sqrt[8]{z} = 8\log_{\mathbf{R}}\left|\sqrt[8]{z}\right| + 8\log_D \operatorname{sgn}\sqrt[8]{z}.$$

Put $z_1 = SR_{\mathbf{C}}(z,n+7)$, $z_2 = SR_{\mathbf{C}}(z_1,n+7)$, $z_3 = SR_{\mathbf{C}}(z_2,n+7)$, $x = SR_{\mathbf{R}}(z_3\overline{z_3},n+7)$, $w = z_3/x$, and

$$L_{\mathbf{C}}(z,n) = 8L_{\mathbf{R}}(x,n+5) + 8L_D(w,2,n+5).$$

Write $n' = n+7$, $\varepsilon = 2^{-n'} + 4\cdot 2^{-2n'}$, and $\delta = 2\cdot 2^{-n'} + 6\cdot 2^{-2n'}$. Notice that

$$2^{-n'} + \varepsilon + 2^{-n'}\varepsilon = 2\cdot 2^{-n'} + 5\cdot 2^{-2n'} + 4\cdot 2^{-3n'} \leq \delta$$

and

$$2\varepsilon - \varepsilon^2 = 2\cdot 2^{-n'} + 7\cdot 2^{-2n'} - 8\cdot 2^{-3n'} - 16\cdot 2^{-4n'} \geq \delta.$$

Thus, using Lemma 2.3,

$$\left|\frac{z_1}{\sqrt{z}} - 1\right| \leq 2^{-n'} \leq \delta \leq 2\varepsilon - \varepsilon^2$$

implies

$$\left|\frac{\sqrt{z_1}}{\sqrt[4]{z}} - 1\right| \leq \varepsilon,$$

whence

$$\left|\frac{z_2}{\sqrt[4]{z}} - 1\right| \leq 2^{-n'} + \varepsilon + 2^{-n'}\varepsilon \leq \delta.$$

Repeating the same argument, we obtain

$$\left|\frac{z_3}{\sqrt[8]{z}} - 1\right| \leq \delta.$$

Using $\big||z| - 1\big| \leq |z-1|$ and Lemma 2.3, we get

$$\left|\frac{x}{|\sqrt[8]{z}|} - 1\right| \leq 2^{-n'} + \delta + 2^{-n'}\delta \leq 3\cdot 2^{-n'} + 9\cdot 2^{-2n'},$$

hence

$$\begin{aligned}\left|\log_{\mathbf{R}} x - \log_{\mathbf{R}}|\sqrt[8]{z}|\right| &= \left|\log_{\mathbf{R}}\left(x/|\sqrt[8]{z}|\right)\right| \\ &\leq 3\cdot 2^{-n'} + 9\cdot 2^{-2n'} + (3\cdot 2^{-n'} + 9\cdot 2^{-2n'})^2 \\ &\leq 4\cdot 2^{-n'} = 2^{-n-5}\end{aligned}$$

using Lemmas 3.23 and 3.19 (eq. (3)), thus

$$\bigl|L_{\mathbf{R}}(x,n+5)-\log_{\mathbf{R}}|\sqrt[8]{z}|\bigr|\le 2^{-n-4}.$$

Using similar arguments, we obtain $\bigl|w/\operatorname{sgn} z_3-1\bigr|\le 2^{-n'}+O(2^{-2n'})$, $\bigl|w/\operatorname{sgn}\sqrt[8]{z}-1\bigr|\le 3\cdot 2^{-n'}+O(2^{-2n'})$ (which implies $|w-1|\le\frac{1}{2}$ as $|\operatorname{sgn}\sqrt[8]{z}-1|\le 0.41$ using Lemma 3.29 and the proof of Lemma 3.26 (i)), and $\bigl|\log_D w-\log_D\operatorname{sgn}\sqrt[8]{z}\bigr|\le 3\cdot 2^{-n'}+O(2^{-2n'})\le 2^{-n-5}$, whence

$$\bigl|L_D(w,2,n+5)-\log_D\operatorname{sgn}\sqrt[8]{z}\bigr|\le 2^{-n-4},$$

which implies $|L_{\mathbf{C}}(z,n)-\log_{\mathbf{C}} z|\le 8(2^{-n-4}+2^{-n-4})=2^{-n}$.

(viii): We put $LE(z,r,n)=L_{\mathbf{C}}\bigl(E_{\mathbf{C_L}}(z,r,n+2),n+1\bigr)$. By (i), we have

$$E_{\mathbf{C_L}}(z,r,n+2)=(1+w)\exp z$$

for some w such that $|w|\le 2^{-(n+2)}$. We have $\operatorname{Re}\exp z>0$ by Lemma 3.45, and trivially $\operatorname{Re}(1+w)>0$, thus

$$\bigl|\log_{\mathbf{C}} E_{\mathbf{C_L}}(z,r,n+2)-\log_{\mathbf{C}}\exp z\bigr|=|\log_D(1+w)|\le 2^{-(n+2)}+2^{-2(n+2)}\le 2^{-(n+1)}$$

by Lemmas 3.37, 3.36, and 3.19 (eq. (3)), while

$$\bigl|LE(z,r,n)-\log_{\mathbf{C}} E_{\mathbf{C_L}}(z,r,n+2)\bigr|\le 2^{-(n+1)}$$

by (vii).

(ix): We compute $m\in\mathbf{L}$ such that $m\ge 3$ and $2^m\ge|\operatorname{Im} z|$, and put

$$\begin{aligned}P&=\operatorname{Im} L_{\mathbf{C}}(-1,n+m+1),\\ N&=\left\lfloor\frac{\operatorname{Im} z}{2P}\right\rceil,\\ E_\times(z,r,n)&=E_{\mathbf{C_L}}(z-2PNi,r+4,n+2).\end{aligned}$$

Put $w=z-2PNi$. We have $|\pi-P|\le 2^{-n-m-1}$ by (vii), thus $|\operatorname{Im} w|\le P\le 4$ using Proposition 3.44, and $|w|\le r+4$. Consequently,

$$\left|\frac{E_\times(z,r,n)}{\exp w}-1\right|\le 2^{-n-2}$$

by (i). Moreover,

$$\bigl|2(\pi-P)N\bigr|\le 2^{-n-m}\left(\frac{|\operatorname{Im} z|}{2P}+\frac{1}{2}\right)\le 2^{-n-m}\frac{2^m}{4}=2^{-n-2}$$

using Proposition 3.44, hence

$$\begin{aligned}\left|\frac{\exp w}{\exp z}-1\right|&=\bigl|\exp(-2PNi)-1\bigr|=\bigl|\exp_{\mathbf{C_L}}\bigl(2(\pi-P)Ni\bigr)-1\bigr|\\ &\le\bigl|2(\pi-P)N\bigr|+\bigl|2(\pi-P)N\bigr|^2\le 2^{-n-1}\end{aligned}$$

using Lemma 3.10 (iv), and

$$\left|\frac{E_\times(z,r,n)}{\exp z}-1\right| \le 2^{-n-1}+2^{-n-2}+2^{-2n-3} \le 2^{-n}$$

by Lemma 2.3 (i).

(x): We put

$$E_+(z,r,n)=\begin{cases} E_\times\bigl(z,\max\{n,r\},n+2r\bigr) & \text{if } -n\le \operatorname{Re} z\le r,\\ 0 & \text{otherwise.}\end{cases}$$

If $\operatorname{Re} z \le -n$, we have

$$|\exp z| = \exp \operatorname{Re} z \le \exp(-n) \le 2^{-n}$$

by Lemmas 3.10 and 3.54 (this bound holds trivially if $\operatorname{Re} z \notin \mathbf{R_L}$). If $-n \le \operatorname{Re} z \le r$, (ix) gives

$$\bigl|E_\times\bigl(z,\max\{n,r\},n+2r\bigr)-\exp z\bigr| \le 2^{-n-2r}|\exp z| \le 2^{-n-2r}\exp r \le 2^{-n}$$

using Lemmas 3.10 and 3.54 again. □

References

[1] Milton Abramowitz and Irene A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, Dover Publications, New York, 1972.

[2] David A. Mix Barrington, Neil Immerman, and Howard Straubing, *On uniformity within NC^1*, Journal of Computer and System Sciences 41 (1990), no. 3, pp. 274–306.

[3] Robert L. Constable, *Type two computational complexity*, in: Proceedings of the fifth Annual ACM Symposium on Theory of Computing, 1973, pp. 108–121.

[4] Stephen A. Cook and Phuong Nguyen, *Logical foundations of proof complexity*, Perspectives in Logic, Cambridge University Press, New York, 2010.

[5] Antonio J. Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer, 2005.

[6] András Hajnal, Wolfgang Maass, Pavel Pudlák, Márió Szegedy, and György Turán, *Threshold circuits of bounded depth*, Journal of Computer and System Sciences 46 (1993), no. 2, pp. 129–154.

[7] William Hesse, Eric Allender, and David A. Mix Barrington, *Uniform constant-depth threshold circuits for division and iterated multiplication*, Journal of Computer and System Sciences 65 (2002), no. 4, pp. 695–716.

[8] Emil Jeřábek, *Open induction in a bounded arithmetic for* TC^0, Archive for Mathematical Logic 54 (2015), no. 3–4, pp. 359–394.

[9] ———, *Iterated multiplication in VTC^0*, Archive for Mathematical Logic 61 (2022), no. 5–6, pp. 705–767.

[10] ———, *Models of* VTC^0 *as exponential integer parts*, arXiv:2209.01197 [math.LO], 2022, `https://arxiv.org/abs/2209.01197`.

[11] Jan Johannsen, *Weak bounded arithmetic, the Diffie-Hellman problem, and Constable's class K*, in: Proceedings of the 14th Annual IEEE Symposium on Logic in Computer Science, 1999, pp. 268–274.

[12] Jan Johannsen and Chris Pollett, *On proofs about threshold circuits and counting hierarchies (extended abstract)*, in: Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science, 1998, pp. 444–452.

[13] ———, *On the Δ^b_1-bit-comprehension rule*, in: Logic Colloquium '98: Proceedings of the 1998 ASL European Summer Meeting held in Prague, Czech Republic (S. R. Buss, P. Hájek, and P. Pudlák, eds.), ASL, 2000, pp. 262–280.

[14] Alexis Maciel and Denis Thérien, *Efficient threshold circuits for power series*, Information and Computation 152 (1999), no. 1, pp. 62–73.

[15] Kurt Mahler, *On the approximation of π*, Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen, Series A: Mathematical Sciences 56 (1953), no. 1, pp. 30–42.

[16] Phuong Nguyen and Stephen A. Cook, *Theories for TC^0 and other small complexity classes*, Logical Methods in Computer Science 2 (2006), no. 1, article no. 3, 39 pp.

[17] Ivan Niven, *A simple proof that π is irrational*, Bulletin of the Americal Mathematical Society 53 (1947), no. 6, p. 509.

[18] Frank W. J. Olver, Daniel W. Lozier, Ronald F. Boisvert, and Charles W. Clark (eds.), *NIST handbook of mathematical functions*, Cambridge University Press, Cambridge, 2010.

[19] Ian Parberry and Georg Schnitger, *Parallel computation with threshold functions*, Journal of Computer and System Sciences 36 (1988), no. 3, pp. 278–302.

[20] John H. Reif, *Logarithmic depth circuits for algebraic functions*, SIAM Journal on Computing 15 (1986), no. 1, pp. 231–242.

[21] John H. Reif and Stephen R. Tate, *On threshold circuits and polynomial computation*, SIAM Journal on Computing 21 (1992), no. 5, pp. 896–908.

[22] Jean-Pierre Ressayre, *Integer parts of real closed exponential fields*, in: Arithmetic, proof theory, and computational complexity (P. Clote and J. Krajíček, eds.), Oxford Logic Guides vol. 23, Oxford University Press, 1993, pp. 278–288.

[23] Dana Scott, *On completing ordered fields*, in: Applications of Model Theory to Algebra, Analysis, and Probability (W. A. J. Luxemburg, ed.), Holt, Rinehart and Winston, New York, 1969, pp. 274–278.

[24] John C. Shepherdson, *A nonstandard model for a free variable fragment of number theory*, Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques 12 (1964), no. 2, pp. 79–86.

[25] Seth Warner, *Topological fields*, North-Holland Mathematics Studies vol. 157, North-Holland, New York, 1989.

[26] Domenico Zambella, *Notes on polynomially bounded arithmetic*, Journal of Symbolic Logic 61 (1996), no. 3, pp. 942–966.

[27] Doron Zeilberger and Wadim Zudilin, *The irrationality measure of π is at most* $7.103205334137\ldots$, Moscow Journal of Combinatorics and Number Theory 9 (2020), no. 4, pp. 407–419.