# Digital Algebra and Circuits

Jean Vuillemin

Ecole Normale Supérieure, 45 rue d'Ulm, 75005 Paris France.

**Abstract.** Digital numbers $\mathbf{D}$ are the world's most popular data representation: nearly all texts, sounds and images are coded somewhere in time and space by binary sequences. The mathematical construction of the fixed-point $\mathbf{D} \simeq \mathbf{Z}_2$ and floating-point $\mathbf{D}' \simeq \mathbf{Q}_2$ digital numbers is a dual to the classical constructions of the real numbers $\mathbf{R}$.

The domain $\mathbf{D}'$ contains the binary integers $\mathbf{N}$ and $\mathbf{Z}$, as well as $\mathbf{Q}$. The arithmetic operations in $\mathbf{D}'$ are the usual ones when restricted to integers or rational numbers. Similarly, the polynomial operations in $\mathbf{D}'$ are the usual ones when applied to finite binary polynomials $\mathbf{F}_2[\mathbf{z}]$ or their quotients $\mathbf{F}_2(\mathbf{z})$. Finally, the set operations in $\mathbf{D}'$ are the usual ones over finite or infinite subsets of $\mathbf{N}$.

The resulting algebraic structure is rich, and we identify over a dozen rings, fields and Boolean algebras in $\mathbf{D}'$. Each structure is well-known in its own right. The unique nature of $\mathbf{D}'$ is to combine all into a single algebraic structure, where operations of different nature happily mix. The two's complement formula $-x = 1 + \neg x$ is an example. Digital algebra is concerned with the relations between a dozen operators. Digital synchronous circuits are built from a simple subset of these operators: three Boolean gates and the unit-delay $\mathbf{z}$.

Digital analysis is simpler and more intuitive than analysis in $\mathbf{R}$. The computable digital functions $\mathbf{D} \mapsto \mathbf{D}$ are continuous: each output bit depends upon finitely many input bits. Infinite circuits compute causal functions: present output depends upon past inputs. Sequential functions are equivalently computed by FSM and by finite circuits.

The $\nu$-transform is an infinite binary truth-table for causal functions. The $\nu$-transform provides a natural one-to-one correspondence between algebraic digital numbers and sequential functions. Questions about sequential functions are transformed by $\nu$ into questions about algebraic digital numbers, where the whole of digital algebra applies.

An algebraic digital number is finitely represented by a unique minimal regular binary tree RBT. The inverse transform of the RBT is the minimal deterministic FSM for computing the (reversed) sequential function.

An algebraic digital number is finitely represented by a unique minimal up-polynomial MUP of which it is root. The MUP is smaller than the RBT. It is exponentially smaller than the minimal deterministic FSM for a shift-register circuit.

The net-list of a circuit is transformed by $\nu$ into the isomorphic truth-list: a system of equations over algebraic numbers. Circuit examples show how the truth-list is cast to normal form - either RBT or MUP - through a sequence of simple identities from digital algebra.

*This contribution is dedicated to Zohar Manna on his 64-th birthday.*

# 1 Introduction

Let us operate a *digital* circuit and probe some internal signal $s$. The observed value is a bit $s_t \in \mathbf{B} = \{0\ \ 1\}$ at all *real* time $t \in \mathbf{R} \geq 0$. In a *digital synchronous* DS circuit, signals can only change at *integer* time: $s_t = s_n$ where $n = \lfloor t \rfloor \in \mathbf{N}$. Signal $s$ is a *digital number* $s \in \mathbf{D}$ presented by the indefinite $\mathrm{N} \in \mathbf{N}$ sequence $s = s_0 \cdots s_{\mathrm{N}} \cdots$ of bits $s_{\mathrm{N}} \in \mathbf{B}$.

## 1.1 Digital numbers

Digital numbers $\mathbf{D} \simeq \mathbf{Z}_2$ include all natural numbers $\mathbf{N}$, integers $\mathbf{Z}$ and rational numbers $\mathbf{Z}_{(2)} \simeq \mathbf{Q} \cap \mathbf{D}$ with an odd denominator. But $\frac{1}{2} \notin \mathbf{D}$ is not a digital number. The floating-point digital numbers $\mathbf{D}' = \langle \mathbf{D}, \frac{1}{2} \rangle \simeq \mathbf{Q}_2$ contain $\mathbf{D}$ and all rational numbers $\mathbf{Q}$.

Hensel invents/discovers the *p-adic* integers $\mathbf{Z}_p$ and numbers $\mathbf{Q}_p$ near 1900. Such numbers extend the arithmetic properties of $\mathbf{Z}$ and $\mathbf{Q}$ through an indefinite expansion in base $p \in \mathbf{N}{+}2$. Ostrowski's theorem [8] states that every field which extends the rational field $\langle \mathbf{Q}, , + \ - \ \times \ / \rangle$ and preserves the norm over $\mathbf{Q}$ must be isomorphic to either $\mathbf{R}$, or to $\mathbf{Q}_p$ for some prime number $p$.

The distance in $\mathbf{Q}_p$ is *ultra-metric* and the ultra-metric inequality implies the classical triangle inequality. Properties of the real numbers which are derived from the triangle inequality hold for the $p$-adic numbers, with exactly the same proof. Stronger properties often result. For example [8], an infinite sum $s = \sum s_{\mathrm{N}}$ of numbers $s_{\mathrm{N}} \in \mathbf{D}'$ converges $s \in \mathbf{D}'$ if and only if the general term goes to $0 = \lim_{\mathrm{N} \to \infty} \|s_{\mathrm{N}}\|$. The following corollary is useful.

**Lemma 1.** *The infinite sum* $s = \sum 2^{\mathrm{N}} s_{\mathrm{N}}$ *converges to a digital number* $s \in \mathbf{D}$ *for all sequences of digital numbers* $s_{\mathrm{N}} \in \mathbf{D}$.

Digital numbers support integer arithmetics: $\langle \mathbf{D}', , +, -, \otimes, / \rangle$ is isomorphic to the field $\mathbf{Q}_2$ of 2-adic numbers.

Digital numbers support binary polynomial arithmetics: $\langle \mathbf{D}', , \oplus \ \otimes \ \oslash \rangle$ is isomorphic to the field $\mathbf{F}_2(\!(\mathbf{z})\!)$ of Laurent formal power series over $\mathbf{F}_2$.

The last two structures generalize to every base $p$ where $p > 1$ is a prime number. The characteristic property of base $p = 2$ is to also support logical operations: $\langle \mathbf{D}, , \neg \ \cap \ \cup \rangle$ is a Boolean algebra isomorphic to the subsets of $\mathbf{N}$.

## 1.2 Digital synchronous circuits

The relevance of *2-adic* integers $\mathbf{Z}_2$ to computer arithmetics [9] and to DS circuits [11] has long been known. Example 1 is a point in case: the *Minus* circuit computes Hensel's opposite $y = -x$. The input $x = \sum 2^{\mathrm{N}} x_{\mathrm{N}}$ is *bit-serial*: bit $x_{\mathrm{N}}$ is presented on an input pin during cycle $\mathrm{N}$. The output $y = \sum 2^{\mathrm{N}} y_{\mathrm{N}}$ is also bit-serial. Both digital numbers are related by $x + y = 0$, where $+$ is the sum in $\mathbf{D}$. Equality $x + y = 0$ states that, for all $\mathrm{N} \in \mathbf{N}$ the sum of the two integers $x_{0 \cdots \mathrm{N}-1} = \sum_{k<\mathrm{N}} 2^k x_k$ and $y_{0 \cdots \mathrm{N}-1} = \sum_{k<\mathrm{N}} 2^k y_k$ is such that $x_{0 \cdots \mathrm{N}-1} + y_{0 \cdots \mathrm{N}-1} = 0 \pmod{2^{\mathrm{N}}}$. At all cycles, the sum is correct so far.

*Example 1 (Minus).* Let circuit $y = minus(x)$ be defined by the net-list

$$r = \mathbf{z}(x \cup r),\ y = x \oplus r.$$

The binary values $r_{\mathbf{N}}, y_{\mathbf{N}} \in \mathbf{B}$ of $r$, $y$ are computed at cycle $\mathbf{N}$ from the input bits $x_{\mathbf{N}}, x_{\mathbf{N}-1} \in \mathbf{B}$[1] by $r_{\mathbf{N}} = x_{\mathbf{N}-1} \cup r_{\mathbf{N}-1}$ and $y_{\mathbf{N}} = x_{\mathbf{N}} \oplus r_{\mathbf{N}}$. Replacing for gate definitions leads to $r_{\mathbf{N}} = x_{\mathbf{N}-1} + r_{\mathbf{N}-1} - x_{\mathbf{N}-1}r_{\mathbf{N}-1}$ and $y_{\mathbf{N}} = x_{\mathbf{N}} + r_{\mathbf{N}} - 2x_{\mathbf{N}}r_{\mathbf{N}}$, an equivalent system expressed with integer operations. Let $x = \sum 2^{\mathbf{N}} x_{\mathbf{N}}$ and $y = \sum 2^{\mathbf{N}} y_{\mathbf{N}}$ be the corresponding digital numbers, and similarly of $r$ and $p = x \cap r$. Substituting in the definitions yields $r = 2(x + r - p)$ and $y = x + r - 2p$. Subtract $y - r = x + r - 2p - 2(x + r - p)$ and simplify to find $y = -x$.

The *Minus circuit* from example 1 has three gates: one register $\mathbf{z}$ (also known as up-shift, unit-time-delay, synchronous flip-flop and times 2) and two memory-less gates $\cup$ for OR and $\oplus$ for XOR. Addition $+$ of digital numbers can similarly be computed by a finite circuit with six gates. Both products - with carries for $\times$, and without carries for $\otimes$ - can also be computed by bit-serial circuits [11]. However, both circuits are infinite!

### 1.3 Digital functions

A digital function $f \in \mathbf{D} \mapsto \mathbf{D}$ is continuous if each output bit depends upon finitely many input bits.

A digital function is *causal* $f \in \mathbf{D} \overset{c}{\to} \mathbf{D}$ if each output bit only depends upon the previous input bits. Equivalently, $f$ is represented by an *infinite binary decision tree* where each node *tests* an input bit and each edge carries an output bit. Equivalently, $f$ is computed by some infinite DS circuit [11].

The *truth table* $F = \nu f \in 4\mathbf{D}$ is the infinite binary sequence of output bits gathered by traversing the decision tree for $f \in \mathbf{D} \overset{c}{\to} \mathbf{D}$ in hierarchical order. Conversely, each table $F \in 4\mathbf{D}$ defines a unique function $f = \nu^{-}F \in \mathbf{D} \overset{c}{\to} \mathbf{D}$. The *$\nu$-transform* is (almost) a Boolean algebra isomorphism between causal functions and digital numbers.

A causal function is *sequential* if $f \in \mathbf{D} \overset{s}{\to} \mathbf{D}$ is computable by a *finite* circuit. Equivalently, $f$ is computable by a finite state machine. Equivalently, the language recognized by $f$ is *regular*. These equivalent characterizations of sequentiality are well known [7].

The classical methods for verifying *memory-less* circuits use BDDs [3]. The BDD data-structure is a *Strong Normal Form* SNF: every Boolean function in the net-list has a unique representation; testing node equality reduces to testing a pointer equality, in constant time.

The equivalent SNF for sequential circuits is the minimal deterministic Mealy mdFSM [7]. The limits come from size: the number of states in the mdFSM grows exponentially with the number of registers in the circuit.

[1] by convention $x_{-1} = r_{-1} = 0$ for negative indices

### 1.4 Algebraic digital numbers

A new characterization [4, 12] of sequential functions is provided: the $\nu$-transform of a *sequential* function $f \in \mathbf{D} \overset{s}{\to} \mathbf{D}$ is an *algebraic* digital number $\nu f \in \mathbf{A}$.

The *net-list* of a circuit is $\nu$-transformed - equation for equation - into the *truth-list*, an equivalent system of equations over digital numbers. Properties of *sequential* functions $\nu$-transform to properties of *algebraic* digital numbers.

A first SNF for algebraic numbers is provided by *regular binary trees* RBT. The RBT is closely related to the $\nu$-transform of the mdFSM for the input-reversed function. Both share the same size problem. The RBT representation which follows - since $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Z}_{(2)} \subset \mathbf{A}$ - for integers and (some) rational numbers is smaller than the usual representation by finite ultimately periodic binary sequences.

A second SNF for an algebraic number $y \in \mathbf{A}$ is provided by the *minimal* polynomial with root $y$ - plus a few bits to lock that root. A third SNF is the *minimal up-polynomial MUP* with root $y$. An up-polynomial is a special form of polynomial where squaring is the only operation available. The *up-degree* of MUP is smaller than the degree of the minimal polynomial.

The MUP of $y \in \mathbf{A}$ can be derived from the truth-list of a circuit, by equivalent rewriting through the rich algebraic properties of *field* $\mathbf{D}'$. The MUP is smaller than the RBT. The *shift-register* example shows that it can be exponentially smaller.

## 2 Digital algebra

### 2.1 Digital numbers

**Definition 1.** *A digital number $d \in \mathbf{D}$ is isomorphically represented by:*

1. *the infinite binary $\mathrm{B}^d_{\mathbf{N}} \in \mathbf{B}$ sequence $\mathrm{B}^d_{0\ldots} = \mathrm{B}^d_0 \cdot \mathrm{B}^d_{1\ldots} \in \mathbf{B}^\infty$;*
2. *the integer $d(\mathrm{N}) = d_{\mathbf{N}} = \mathrm{B}^d_{\mathbf{N}}$ predicate $d() \in \mathbf{N} \mapsto \mathbf{B}$;*
3. *the set $d\{\} = \{\mathrm{N} :\ 1 = d_{\mathbf{N}}\}$ of natural numbers $d\{\} \in 2^{\mathbf{N}}$;*
4. *the binary $d(\mathbf{z}) = \sum \mathbf{z}^{\mathbf{N}} d_{\mathbf{N}}$ series $d(\mathbf{z}) \in \mathbf{Z}_{\mathbf{z}}$;*
5. *the 2-adic $d(2) = \sum 2^{\mathbf{N}} d_{\mathbf{N}}$ integer $d(2) \in \mathbf{Z}_2$.*

Note that the real number $d(1/2) = \sum d_{\mathbf{N}} 2^{-\mathbf{N}} \in \mathbf{R}$ is not characteristic of $d \in \mathbf{D}$. Indeed, the digital sequences $a = 1(0)^\infty$ and $b = 0(1)^\infty$ both map to the same real number $a(1/2) = b(1/2) = 1$ while $a(2) = 1$ and $b(2) = -2$ are different.

The infinite binary representation of a natural number $\mathbf{N}$ is ultimately zero. For example: $7 \simeq 1110^\infty \simeq 1 + \mathbf{z} + \mathbf{z}^2 \simeq \{0, 1, 2\}$.

The infinite binary representation of an integer $\mathbf{Z}$ is ultimately constant. For example: $-4 \simeq 001^\infty \simeq \frac{\mathbf{z}^2}{1-\mathbf{z}} \simeq \{n :\ n > 1\}$.

The infinite binary representation in $\mathbf{Z}_{(2)} = \mathbf{Q} \cap \mathbf{D}$ is ultimately periodic. For example: $-2/3 \simeq (01)^\infty \simeq \frac{\mathbf{z}}{1-\mathbf{z}^2} \simeq 1 + 2\mathbf{N}$.

## 2.2 Digital operations

An operator over $\mathbf{D}$ is defined for each representation by isomorphism

$$\mathbf{D} \simeq \mathbf{B}^{\infty} \simeq \mathbf{N} \mapsto \mathbf{B} \simeq 2^{\mathbf{N}} \simeq \mathbf{Z}_2 \simeq \mathbf{Z}_{\mathbf{z}}.$$

**Logical operations**

- NOT: $\neg a = [\textsc{n} \mapsto 1 - a_{\mathbf{N}}]$.
- AND: $a \cap b = [\textsc{n} \mapsto a_{\mathbf{N}} b_{\mathbf{N}}]$.
- OR: $a \cup b = [\textsc{n} \mapsto a_{\mathbf{N}} + b_{\mathbf{N}} - a_{\mathbf{N}} b_{\mathbf{N}}]$.
- XOR: $a \oplus b = [\textsc{n} \mapsto a_{\mathbf{N}} + b_{\mathbf{N}} - 2a_{\mathbf{N}} b_{\mathbf{N}}]$.

**Arithmetic operations** The infinite sums below converge in $\mathbf{D}$ by lemma 1.

- Opposite: $-a = \sum -a_{\mathbf{N}} 2^{\mathbf{N}} = 1 + \neg a$.
- Sum: $a + b = \sum (a_{\mathbf{N}} + b_{\mathbf{N}}) 2^{\mathbf{N}}$.
- Product: $a \times b = \sum 2^{\mathbf{N}} p_{\mathbf{N}}$ where $p_{\mathbf{N}} = \sum_{i+j=\mathbf{N}} a_i b_j$.
- Convolution: $a \otimes b = \sum 2^{\mathbf{N}} c_{\mathbf{N}}$ where $c_{\mathbf{N}} = \bigoplus_{i+j=\mathbf{N}} a_i b_j$.

The $\textsc{n}$-th *power* of $a \in \mathbf{D}$ is defined by $a^{0\times} = 1$ and by $a^{(1+\textsc{n})\times} = a \times a^{\mathbf{N}\times}$. The *convolution power* is defined by $a^{0\otimes} = 1$ and by $a^{(1+\textsc{n})\otimes} = a \otimes a^{\mathbf{N}\otimes}$.

**Shifts, sampling and shuffle**

- Up-shift: $\mathbf{z}a = [\textsc{n} \mapsto a_{\mathbf{N}-1}]$ where $a_{-1} = 0$; let $\mathbf{z}_b a = b + \mathbf{z}a$ for $b \in \mathbf{B}$.
- Down-shift: $\mathbf{z}^{-}a = [\textsc{n} \mapsto a_{\mathbf{N}+1}]$.
- Down-sample: $\downarrow a = [\textsc{n} \mapsto a_{2\mathbf{N}}]$ and $\downarrow' a = [\textsc{n} \mapsto a_{1+2\mathbf{N}}]$.
- Up-power: $\uparrow a = [2\textsc{n} \mapsto a_{\mathbf{N}},\ 1 + 2\textsc{n} \mapsto 0]$.
- Shuffle: $a \odot b = [2\textsc{n} \mapsto a_{\mathbf{N}},\ 1 + 2\textsc{n} \mapsto b_{\mathbf{N}}]$.

The $\textsc{n}$-th *up-power* of $a \in \mathbf{D}$ is defined by $\uparrow^0 a = a$ and by $\uparrow^{1+\mathbf{N}} a = \uparrow\uparrow^{\mathbf{N}} a$. It is related to the convolution power by $\uparrow^{\mathbf{N}} a = a^{2^{\mathbf{N}}\otimes} = a(\mathbf{z}^{2^{\mathbf{N}}})$.

The $\textsc{n}$-th *sample* of $a \in \mathbf{D}$ is defined by $\downarrow^1 a = a$, by $\downarrow^{2\mathbf{N}} a = \downarrow^{\mathbf{N}}\downarrow a$ and by $\downarrow^{1+2\mathbf{N}} a = \downarrow^{\mathbf{N}}\downarrow' a$.

**Combined operations** Let

$$e \in \langle 0\,1\,a\,b,\ \neg\ \mathbf{z}\,\mathbf{z}^{-}\ \downarrow\downarrow'\uparrow,\ \cap\ \cup\ \oplus\ \otimes\ +\ -\ \times\ \odot\rangle$$

denote an expression which is formed from the constants 0,1, variables $a, b \in \mathbf{D}$, the 6 unary operators between both commas, and the remaining 8 binary operators. The digital value $e \in \mathbf{D}$ of the expression is uniquely defined from the input values $a, b \in \mathbf{D}$ by composing the digital operators defined in the preceding section.

Digital algebra considers the relations between the sixteen operators above.

### 2.3 Digital rings

**Proposition 1.** Digital algebra $\langle \mathbf{D}, \neg, \cap \cup \oplus\ \otimes\ + - \times \rangle$ *combines the following classical algebraic structures.*

1. $\langle \mathbf{D}, \neg, \cup\ \cap \rangle$ *is isomorphic to the* Boolean Algebra $2^{\mathbf{N}}$ *formed by sets of natural numbers.* $\langle \mathbf{D}, , \oplus\ \cap \rangle$ *is isomorphic to the corresponding* Boolean ring*, where* $\textsc{d} = \textsc{d} \cap \textsc{d}$ *and* $0 = \textsc{d} \oplus \textsc{d}$*.*
2. $\langle \mathbf{D}, , \oplus\ \otimes \rangle$ *is isomorphic to the* ring $\mathbf{Z}_{\mathbf{z}} = \mathbf{F}_2((\mathbf{z})) \cap \mathbf{D}$ *of binary* series.
3. $\langle \mathbf{D}, -, +\ \times \rangle$ *is isomorphic to the* ring $\mathbf{Z}_2$ *of* 2-adic *integers.*

Since $\mathbf{z}a = 2 \otimes a = 2 \times a$ and $\uparrow a = a \otimes a = a(\mathbf{z}^2)$, the properties of up-shift and up-power follow from those of convolution.

Down-shift is inverse $a = \mathbf{z}^{-}\mathbf{z}a$ to the left of up-shift $\mathbf{z}$, but not to the right since $a - a_0 = \mathbf{z}\mathbf{z}^{-}a$.

**Proposition 2.** Digital algebra $\langle \mathbf{D}, \neg\ \mathbf{z}\,\mathbf{z}^{-}\ \downarrow \downarrow' \uparrow, \cap \cup \oplus\ \otimes\ + - \times\ \odot \rangle$ *contains the following chain of sub-algebra* $\mathbf{F}_2 \subset \mathbf{N} \subset \mathbf{Z} \subset \mathbf{Z}_{(2)} \subset \mathbf{A} \subset \mathcal{C} \subset \mathbf{D}$*.*

1. *A property of digital operators - excluding* $\{\neg\, -\}$ *- is true over* $\mathbf{D}$ *if and only if it holds over natural numbers* $\mathbf{N}$*.*
2. *A property of digital operators - excluding* $\{\uparrow\ \otimes \odot\}$ *- is true over* $\mathbf{D}$ *if and only if it holds over the integers* $\mathbf{Z}$*.*
3. *A property of digital operators is true over* $\mathbf{D}$ *if and only if it holds over the rational digital numbers* $\mathbf{Z}_{(2)} = \mathbf{Q} \cap \mathbf{D}$*.*
4. *Similarly for the* algebraic *digital numbers* $\mathbf{A} = \mathbf{A}_{\mathbf{z}} \cap \mathbf{D}$*.*
5. *Similarly for the* computable *digital numbers* $\mathcal{C}$*.*
6. *A property of digital operators - excluding* $\neg$ *- is true over* $\mathbf{D}$ *if and only if it holds over the floating-point digital numbers* $\mathbf{D}'$*.*

Shuffle and down-sampling are related by $a = (\downarrow a) \odot (\downarrow' a)$. There results an isomorphism $\mathbf{D} \simeq \mathbf{D} \odot \mathbf{D}$ between digital numbers and pairs of digital numbers, and similarly for natural $\mathbf{N} \simeq \mathbf{N} \odot \mathbf{N}$, rational $\mathbf{Z}_{(2)} \simeq \mathbf{Z}_{(2)} \odot \mathbf{Z}_{(2)}$, algebraic $\mathbf{A} \simeq \mathbf{A} \odot \mathbf{A}$ and computable $\mathcal{C} \simeq \mathcal{C} \odot \mathcal{C}$ digital numbers.

Finally note that set inclusion $\subset$ defines a *partial order* on $\mathbf{D}$. The lexicographic order defined by $a \prec b \Leftrightarrow \|a\| < \|b\|$ or $\|a\| = \|b\|$ and $\mathbf{z}^{-}a \prec \mathbf{z}^{-}b$ is a *total order* on $\mathbf{D}$.

### 2.4 Floating point digital numbers

The *floating-point digital numbers* $\mathbf{D}'$ result from adding the constant $\frac{1}{2}$ to $\mathbf{D}$, removing the logical negation $\neg$, and closing under all remaining operations.

A non-zero floating-point digital number $\textsc{d} \in \mathbf{D}'$ is uniquely [8] represented by $\textsc{d} = 2^v m$ where exponent $v \in \mathbf{Z}$ is an integer and mantissa $m \in 1 + 2\mathbf{D}$ is an odd $m_0 = 1$ digital number.

The rational number $\|\textsc{d}\| = 2^{-v}$ is the *norm* of $q \neq 0$ and $\|0\| = 0$. The corresponding *distance* $\|\textsc{d} - \textsc{d}'\| = \|\textsc{d} \oplus \textsc{d}'\|$ is *ultra-metric* $\|\textsc{d} + \textsc{d}'\| \leq \max(\|\textsc{d}\|, \|\textsc{d}'\|)$. The *ultra-metric* inequality implies the *triangle* inequality: $\|\textsc{d}+\textsc{d}'\| \leq \|\textsc{d}\|+\|\textsc{d}'\|$.

Every operator $\diamond \in \langle \mathbf{z} \downarrow \downarrow' \uparrow, \cap \cup \oplus \ \otimes \ + \ - \ \times \odot \rangle$ over $\mathbf{D}$ is extended to an operator $\diamond'$ over $\mathbf{D}'$ by $2^v m \diamond' 2^{v'} m' = 2^u(2^{v-u} m \diamond 2^{v'-u} m')$ for $u = \min(v, v')$.

A non-zero number $s = 2^v(1{+}2m)$ has inverses with respect to both multiply and convolve:

- $1/s = 2^{-v} m'$ with $m' = \sum 2^{\mathbf{N}} m^{\mathbf{N}\times}$ such that $(1/s) \times s = 1$;
- $1 \oslash s = 2^{-v} m''$ with $m'' = \bigoplus 2^{\mathbf{N}} m^{\mathbf{N}\otimes}$ such that $(1 \oslash s) \otimes s = 1$.

The corresponding divisions are $a/b = (1/a) \times b$ and $a \oslash b = (1 \oslash a) \otimes b$.

There are two classes of algebraic numbers in $\mathbf{D}'$, one $\mathbf{A}_2$ for integer operations $\{+ \ - \ \times /\}$ and the other $\mathbf{A}_{\mathbf{z}}$ for polynomial operations $\{\oplus \ \otimes \ \oslash\}$.

**Definition 2.** *Let* $\mathrm{D} \in \mathbf{D}'$ *be a floating-point digital number.*

$\mathbf{A}_2$ *Number* $\mathrm{D}$ *is* 2-algebraic $\mathrm{D} \in \mathbf{A}_2$ *if it is root* $0 = Q(\mathrm{D})$ *of a polynomial* $Q(\mathbf{y}) = \sum_{k \le d} q_k \times \mathbf{y}^{k\times}$ *with rational coefficients* $q_k \in \mathbf{Q}$.

$\mathbf{A}_{\mathbf{z}}$ *Number* $\mathrm{D}$ *is* $\mathbf{z}$-algebraic $\mathrm{D} \in \mathbf{A}_{\mathbf{z}}$ *if it is root* $0 = Q(\mathrm{D})$ *of a polynomial* $Q(\mathbf{y}) = \bigoplus_{k \le d} q_k \otimes \mathbf{y}^{k\otimes}$ *with rational coefficients* $q_k \in \mathbf{F}_2(\mathbf{z})$.

*Either polynomial* $Q$ *is non-trivial:* $q_d \neq 0$ *for* $d > 0$.

We are exclusively concerned here with field $\mathbf{A}_{\mathbf{z}}$.

### 2.5 Digital fields

**Proposition 3.** Floating-point digital numbers $\mathbf{D}'$ *include five fields:*

1. $\langle \mathbf{D}', , + \ - \ \times /\rangle$ *is isomorphic to the* field $\mathbf{Q}_2$ *of* 2-adic numbers.
2. *The field* $\mathbf{Q}$ *of rational numbers is a sub-field of* $\mathbf{A}_2$.
3. $\langle \mathbf{D}', , \oplus \ \otimes \ \oslash\rangle$ *is isomorphic to the* field $\mathbf{F}_2(\!(\mathbf{z})\!)$ *of binary* Laurent series.
4. *The field* $\mathbf{A}_{\mathbf{z}}$ *of algebraic series over* $\mathbf{F}_2(\mathbf{z})$ *is a sub-field of* $\mathbf{F}_2(\!(\mathbf{z})\!)$.
5. *The field* $\mathbf{F}_2(\mathbf{z})$ *of polynomial fractions is a sub-field of* $\mathbf{A}_{\mathbf{z}}$.

## 3 Digital functions

A digital function $f \in \mathbf{D} \mapsto \mathbf{D}$ maps $x = \sum 2^{\mathbf{N}} x_{\mathbf{N}} \in \mathbf{D}$ to $y = f(x) = \sum 2^{\mathbf{N}} y_{\mathbf{N}}$. Let $f_{\mathbf{N}}$ be defined by $f_{\mathbf{N}}(x) = y_{\mathbf{N}} \in \mathbf{B}$ for $x \in \mathbf{D}$. Function $f = \sum 2^{\mathbf{N}} f_{\mathbf{N}}$ is an infinite sum of digital predicates $f_{\mathbf{N}} \in \mathbf{D} \mapsto \mathbf{B}$.

### 3.1 Continuity and computability

A function $f \in \mathbf{D} \mapsto \mathbf{D}$ is *continuous* if $0 = \lim \|x{-}x'\| \Rightarrow 0 = \lim \|f(x){-}f(x')\|$ for all $x, x' \in \mathbf{D}$. This is the same definition as continuity over the reals $\mathbf{R}$.

A predicate $h \in \mathbf{D} \mapsto \mathbf{B}$ is continuous if and only if $h(x) = g(x_0 \cdots x_{m-1})$ for some *Boolean function* $g \in \mathbf{B}^m \mapsto \mathbf{B}$ and $m \in \mathbf{N}$. By contrast, a real predicate $h \in \mathbf{R} \mapsto \mathbf{B}$ is continuous if and only if it is trivial: $h(x) = 0$ or $h(x) = 1$.

A digital function $f = \sum 2^{\mathbf{N}} f_{\mathbf{N}}$ is *continuous* if and only if all $f_{\mathbf{N}} \in \mathbf{D} \mapsto \mathbf{B}$ are continuous. This is equivalent [11] to the fact that each output bit only depends upon *finitely many* input bits. In other words, a function is *continuous* if and only if it is *uniformly-continuous* [8]. By contrast, the sum $s = a +_{\mathbf{R}} b = \sum 2^{-\mathbf{N}} s_{\mathbf{N}}$ of two real binary numbers $a = \sum 2^{-\mathbf{N}} a_{\mathbf{N}}$ and $b = \sum 2^{-\mathbf{N}} b_{\mathbf{N}}$ is a continuous operation with respect to the norm on $\mathbf{R}$, but it is not continuous with respect to the 2-adic norm: bit $s_0$ of the sum over $\mathbf{R}$ can depend upon an arbitrary number of bits in $a$ and $b$, while bit $s_0$ of the sum over $\mathbf{Z}_2$ is $a_0 \oplus b_0$.

A digital function $f = \sum 2^{\mathbf{N}} f_{\mathbf{N}}$ is *computable* if it is continuous and $[\textsc{n} \mapsto f_{\mathbf{N}}]$ is a computable sequence of Boolean functions. In other words, there is a finite program for computing $y = f_{\mathbf{N}}(x)$ in a finite amount of time, over all integers $\textsc{n}$ and computable digital inputs $x \in \mathcal{C}$. All the digital functions defined here are computable except $+_{\mathbf{R}}$.

### 3.2 Causality

Physics demands that the function of a circuit be *strictly causal*: present output values only depend upon past input values. In the ideal mathematical model of DS circuits, Boolean gates have *zero delay* and the function is *weakly causal*: present output values only depend upon past and present input values.

**Proposition 4.** *A digital function is* causal $f \in \mathbf{D} \overset{c}{\to} \mathbf{D}$ *if and only if the following equivalent [11] characterizations apply.*

- *$f$ is computed by a node in some* infinite *DS circuit.*
- $\|f(x) - f(x')\| \leq \|x - x'\|$ *for all digital numbers* $x, x' \in \mathbf{D}$.
- $f(x) = \sum 2^{\mathbf{N}} f_{\mathbf{N}}(x_0 \cdots x_{\mathbf{N}})$ *where* $f_{\mathbf{N}} \in \mathbf{B}^{\mathbf{N}+1} \mapsto \mathbf{B}$.

### 3.3 Sequentiality

Physics also demands that circuits be *finite*.

**Proposition 5.** *A causal function is* sequential $f \in \mathbf{D} \overset{s}{\to} \mathbf{D}$ *if and only if the following equivalent characterizations apply.*

- *$f$ is causal and computable with bounded memory.*
- *$f$ is computed by a node in some finite DS circuit.*
- *$f$ is computed by some Mealy FSM.*

**Proposition 6.** *The following are two SNFs for* $f \in \mathbf{D} \overset{s}{\to} \mathbf{D}$.

- *The minimal deterministic Mealy mdFSM$(f)$. It is isomorphic to the set* $\{f(a + 2^i x) \div 2^i : a < 2^i\}$ *of* suffixes *of $f$. Let* $s = \textbf{states}\ f \in \mathbf{N} + 1$ *denote the common size.*
- *The* minimal memory circuit $MMC(f)$ *contains* $m = \lceil \log_2(s) \rceil$ *registers and its Boolean logic is derived from mdFSM.*

*No DS circuit with $m - 1$ registers computes $f$.*

### 3.4 Characterization of sequential functions

**Definition 3.** *Let $f(x) = \sum 2^{\mathbf{N}} f_{\mathbf{N}}(x_0 \cdots x_{\mathbf{N}})$ be a causal function.*
*The $\nu$-*transform *of $f$ is the digital number $F = \nu f \in 4\mathbf{D}$ defined by*

$$F(k) = f_{l-2}(\textsc{b}^k_{l-2} \cdots \textsc{b}^k_0) \in \mathbf{B}$$

*if the binary representation of $k = \sum 2^{\mathbf{N}} \textsc{b}^k_{\mathbf{N}}$ has length $l = \lceil \log_2(k+1) \rceil \geq 2$, and by $F(0) = F(1) = 0$ otherwise.*

The $\nu$-transform is an infinite truth-table which gathers all output bits of $f$ for all inputs in order $\nu f = 00 f_0(2) f_0(3) f_1(4) f_1(6) f_1(5) f_1(7) f_2(8) f_2(12) \cdots$

**Proposition 7.** *The $\nu$-transform is an isomorphism $4\mathbf{D} \simeq \nu(\mathbf{D} \overset{c}{\to} \mathbf{D})$ between causal functions $\mathbf{D} \overset{c}{\to} \mathbf{D}$ and multiple of 4 digital numbers $4\mathbf{D}$. The related $\nu'(f) = (\nu f) \div 4$ is a Boolean algebra isomorphism:*

$$\nu'(\neg f) = \neg \nu' f, \qquad \nu'(f \oplus g) = \nu' f \oplus \nu' g,$$
$$\nu'(f \cap g) = \nu' f \cap \nu' g, \; \nu'(f \cup g) = \nu' f \cup \nu' g.$$

*The transform of the identity $f(x) = x$ is the rational number $\nu(x) = 00(01)^\infty = \frac{\mathbf{z}^3}{1-\mathbf{z}^2} = -8/3$ and similarly for $\nu(0) = 0$ and $\nu(-1) = \frac{\mathbf{z}^2}{1-\mathbf{z}} = -4$.*
*The transform of $2f$ is quadratic: $\nu(2f) = F \odot F = 3 \uparrow F$ for $F = \nu f$.*

The theory of *p-automatic sequences* originates with Cobham [6]. The theorem of Christol&al [4], [5] identifies *p-automatic sequences* with *p-algebraic numbers*, i.e. Laurent series in $\mathbf{F}_p((\mathbf{z}))$ which are algebraic over the field $\mathbf{F}_p(\mathbf{z})$.

In terms of causal functions rather than automata, the *2-automatic* sequence[2] of $f \in \mathbf{D} \overset{c}{\to} \mathbf{D}$ is the digital number

$$\alpha f = f_0(0) f_1(1) f_2(2) f_2(3) f_3(4) f_3(6) f_3(5) f_3(7) f_4(8) f_4(12) \cdots$$

Unlike the $\nu$-transform, this correspondence is not one-to-one: the identity function $i(x) = x$ and the constant function $c(x) = -2$ have equal $\alpha(i) = \alpha(c) = -2$ 2-automatic sequences. Yet, they are close enough so that one [12] can derive from Christol's theorem that the $\nu$-transform of a sequential function is 2-algebraic. In addition, proposition 7 yields an isomorphism which is characteristic of the base $p = 2$.

**Theorem 1.** *The $\nu$-transform is an isomorphism $4\mathbf{A} \simeq \nu(\mathbf{D} \overset{s}{\to} \mathbf{D})$ between sequential functions $\mathbf{D} \overset{s}{\to} \mathbf{D}$ and algebraic numbers $4\mathbf{A} = \mathbf{A}_{\mathbf{z}} \cap 4\mathbf{D}$.*

## 4 Digital synchronous circuits

### 4.1 Net-list

A DS circuit is described by its *net-list* $L \in \mathcal{C}(-1\, x, \, \mathbf{z}, \cap \oplus \cup)^3$. The net-list is a finite or infinite sequence of definitions $v_{\mathbf{N}} = E_{\mathbf{N}}$, one for each net $\mathcal{V} = \bigcup v_{\mathbf{N}}$ in

[2] using the "lecture directe" in [5]

[3] Without loss in size, we replace NOT by the equivalent $\neg a = -1 \oplus a$.

the circuit. Through *topological sort* [10], we may freely assume that expression $E_{\mathbf{N}} \in \{x,\, \mathbf{z}v_{\mathbf{N}'},\, \neg v_{\mathbf{N}_0},\, v_{\mathbf{N}_0} \cap v_{\mathbf{N}_1},\, v_{\mathbf{N}_0} \oplus v_{\mathbf{N}_1},\, v_{\mathbf{N}_0} \cup v_{\mathbf{N}_1}\}$ is such that $\textsc{n}_0 < \textsc{n}$ and $\textsc{n}_1 < \textsc{n}$. The input of a Boolean operation is defined before it is used. It is thus impossible to introduce *combinational cycles* within DS circuits. No restriction applies to the input of a register $v_{\mathbf{N}} = \mathbf{z}v_{\mathbf{N}'}$, except that $v_{\mathbf{N}'} \in \mathcal{V}$ must be defined somewhere in the net-list. The register equation introduces a *feed-back cycle* when $\textsc{n}' \geq \textsc{n}$. By construction, all feed-back cycles within a DS circuit must contain at least one register $\mathbf{z}$.

### 4.2 Truth-list

By proposition 7, the net-list $L \in \mathcal{C}(-1\, x,\, \mathbf{z},\, \cap \oplus \cup)$ of a circuit is transformed - equation for equation - by $\nu$ into the *truth-list* $\nu L \in \mathcal{C}(-4\ \frac{-8}{3},,\odot \cap \oplus\cup)$.

The truth-list is a system of equations over digital numbers, built from rational constants, shuffle and logical operators. This system has a unique solution which is the $\nu$-transform of the function of each net $v$ in the net-list. By theorem 1 the solution of a *finite* system is algebraic $\nu(v) \in 4\mathbf{A}$ for every $v \in L$.

*Example 2.* The net-list $y = x \oplus \mathbf{z}y$ of a single bit binary counter $\nu$-transforms to the truth-list $Y = X \oplus (Y \odot Y)$ where $Y = \nu(y)$ and $X = \nu(x) = \frac{\mathbf{z}^3}{1-\mathbf{z}^2}$. This is equivalent to $Y(\mathbf{z}) = \frac{\mathbf{z}^3}{1-\mathbf{z}^2} \oplus (1+\mathbf{z})Y(\mathbf{z}^2)$ and series $Y(\mathbf{z}) \in \mathbf{A}$ is root $0 = P(Y, \mathbf{z})$ of the polynomial $P(\mathbf{y}, \mathbf{z}) = \frac{\mathbf{z}^3}{1-\mathbf{z}^2} + \mathbf{y} + (1+\mathbf{z})\mathbf{y}^2 \in \mathbf{F}_2(\mathbf{z})[\mathbf{y}]$. Number $Y = [\textsc{n} \mapsto Y_{\mathbf{N}}]$ is the logical NOT of the *Thue-Morse* sequence [1] minus 1:

$$Y_0 = Y_1 = 0,\ \ Y_{2\mathbf{N}} = Y_{\mathbf{N}} \text{ and } Y_{1+2\mathbf{N}} = 1 - Y_{\mathbf{N}}.$$

### 4.3 Transformed circuit analysis

The common practice in testing circuits is to add some sequential logic which is specific of the property under test, and to observe the output $y$ from this test logic. One so reduces testing to deciding if $y = 0$ or not. Circuit simulation can establish that $y \neq 0$ when that is the case, but $y = 0$ requires symbolic algebra to be proved. Symbolic algebra can also prove that $y \neq 0$, and sometimes faster than simulation.

Testing if $y = 0$ in a circuit given by a net-list $L$ is $\nu$-transformed to testing if $Y = 0$ in the truth-list $\nu L$. A problem on $n = |L|$ sequential functions is transformed into a problem of the same size $n$ on algebraic numbers.

We gain because the algebraic structure of the transform domain $\mathbf{A}$ is *richer* than that of the original $\mathbf{D} \overset{s}{\to} \mathbf{D}$.

- No loss in size arises for memory-less logic, since $\nu$ is (almost) a Boolean algebra isomorphism.
- No loss arises for the mdFSM, since the RBT is simply related in size.
- No loss and possibly significant size gain are achieved by the MUP.

### 4.4 Two examples

Let us illustrate the previous points with the *minus* circuit from example 1:

$$\begin{array}{r} \text{net-list}: \; x = \mathit{input}; \quad r = \mathbf{z}u; \qquad u = x \cup r; \quad y = x \oplus r. \\ \text{truth-list}: X = 0 \odot -2; \, R = U \odot U; \, U = X \cup R; \, Y = X \oplus R. \end{array} \tag{1}$$

The constants $0 = 0 \odot 0$, $-1 = -1 \odot -1$, $1 = 1 \odot 0$, $-2 = -2 \odot -1$ and $-4 = -2 \odot -2$ are well-known. The aim of normalization is to eliminate all Boolean definitions from the truth-list, and replace by shuffle definitions.

**Lemma 2.** *Let $g \in \mathbf{B}^2 \mapsto \mathbf{B}$ be a Boolean function. Then, for all $a, b, c, d \in \mathbf{D}$:*

$$f(a, b) \odot f(c, d) = f(a \odot c, b \odot d).$$

So, we can replace the Boolean definitions for $U$ and $Y$ in (1) by the equivalent:

$$\begin{array}{r} X = 0 \odot -2; \, R = U \odot U; \quad U = X \cup R; \quad Y = X \oplus R. \\ V = U \oplus -2; \, U = U \odot -2; \, Y = U \odot V. \end{array} \tag{2}$$

Note that the variables $X$ and $R$ are no longer used. In exchange, a new variable $V$ is added. Its Boolean definition is in turn replaced by a shuffle definition, and we finally obtain the RBT for minus:

$$V = V \odot 1; \, U = U \odot -2; \, Y = U \odot V. \tag{3}$$

Rewriting $U = U \odot -2 = \frac{\mathbf{z}^3}{1-\mathbf{z}^2} + \uparrow U$ yield the minimal up-polynomial $P_U = \frac{\mathbf{z}^3}{1-\mathbf{z}^2} + \mathbf{y} + \uparrow \mathbf{y}$ The only root is $U$. Rewriting $Y = U \odot V = \frac{\mathbf{z}^3}{1-\mathbf{z}^2} + (1 + \mathbf{z}) \uparrow U$ gives an expression in $U$. Elimination of $U$ through $0 = P_U(U)$ yield the MUP for the output $P_Y = q + \mathbf{y} + \frac{1}{1-\mathbf{z}} \uparrow \mathbf{y}$. The rational coefficient $q$ is equivalently represented by $q = 0001(01011010)^\infty = \frac{\mathbf{z}+\mathbf{z}^2+\mathbf{z}^3}{(1-\mathbf{z})^5} = 40/17$. The representation of $q$ by RBT has 6 nodes: $q = q1 \odot q2$; $q1 = q3 \odot q3$; $q2 = q4 \odot q5$; $q3 = -2 \odot 0$; $q4 = 0 \odot -1$; $q5 = 1 \odot -1$.

Polynomial $P_Y$ has two roots and we locate $Y$ by $Y_0 = 0$. This is sufficient since $P_Y$ has exactly one even root.

Our second example is a $n$ bit *shift-register* with net-list

$$s_0 = x; s_1 = \mathbf{z}s_0; \cdots s_n = \mathbf{z}s_{n-1}.$$

- The number of states in the mdFSM for $s_n$ is $2^n$.
- The RBT for $S_n = \nu s_n$ has $n + 1$ nodes.
- The MUP for $S_n = \nu s_n$ is $P_n(\mathbf{y}) = q_n + \mathbf{y}$ for $q_n = \frac{2^{2^n}(2^{2^n}-1)}{1-2^{2^{n+1}}}$ rational. The length of the binary representation of $q_n = 0^{2^{n+1}}(0^{2^n}1^{2^n})^\infty$ is $2^{n+2}$. The RBT representation of $q_n$ has $n + 1$ nodes.

This example provides a strong argument for representing the rational coefficients of the MUP by the RBT, rather than by an ultimately periodic binary sequence, or by quotient of integers.

## 5 Algebraic digital numbers

Through this last section, we use the symbols $+, \times$ from integer arithmetics to actually represent the polynomial operations $\oplus, \otimes$. This is all right since all, from here on, takes place in the field $\mathbf{Q_z} = \mathbf{F}_2(\!(\mathbf{z})\!)$ of binary Laurent series.

**Definition 4.** *A digital series $s \in \mathbf{D}' \simeq \mathbf{Q_z}$ is* algebraic[4] $s \in \mathbf{A_z}$ *if it is root*[5] $0 = \sum_{k \leq d} p_k s^k$ *of a polynomial $P \in \mathbf{F}_2[\mathbf{z}, \mathbf{y}]$ with coefficients $p_k \in \mathbf{F}_2[\mathbf{z}]$ and $p_d \neq 0$ for $d = \deg_{\mathbf{y}}(P) > 0$.*

Equivalently, $s$ is root $0 = \sum_{k \leq d} q_k s^k$ of a *monic* $q_d = 1$ polynomial $Q = P/p_d \in \mathbf{F}_2(\mathbf{z})[\mathbf{y}]$ with rational coefficients $q_k(\mathbf{z}) = p_k(\mathbf{z})/p_d(\mathbf{z}) \in \mathbf{F}_2(\mathbf{z})$.

### 5.1 Minimal polynomial

**Definition 5.** *The* algebraic degree $d_m = \deg(s)$ *of $s \in \mathbf{A_z}$ is the least degree $d_m = \min\{\deg_{\mathbf{y}}(Q) :\ 0 = Q(s), Q \neq 0\}$ among polynomials with root $s$.*

The dimension of the vector space $\mathcal{L} = \mathbf{F}_2(\mathbf{z})\langle 1\, s, \otimes \rangle$ generated over $\mathbf{F}_2(\mathbf{z})$ by the convolution powers of $s$ is finite and equal to $d_m$: $\mathcal{L} = \mathbf{F}_2(\mathbf{z})[1, s, \cdots s^{d_m - 1}]$.

The *minimal polynomial* of $s$ is the *unique* monic polynomial $Q \in \mathbf{F}_2(\mathbf{z})[\mathbf{y}]$ with root $0 = Q(s)$ and minimal degree $d_m = \deg(s)$. Uniqueness of $Q$ follows by contradiction: a common root $0 = Q(s) = Q'(s)$ to different $Q \neq Q'$ monic $q_d = 1$ polynomials with equal degree $d$ must also be root of $Q \oplus Q'$ - a non-trivial polynomial of degree $< d$.

The minimal polynomial of $\nu f \in 4\mathbf{A}$ yields a SNF for sequential function $f \in \mathbf{D} \overset{s}{\to} \mathbf{D}$. Yet, this representation is not simply related to any of the previous.

### 5.2 Minimal up-polynomial

A more economical representation arises by replacing convolution powers $s^{\mathbf{N}}$ by up-powers $\uparrow^{\mathbf{N}} s = s^{2^{\mathbf{N}}} = s(\mathbf{z}^{2^{\mathbf{N}}})$. It follows that $\uparrow^{\mathbf{N}} (s \oplus s') = (\uparrow^{\mathbf{N}} s) \oplus (\uparrow^{\mathbf{N}} s')$ is *linear*, and similarly for $\uparrow^{\mathbf{N}} (s \otimes s') = (\uparrow^{\mathbf{N}} s) \otimes (\uparrow^{\mathbf{N}} s')$.

**Proposition 8.** *The* minimal up-polynomial $P \in \mathbf{F}_2(\mathbf{z})[\mathbf{y}]$ *of $s \in \mathbf{A}$ is the unique $P(\mathbf{y}) = p_0 + p_1\mathbf{y} + p_2 \uparrow \mathbf{y} + \cdots + p_{d+1} \uparrow^d \mathbf{y}$ with root $0 = P(s)$ and minimal* up-degree $d \in \mathbf{N}$ *which is* unitary $p_1 = 1$. *The up-degree $d = \deg_2(s)$ of $P$ is smaller $d < d_m$ than the minimal degree $d_m = \deg(s)$, while $d_m \leq 2^d$.*

Uniqueness of the MUP follows by contradiction, as above. The unitary conditions $p_1 = 1$ and $p_d \neq 0$ are dual to the former monic conditions $p_0 \neq 0$ and $p_d = 1$.

For example, the Baum-Sweet series [2] has a minimal polynomial $1 + \mathbf{z}\mathbf{y} + \mathbf{y}^3$ of degree 3, and a minimal up-polynomial $\mathbf{y} + \mathbf{z} \uparrow \mathbf{y} + \uparrow^2 \mathbf{y}$ of up-degree 2. The root $a = \sum z^{2^{4\mathbf{N}}}$ of $\mathbf{z} + \mathbf{y} + \uparrow^4 \mathbf{y}$ has up-degree $4 = \deg_2(a)$ while $16 = \deg(a)$.

[4] we should really say **z**-algebraic, to distinguish from $\mathbf{A}_2$

[5] we should really write $0 = \bigoplus_{k \leq d} p_k \otimes s^{k\otimes}$

**Root location** By the fundamental theorem of Algebra, an up-polynomial of up-degree $d$ may have up to $2^d$ roots in $\mathbf{Q_z}$. For example, $P(\mathbf{y}) = \mathbf{z} + \mathbf{y} + \uparrow \mathbf{y}$ has two roots $f$ and $1 + f$; the Fredhom [5] series $f = \sum \mathbf{z}^{2^{\mathbf{N}}}$ is the standard root.

**Proposition 9.** *Let* $P(\mathbf{y}) = p_0 + \mathbf{y} + \sum_{1 \leq i \leq d} p_i \uparrow^i \mathbf{y} = \mathbf{y} + Q(\uparrow \mathbf{y})$ *be a unitary up-polynomial. Consider the* $s_{\mathbf{N}} \in \mathbf{F}_2(\mathbf{z})$ *defined by* $s_0 = 0$ *and* $s_{\mathbf{N}+1} = Q(\uparrow s_{\mathbf{N}})$. $P$ *has a root if and only if* $s = \sum s_{\mathbf{N}}$ *converges to some* $s \in \mathbf{Q_z}$. *Series* $s$ *is the* standard root *of* $P$ *and* $0 = P(s)$. *Every root* $0 = P(r)$ *of* $P$ *can be uniquely written as* $r = n2^{-v} + s'$, *where* $v \in \mathbf{N}$ *and* $n \in \mathbf{N}$ *is the least integer such that* $s'$ *is the standard root of* $P'(\mathbf{y}) = P(\mathbf{y}) + P(n2^{-v})$.

For example, the standard root of $\mathbf{y} + \mathbf{z} \uparrow \mathbf{y} + \uparrow^2 \mathbf{y}$ is zero. The other root is the Baum-Sweet series $b = 1 + s$ where $s$ is the standard root of $\mathbf{y} + \mathbf{z} + \mathbf{z} \uparrow \mathbf{y} + \uparrow^2 \mathbf{y}$.

**Comparison** The size of the MUP is smaller than that of the RBT.

**Proposition 10.** *Let* $y \in \mathbf{A}$ *be an algebraic digital number.*

1. *The minimal up-polynomial* $0 = P(y)$ *of* $y$ *has up-degree* $d = \log_2(\deg_{\mathbf{y}}(P))$.
2. *The vector space* $\mathcal{D} = \mathbf{F}_2(\mathbf{z})\langle 1\, y,\, \downarrow\, \downarrow' \rangle$ *generated over* $\mathbf{F}_2(\mathbf{z})$ *by* $1, y$ *and sampling is equal that* $\mathcal{U} = \mathbf{F}_2(\mathbf{z})\langle 1\, y,\, \uparrow \rangle$ *generated by up-powers. The common finite dimension is equal to* $d + 1$.
3. *The* sampling set $\mathcal{S} = \langle y,\, \downarrow\, \downarrow' \rangle$ *of* $y$ *is finite of size* $s$. *Size* $s$ *is greater than or equal to* $d$.

## References

1. J. P. Allouche. Automates finis en théorie des nombres. *Expositiones Mathematicae*, 5:239–266, 1987.
2. L. E. Baum and M. M. Sweet. Continued fractions of algebraic power series in characteristic 2. *Annals of Mathematics*, 103:593–610, 1976.
3. R. E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Trans. on Computers*, 35:8:677–691, 1986.
4. G. Christol. Ensembles presque periodiques k-reconaissables. *Theoretical Computer Science*, 9:141–145, 1979.
5. G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algèbriques, automates et substitutions. *Bull. Soc. Math. France*, pages 401–419, 1980.
6. A. Cobham. Uniform tag sequences. *Math. Systems Theory*, 6:164–192, 1972.
7. S. Eilenberg. *Automata, Languages, and Machines, vol. I.* Academic Press, 1974.
8. F. Q. Gouvêa. *p-adic numbers: an introduction - second edition.* Springer, 1991.
9. D. E. Knuth. *The Art of Computer Programming, vol. 2, Seminumerical Algorithms.* Addison Wesley, 1981.
10. G. De Micheli. *Synthesis and optimizations of digital circuits.* McGraw-Hill, 1994.
11. J. Vuillemin. On circuits and numbers. *IEEE Trans. on VLSI*, 43:8:868–879, 1994.
12. J. Vuillemin. Finite circuits are characterized by 2-algebraic truth-tables. In *Advances in Computing Science - ASIAN 2000*, volume 1961 of *L.N.C.S.*, pages 1–12. Springer-Verlag, 2000.