FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 371–378, 2015
DOI: 10.1515/forma-2015-0029

DE GRUYTER OPEN
degruyter.com/view/j/forma

Algebra of Polynomially Bounded Sequences and Negligible Functions

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article we formalize negligible functions that play an essential role in cryptology [10], [2]. Generally, a cryptosystem is secure if the probability of succeeding any attacks against the cryptosystem is negligible. First, we formalize the algebra of polynomially bounded sequences [20]. Next, we formalize negligible functions and prove the set of negligible functions is a subset of the algebra of polynomially bounded sequences. Moreover, we then introduce equivalence relation between polynomially bounded sequences, using negligible functions.

MSC: 68Q25 94A60 03B35

Keywords: polynomially bounded function; negligible functions

MML identifier: ASYMPT_3, version: 8.1.04 5.33.1254

The notation and terminology used in this paper have been introduced in the following articles: [29], [16], [17], [20], [4], [19], [9], [24], [21], [5], [6], [26], [25], [1], [7], [13], [22], [12], [3], [11], [30], [27], [14], [15], [23], [28], [18], and [8].

1. Preliminaries

Let us consider a real number r. Now we state the propositions:

(1) $r < |r| + 1$.

(2) There exists a natural number N such that for every natural number n such that $N \leqslant n$ holds $r < \frac{n}{\log_2 n}$.

Let us consider a natural number k. Now we state the propositions:

(3) There exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $x^k < 2^x$. The theorem is a consequence of (2).

ISSN 1426–2630(Print), 1898-9934(Online)

(4) There exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $\frac{1}{2^x} < \frac{1}{x^k}$. The theorem is a consequence of (3).

Now we state the proposition:

(5) Let us consider a natural number z. Suppose $2 \leqslant z$. Let us consider a natural number k. Then there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $\frac{1}{z^x} < \frac{1}{x^k}$. The theorem is a consequence of (4).

Observe that there exists a finite 0-sequence of $\mathbb{R}$ which is positive yielding and there exists a positive yielding finite 0-sequence of $\mathbb{R}$ which is non empty.

Now we state the proposition:

(6) Let us consider a finite 0-sequence c of $\mathbb{R}$, and a real number a. Then $a \cdot c$ is a finite 0-sequence of $\mathbb{R}$.

Let c be a finite 0-sequence of $\mathbb{R}$ and a be a real number. Observe that $a \cdot c$ is finite as a transfinite sequence of elements of $\mathbb{R}$.

Now we state the proposition:

(7) Let us consider a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$, and a real number a. Suppose $0 < a$. Then $a \cdot c$ is a non empty, positive yielding finite 0-sequence of $\mathbb{R}$. The theorem is a consequence of (6).

Let c be a non empty, positive yielding finite 0-sequence of $\mathbb{R}$ and a be a positive real number. Observe that $a \cdot c$ is non empty and positive yielding as a finite 0-sequence of $\mathbb{R}$.

Let c be a finite 0-sequence of $\mathbb{R}$. We introduce the notation $\operatorname{polynom} c$ as a synonym of $\mathrm{Seq}_{\mathrm{poly}}(c)$.

Now we state the propositions:

(8) Let us consider a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$, and a natural number x. Then $0 < (\operatorname{polynom} c)(x)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty, positive yielding finite 0-sequence c of $\mathbb{R}$ such that $\operatorname{len} c = \$_1$ for every natural number x, $0 < (\operatorname{polynom} c)(x)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [20, (28), (29)], [1, (44)], [5, (3), (47)]. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. $\square$

(9) Let us consider non empty, positive yielding finite 0-sequences c, c_1 of $\mathbb{R}$, and a real number a. Suppose $c_1 = a \cdot c$. Let us consider a natural number x. Then $(\operatorname{polynom} c_1)(x) = a \cdot (\operatorname{polynom} c)(x)$.

Proof: For every object i such that $i \in \operatorname{dom}(c_1 \cdot \{x^{1 \cdot n+0}\}_{n \in \mathbb{N}})$ holds $(c_1 \cdot \{x^{1 \cdot n+0}\}_{n \in \mathbb{N}})(i) = (a \cdot (c \cdot \{x^{1 \cdot n+0}\}_{n \in \mathbb{N}}))(i)$ by [20, (26)]. $\square$

2. Algebra of Polynomially Bounded Sequences

Let p be a sequence of real numbers. We say that p is absolutely polynomially bounded if and only if

(Def. 1) there exists a natural number k such that $|p| \in O(\{n^k\}_{n \in \mathbb{N}})$.

One can verify that every sequence of real numbers which is polynomially bounded is also absolutely polynomially bounded.

Now we state the proposition:

(10) Let us consider an element r of $\mathbb{N}$, and a sequence s of real numbers. If $s = \mathbb{N} \longmapsto r$, then s is absolutely polynomially bounded.

One can check that there exists a function from $\mathbb{N}$ into $\mathbb{R}$ which is absolutely polynomially bounded.

Let f, g be absolutely polynomially bounded functions from $\mathbb{N}$ into $\mathbb{R}$. One can verify that $f + g$ is absolutely polynomially bounded as a function from $\mathbb{N}$ into $\mathbb{R}$ and $f \cdot g$ is absolutely polynomially bounded as a function from $\mathbb{N}$ into $\mathbb{R}$.

Let f be an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$ and a be an element of $\mathbb{R}$. Observe that $a \cdot f$ is absolutely polynomially bounded as a function from $\mathbb{N}$ into $\mathbb{R}$.

The functor $\mathcal{O}_{\rm poly}$ yielding a subset of RAlgebra $\mathbb{N}$ is defined by

(Def. 2) for every object x, $x \in it$ iff x is an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$.

Note that $\mathcal{O}_{\rm poly}$ is non empty.

The functor RAlgebra$\mathcal{O}_{\rm poly}$ yielding a strict algebra structure is defined by

(Def. 3) the carrier of $it = \mathcal{O}_{\rm poly}$ and the multiplication of $it = \cdot_{\mathbb{R}^{\mathbb{N}}} \restriction \mathcal{O}_{\rm poly}$ and the addition of $it = +_{\mathbb{R}^{\mathbb{N}}} \restriction \mathcal{O}_{\rm poly}$ and the external multiplication of $it = \cdot^{\mathbb{R}}_{\mathbb{R}^{\mathbb{N}}} \restriction (\mathbb{R} \times \mathcal{O}_{\rm poly})$ and the one of $it = \mathbf{1}_{\mathbb{R}^{\mathbb{N}}}$ and the zero of $it = \mathbf{0}_{\mathbb{R}^{\mathbb{N}}}$.

One can verify that RAlgebra$\mathcal{O}_{\rm poly}$ is non empty.

Now we state the propositions:

(11) The carrier of RAlgebra$\mathcal{O}_{\rm poly} \subseteq$ the carrier of RAlgebra $\mathbb{N}$.

(12) Let us consider an object f. Then $f \in$ RAlgebra$\mathcal{O}_{\rm poly}$ if and only if f is an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$.

Let us consider points f, g of RAlgebra$\mathcal{O}_{\rm poly}$ and points f_1, g_1 of RAlgebra $\mathbb{N}$. Let us assume that $f = f_1$ and $g = g_1$. Now we state the propositions:

(13) $f \cdot g = f_1 \cdot g_1$.

(14) $f + g = f_1 + g_1$.

Now we state the propositions:

(15) Let us consider a point f of RAlgebra$\mathcal{O}_{\text{poly}}$, a point f_1 of RAlgebra $\mathbb{N}$, and an element a of $\mathbb{R}$. If $f = f_1$, then $a \cdot f = a \cdot f_1$.

(16) $0_{\text{RAlgebra}\mathcal{O}_{\text{poly}}} = 0_{\text{RAlgebra}\,\mathbb{N}}$.

(17) $1_{\text{RAlgebra}\mathcal{O}_{\text{poly}}} = 1_{\text{RAlgebra}\,\mathbb{N}}$.

One can check that RAlgebra$\mathcal{O}_{\text{poly}}$ is strict, Abelian, add-associative, right zeroed, right complementable, commutative, associative, right unital, right distributive, vector associative, scalar associative, vector distributive, and scalar distributive.

Now we state the proposition:

(18) RAlgebra$\mathcal{O}_{\text{poly}}$ is an algebra.

Let us consider vectors f, g, h of RAlgebra$\mathcal{O}_{\text{poly}}$ and functions f', g', h' from $\mathbb{N}$ into $\mathbb{R}$.

Let us assume that $f' = f$ and $g' = g$ and $h' = h$. Now we state the propositions:

(19) $h = f + g$ if and only if for every natural number x, $h'(x) = f'(x) + g'(x)$. The theorem is a consequence of (11) and (14).

(20) $h = f \cdot g$ if and only if for every natural number x, $h'(x) = f'(x) \cdot g'(x)$. The theorem is a consequence of (11) and (13).

Now we state the proposition:

(21) Let us consider vectors f, h of RAlgebra$\mathcal{O}_{\text{poly}}$, and functions f', h' from $\mathbb{N}$ into $\mathbb{R}$. Suppose $f' = f$ and $h' = h$. Let us consider a real number a. Then $h = a \cdot f$ if and only if for every natural number x, $h'(x) = a \cdot f'(x)$. The theorem is a consequence of (11) and (15).

3. Negligible Functions

Definition 1.3.5 of [10], p.16: Let f be a function from $\mathbb{N}$ into $\mathbb{R}$. We say that f is negligible if and only if

(Def. 4) for every non empty, positive yielding finite 0-sequence c of $\mathbb{R}$, there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $|f(x)| < \frac{1}{(\text{polynom}\, c)(x)}$.

Now we state the propositions:

(22) Let us consider a real number r. Suppose $0 < r$. Then there exists a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$ such that for every natural number x, $(\text{polynom}\, c)(x) = r$.

(23) Let us consider a function f from $\mathbb{N}$ into $\mathbb{R}$. Suppose f is negligible. Let us consider a real number r. Suppose $0 < r$. Then there exists a natural

number N such that for every natural number x such that $N \leqslant x$ holds $|f(x)| < r$. The theorem is a consequence of (22).

(24) Let us consider a function f from $\mathbb{N}$ into $\mathbb{R}$. If f is negligible, then f is convergent and $\lim f = 0$. The theorem is a consequence of (23).

Let us observe that $\{0\}_{n \in \mathbb{N}}$ is negligible and there exists a function from $\mathbb{N}$ into $\mathbb{R}$ which is negligible.

Let f be a negligible function from $\mathbb{N}$ into $\mathbb{R}$. Let us observe that $|f|$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Let a be a real number. One can verify that $a \cdot f$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Let f, g be negligible functions from $\mathbb{N}$ into $\mathbb{R}$. One can check that $f + g$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$ and $f \cdot g$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Now we state the propositions:

(25) INVERSE OF POWER OF 2 IS NEGLIGIBLE:
Let us consider a function f from $\mathbb{N}$ into $\mathbb{R}$. If for every natural number x, $f(x) = \frac{1}{2^x}$, then f is negligible.
PROOF: Set $k = \operatorname{len} c$. Define $\mathcal{F}(\text{natural number}) = 1 \cdot \$_1^k$. Consider y being a sequence of real numbers such that for every natural number x, $y(x) = \mathcal{F}(x)$ from [14, Sch. 1]. Consider N_1 being a natural number such that for every natural number x such that $N_1 \leqslant x$ holds $|(\mathrm{Seq}_{\mathrm{poly}}(c))(x)| \leqslant y(x)$. Consider N_2 being a natural number such that for every natural number x such that $N_2 \leqslant x$ holds $\frac{1}{2^x} < \frac{1}{x^k}$. Set $N = N_1 + N_2$. For every natural number x such that $N \leqslant x$ holds $|f(x)| < \frac{1}{(\mathrm{polynom}\, c)(x)}$ by [1, (12)], (8). $\square$

(26) Let us consider functions f, g from $\mathbb{N}$ into $\mathbb{R}$. Suppose f is negligible and for every natural number x, $|g(x)| \leqslant |f(x)|$. Then g is negligible.

One can check that every function from $\mathbb{N}$ into $\mathbb{R}$ which is negligible is also absolutely polynomially bounded.

The functor negligible-Funcs yielding a subset of $\mathcal{O}_{\mathrm{poly}}$ is defined by

(Def. 5) for every object x, $x \in it$ iff x is a negligible function from $\mathbb{N}$ into $\mathbb{R}$.

Let us observe that negligible-Funcs is non empty.

Let us consider vectors v, w of RAlgebra$\mathcal{O}_{\mathrm{poly}}$ and functions v_1, w_1 from $\mathbb{N}$ into $\mathbb{R}$.

Let us assume that $v = v_1$ and $w_1 = w$. Now we state the propositions:

(27) $v + w = v_1 + w_1$. The theorem is a consequence of (19).

(28) $v \cdot w = v_1 \cdot w_1$. The theorem is a consequence of (20).

Now we state the propositions:

(29) Let us consider a real number a, a vector v of RAlgebra$\mathcal{O}_{\rm poly}$, and a function v_1 from $\mathbb{N}$ into $\mathbb{R}$. If $v = v_1$, then $a \cdot v = a \cdot v_1$. The theorem is a consequence of (21).

(30) Let us consider a real number a, and a vector v of RAlgebra$\mathcal{O}_{\rm poly}$. Suppose $v \in$ negligible-Funcs. Then $a \cdot v \in$ negligible-Funcs. The theorem is a consequence of (29).

Let us consider vectors v, u of RAlgebra$\mathcal{O}_{\rm poly}$.

Let us assume that v, $u \in$ negligible-Funcs. Now we state the propositions:

(31) $v + u \in$ negligible-Funcs. The theorem is a consequence of (27).

(32) $v \cdot u \in$ negligible-Funcs. The theorem is a consequence of (28).

Let f, g be functions from $\mathbb{N}$ into $\mathbb{R}$. We say that $f \approx_{\rm neg} g$ if and only if

(Def. 6) there exists a function h from $\mathbb{N}$ into $\mathbb{R}$ such that h is negligible and for every natural number x, $|f(x) - g(x)| \leqslant |h(x)|$.

One can verify that the predicate is reflexive and symmetric.

Now we state the propositions:

(33) Let us consider functions f, g, h from $\mathbb{N}$ into $\mathbb{R}$. Suppose $f \approx_{\rm neg} g$ and $g \approx_{\rm neg} h$. Then $f \approx_{\rm neg} h$.

(34) Let us consider functions f, g from $\mathbb{N}$ into $\mathbb{R}$. Then $f \approx_{\rm neg} g$ if and only if $f - g$ is negligible. The theorem is a consequence of (26).

(35) Let us consider a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$. Then there exists a real number a and there exist natural numbers k, N such that $0 < a$ and $0 < k$ and for every natural number x such that $N \leqslant x$ holds $(\text{polynom}\, c)(x) \leqslant a \cdot x^k$. The theorem is a consequence of (8).

Let a be a non-negative yielding finite 0-sequence of $\mathbb{R}$ and b be a non-negative yielding sequence of real numbers. Let us observe that $a \cdot b$ is non-negative yielding.

Let a, b be non-negative yielding finite 0-sequences of $\mathbb{R}$. One can check that $a \frown b$ is non-negative yielding.

Let a, b, c be non negative real numbers. Let us note that $\{a^{b \cdot n + c}\}_{n \in \mathbb{N}}$ is non-negative yielding.

Now we state the propositions:

(36) Let us consider a real number a, and a natural number k. Then there exists a non empty, positive yielding finite 0-sequence c of $\mathbb{R}$ such that for every natural number x, $a \cdot x^k \leqslant (\text{polynom}\, c)(x)$.

PROOF: Reconsider $c = \mathbb{Z}_{k+1} \longmapsto |a| + 1$ as a finite 0-sequence of $\mathbb{R}$. For every natural number x, $a \cdot x^k \leqslant (\text{polynom}\, c)(x)$ by [14, (1)], [24, (13), (7)], [1, (44)]. □

(37) Let us consider non empty, positive yielding finite 0-sequences c, s of $\mathbb{R}$. Then there exists a non empty, positive yielding finite 0-sequence d of $\mathbb{R}$ and there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $(\operatorname{polynom} c)(x) \cdot (\operatorname{polynom} s)(x) \leqslant (\operatorname{polynom} d)(x)$.
PROOF: Consider a_1 being a real number, k_1, N_1 being natural numbers such that $0 < a_1$ and $0 < k_1$ and for every natural number x such that $N_1 \leqslant x$ holds $(\operatorname{polynom} c)(x) \leqslant a_1 \cdot x^{k_1}$. Consider a_2 being a real number, k_2, N_2 being natural numbers such that $0 < a_2$ and $0 < k_2$ and for every natural number x such that $N_2 \leqslant x$ holds $(\operatorname{polynom} s)(x) \leqslant a_2 \cdot x^{k_2}$. Consider d being a non empty, positive yielding finite 0-sequence of $\mathbb{R}$ such that for every natural number x, $a_1 \cdot a_2 \cdot x^{k_1+k_2} \leqslant (\operatorname{polynom} d)(x)$. $0 < (\operatorname{polynom} c)(x)$. $0 < (\operatorname{polynom} s)(x)$. $a_1 \cdot x^{k_1} \cdot (a_2 \cdot x^{k_2}) = (a_1 \cdot a_2) \cdot x^{k_1+k_2}$ by [22, (27)]. $\square$

Let f be a negligible function from $\mathbb{N}$ into $\mathbb{R}$ and c be a non empty, positive yielding finite 0-sequence of $\mathbb{R}$. Let us observe that $\operatorname{polynom} c \cdot f$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Now we state the proposition:

(38) Let us consider an absolutely polynomially bounded function g from $\mathbb{N}$ into $\mathbb{R}$. Then there exists a non empty, positive yielding finite 0-sequence d of $\mathbb{R}$ and there exists a natural number N such that for every natural number x such that $N \leqslant x$ holds $|g(x)| \leqslant (\operatorname{polynom} d)(x)$. The theorem is a consequence of (36).

Let f be a negligible function from $\mathbb{N}$ into $\mathbb{R}$ and g be an absolutely polynomially bounded function from $\mathbb{N}$ into $\mathbb{R}$. Let us note that $g \cdot f$ is negligible as a function from $\mathbb{N}$ into $\mathbb{R}$.

Now we state the proposition:

(39) Let us consider vectors v, w of $\mathrm{RAlgebra}\mathcal{O}_{\mathrm{poly}}$.
Suppose $w \in$ negligible-Funcs. Then $v \cdot w \in$ negligible-Funcs. The theorem is a consequence of (12) and (28).

ACKNOWLEDGEMENT: The author would like to express his gratitude to Prof. Yuichi Futa and Prof. Yasunari Shidama for their support and encouragement.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[2] Mihir Bellare. A note on negligible functions, 2002.
[3] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools.* Cambridge University Press, 2001.
[11] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**): 35–40, 1990.
[12] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[13] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.
[14] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[15] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.
[16] Richard Krueger, Piotr Rudnicki, and Paul Shelley. Asymptotic notation. Part I: Theory. *Formalized Mathematics*, 9(**1**):135–142, 2001.
[17] Richard Krueger, Piotr Rudnicki, and Paul Shelley. Asymptotic notation. Part II: Examples and problems. *Formalized Mathematics*, 9(**1**):143–154, 2001.
[18] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[19] Adam Naumowicz. Conjugate sequences, bounded complex sequences and convergent complex sequences. *Formalized Mathematics*, 6(**2**):265–268, 1997.
[20] Hiroyuki Okazaki and Yuichi Futa. Polynomially bounded sequences and polynomial sequences. *Formalized Mathematics*, 23(**3**):205–213, 2015. doi:10.1515/forma-2015-0017.
[21] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(**3**):555–561, 1990.
[22] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.
[23] Konrad Raczkowski and Andrzej Nędzusiak. Series. *Formalized Mathematics*, 2(**4**):449–452, 1991.
[24] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[25] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[26] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[27] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[28] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[29] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.
[30] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received August 15, 2015