Formalized
Mathematics

(a computer assisted approach)

Contents

Several Differentiation Formulas of Special Functions. Part V

Peng Wang
Qingdao University of Science
and Technology
China

Bo Li
Qingdao University of Science
and Technology
China

Summary. In this article, we give several differentiation formulas of special and composite functions including trigonometric, polynomial and logarithmic functions.

The articles [13], [15], [1], [16], [2], [4], [10], [11], [17], [5], [14], [12], [3], [7], [6], [9], and [8] provide the notation and terminology for this paper.

The partial function sec from $\mathbb{R}$ to $\mathbb{R}$ is defined as follows:

(Def. 1) $\sec = \frac{1}{\text{the function cos}}$.

The partial function cosec from $\mathbb{R}$ to $\mathbb{R}$ is defined by:

(Def. 2) $\mathrm{cosec} = \frac{1}{\text{the function sin}}$.

For simplicity, we follow the rules: x, a, b, c are real numbers, n is a natural number, Z is an open subset of $\mathbb{R}$, and f, f_1, f_2 are partial functions from $\mathbb{R}$ to $\mathbb{R}$.

One can prove the following propositions:

(1)   If (the function cos)$(x) \neq 0$, then sec is differentiable in x and $(\sec)'(x) = \frac{(\text{the function sin})(x)}{(\text{the function cos})(x)^2}$.

(2)   If (the function sin)$(x) \neq 0$, then cosec is differentiable in x and $(\mathrm{cosec})'(x) = -\frac{(\text{the function cos})(x)}{(\text{the function sin})(x)^2}$.

(3) $(\frac{1}{x})^n_{\mathbb{Z}} = \frac{1}{x^n_{\mathbb{Z}}}$.

(4)   Suppose $Z \subseteq \mathrm{dom}\,\sec$. Then sec is differentiable on Z and for every x such that $x \in Z$ holds $(\sec)'_{\restriction Z}(x) = \frac{(\text{the function sin})(x)}{(\text{the function cos})(x)^2}$.

(5) Suppose $Z \subseteq \operatorname{dom} \operatorname{cosec}$. Then cosec is differentiable on Z and for every x such that $x \in Z$ holds $(\operatorname{cosec})'_{\restriction Z}(x) = -\frac{\text{(the function cos)}(x)}{\text{(the function sin)}(x)^{\mathbf{2}}}$.

(6) Suppose $Z \subseteq \operatorname{dom}(\operatorname{sec} \cdot f)$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$. Then

(i) $\operatorname{sec} \cdot f$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{sec} \cdot f)'_{\restriction Z}(x) = \frac{a \cdot \text{(the function sin)}(a \cdot x + b)}{\text{(the function cos)}(a \cdot x + b)^{\mathbf{2}}}$.

(7) Suppose $Z \subseteq \operatorname{dom}(\operatorname{cosec} \cdot f)$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$. Then

(i) $\operatorname{cosec} \cdot f$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{cosec} \cdot f)'_{\restriction Z}(x) = -\frac{a \cdot \text{(the function cos)}(a \cdot x + b)}{\text{(the function sin)}(a \cdot x + b)^{\mathbf{2}}}$.

(8) Suppose $Z \subseteq \operatorname{dom}(\operatorname{sec} \cdot \frac{1}{f})$ and for every x such that $x \in Z$ holds $f(x) = x$. Then

(i) $\operatorname{sec} \cdot \frac{1}{f}$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{sec} \cdot \frac{1}{f})'_{\restriction Z}(x) = -\frac{\text{(the function sin)}(\frac{1}{x})}{x^{\mathbf{2}} \cdot \text{(the function cos)}(\frac{1}{x})^{\mathbf{2}}}$.

(9) Suppose $Z \subseteq \operatorname{dom}(\operatorname{cosec} \cdot \frac{1}{f})$ and for every x such that $x \in Z$ holds $f(x) = x$. Then

(i) $\operatorname{cosec} \cdot \frac{1}{f}$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{cosec} \cdot \frac{1}{f})'_{\restriction Z}(x) = \frac{\text{(the function cos)}(\frac{1}{x})}{x^{\mathbf{2}} \cdot \text{(the function sin)}(\frac{1}{x})^{\mathbf{2}}}$.

(10) Suppose $Z \subseteq \operatorname{dom}(\operatorname{sec} \cdot (f_1 + c \, f_2))$ and $f_2 = {}^2_{\mathbb{Z}}$ and for every x such that $x \in Z$ holds $f_1(x) = a + b \cdot x$. Then

(i) $\operatorname{sec} \cdot (f_1 + c \, f_2)$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{sec} \cdot (f_1 + c \, f_2))'_{\restriction Z}(x) = \frac{(b + 2 \cdot c \cdot x) \cdot \text{(the function sin)}(a + b \cdot x + c \cdot x^{\mathbf{2}})}{\text{(the function cos)}(a + b \cdot x + c \cdot x^{\mathbf{2}})^{\mathbf{2}}}$.

(11) Suppose $Z \subseteq \operatorname{dom}(\operatorname{cosec} \cdot (f_1 + c \, f_2))$ and $f_2 = {}^2_{\mathbb{Z}}$ and for every x such that $x \in Z$ holds $f_1(x) = a + b \cdot x$. Then

(i) $\operatorname{cosec} \cdot (f_1 + c \, f_2)$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{cosec} \cdot (f_1 + c \, f_2))'_{\restriction Z}(x) = -\frac{(b + 2 \cdot c \cdot x) \cdot \text{(the function cos)}(a + b \cdot x + c \cdot x^{\mathbf{2}})}{\text{(the function sin)}(a + b \cdot x + c \cdot x^{\mathbf{2}})^{\mathbf{2}}}$.

(12) Suppose $Z \subseteq \operatorname{dom}(\operatorname{sec} \cdot (\text{the function exp}))$. Then

(i) $\operatorname{sec} \cdot (\text{the function exp})$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\operatorname{sec} \cdot (\text{the function exp}))'_{\restriction Z}(x) = \frac{\text{(the function exp)}(x) \cdot \text{(the function sin)}((\text{the function exp})(x))}{\text{(the function cos)}((\text{the function exp})(x))^{\mathbf{2}}}$.

(13) Suppose $Z \subseteq \operatorname{dom}(\operatorname{cosec} \cdot (\text{the function exp}))$. Then

(i) $\operatorname{cosec} \cdot (\text{the function exp})$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $(\text{cosec} \cdot (\text{the function exp}))'_{\restriction Z}(x) =$
$-\frac{(\text{the function exp})(x) \cdot (\text{the function cos})((\text{the function exp})(x))}{(\text{the function sin})((\text{the function exp})(x))^{\mathbf{2}}}$.

(14)   Suppose $Z \subseteq \text{dom}(\sec \cdot (\text{the function ln}))$. Then

   (i) $\sec \cdot (\text{the function ln})$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $(\sec \cdot (\text{the function ln}))'_{\restriction Z}(x) =$
$\frac{(\text{the function sin})((\text{the function ln})(x))}{x \cdot (\text{the function cos})((\text{the function ln})(x))^{\mathbf{2}}}$.

(15)   Suppose $Z \subseteq \text{dom}(\text{cosec} \cdot (\text{the function ln}))$. Then

   (i) $\text{cosec} \cdot (\text{the function ln})$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $(\text{cosec} \cdot (\text{the function ln}))'_{\restriction Z}(x) =$
$-\frac{(\text{the function cos})((\text{the function ln})(x))}{x \cdot (\text{the function sin})((\text{the function ln})(x))^{\mathbf{2}}}$.

(16)   Suppose $Z \subseteq \text{dom}((\text{the function exp}) \cdot \sec)$. Then

   (i) $(\text{the function exp}) \cdot \sec$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $((\text{the function exp}) \cdot \sec)'_{\restriction Z}(x) =$
$\frac{(\text{the function exp})((\sec)(x)) \cdot (\text{the function sin})(x)}{(\text{the function cos})(x)^{\mathbf{2}}}$.

(17)   Suppose $Z \subseteq \text{dom}((\text{the function exp}) \cdot \text{cosec})$. Then

   (i) $(\text{the function exp}) \cdot \text{cosec}$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $((\text{the function exp}) \cdot \text{cosec})'_{\restriction Z}(x) =$
$-\frac{(\text{the function exp})((\text{cosec})(x)) \cdot (\text{the function cos})(x)}{(\text{the function sin})(x)^{\mathbf{2}}}$.

(18)   Suppose $Z \subseteq \text{dom}((\text{the function ln}) \cdot \sec)$. Then

   (i) $(\text{the function ln}) \cdot \sec$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $((\text{the function ln}) \cdot \sec)'_{\restriction Z}(x) =$
$\frac{(\text{the function sin})(x)}{(\text{the function cos})(x)}$.

(19)   Suppose $Z \subseteq \text{dom}((\text{the function ln}) \cdot \text{cosec})$. Then

   (i) $(\text{the function ln}) \cdot \text{cosec}$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $((\text{the function ln}) \cdot \text{cosec})'_{\restriction Z}(x) =$
$-\frac{(\text{the function cos})(x)}{(\text{the function sin})(x)}$.

(20)   Suppose $Z \subseteq \text{dom}((\frac{n}{\mathbb{Z}}) \cdot \sec)$ and $1 \le n$. Then

   (i) $(\frac{n}{\mathbb{Z}}) \cdot \sec$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $((\frac{n}{\mathbb{Z}}) \cdot \sec)'_{\restriction Z}(x) = \frac{n \cdot (\text{the function sin})(x)}{(\text{the function cos})(x)_{\mathbb{Z}}^{n+1}}$.

(21)   Suppose $Z \subseteq \text{dom}((\frac{n}{\mathbb{Z}}) \cdot \text{cosec})$ and $1 \le n$. Then

   (i) $(\frac{n}{\mathbb{Z}}) \cdot \text{cosec}$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $((\frac{n}{\mathbb{Z}}) \cdot \text{cosec})'_{\restriction Z}(x) =$
$-\frac{n \cdot (\text{the function cos})(x)}{(\text{the function sin})(x)_{\mathbb{Z}}^{n+1}}$.

(22)   Suppose $Z \subseteq \text{dom}(\sec - \text{id}_Z)$. Then

   (i) $\sec - \text{id}_Z$ is differentiable on Z, and

   (ii)   for every x such that $x \in Z$ holds $(\sec - \text{id}_Z)'_{\restriction Z}(x) =$
$\frac{(\text{the function sin})(x) - (\text{the function cos})(x)^{\mathbf{2}}}{(\text{the function cos})(x)^{\mathbf{2}}}$.

(23) Suppose $Z \subseteq \mathrm{dom}(-\mathrm{cosec} - \mathrm{id}_Z)$. Then

(i) $-\mathrm{cosec} - \mathrm{id}_Z$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(-\mathrm{cosec} - \mathrm{id}_Z)'_{\restriction Z}(x) = \frac{(\text{the function cos})(x) - (\text{the function sin})(x)^{\mathbf{2}}}{(\text{the function sin})(x)^{\mathbf{2}}}$.

(24) Suppose $Z \subseteq \mathrm{dom}((\text{the function exp})\ \mathrm{sec})$. Then

(i) (the function exp) sec is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function exp})\ \mathrm{sec})'_{\restriction Z}(x) = \frac{(\text{the function exp})(x)}{(\text{the function cos})(x)} + \frac{(\text{the function exp})(x) \cdot (\text{the function sin})(x)}{(\text{the function cos})(x)^{\mathbf{2}}}$.

(25) Suppose $Z \subseteq \mathrm{dom}((\text{the function exp})\ \mathrm{cosec})$. Then

(i) (the function exp) cosec is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function exp})\ \mathrm{cosec})'_{\restriction Z}(x) = \frac{(\text{the function exp})(x)}{(\text{the function sin})(x)} - \frac{(\text{the function exp})(x) \cdot (\text{the function cos})(x)}{(\text{the function sin})(x)^{\mathbf{2}}}$.

(26) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{a}\,(\mathrm{sec} \cdot f) - \mathrm{id}_Z)$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x$ and $a \neq 0$. Then

(i) $\frac{1}{a}\,(\mathrm{sec} \cdot f) - \mathrm{id}_Z$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{a}\,(\mathrm{sec} \cdot f) - \mathrm{id}_Z)'_{\restriction Z}(x) = \frac{(\text{the function sin})(a \cdot x) - (\text{the function cos})(a \cdot x)^{\mathbf{2}}}{(\text{the function cos})(a \cdot x)^{\mathbf{2}}}$.

(27) Suppose $Z \subseteq \mathrm{dom}((-\frac{1}{a})\,(\mathrm{cosec} \cdot f) - \mathrm{id}_Z)$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x$ and $a \neq 0$. Then

(i) $(-\frac{1}{a})\,(\mathrm{cosec} \cdot f) - \mathrm{id}_Z$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((-\frac{1}{a})\,(\mathrm{cosec} \cdot f) - \mathrm{id}_Z)'_{\restriction Z}(x) = \frac{(\text{the function cos})(a \cdot x) - (\text{the function sin})(a \cdot x)^{\mathbf{2}}}{(\text{the function sin})(a \cdot x)^{\mathbf{2}}}$.

(28) Suppose $Z \subseteq \mathrm{dom}(f\ \mathrm{sec})$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$. Then

(i) f sec is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(f\ \mathrm{sec})'_{\restriction Z}(x) = \frac{a}{(\text{the function cos})(x)} + \frac{(a \cdot x + b) \cdot (\text{the function sin})(x)}{(\text{the function cos})(x)^{\mathbf{2}}}$.

(29) Suppose $Z \subseteq \mathrm{dom}(f\ \mathrm{cosec})$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$. Then

(i) f cosec is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(f\ \mathrm{cosec})'_{\restriction Z}(x) = \frac{a}{(\text{the function sin})(x)} - \frac{(a \cdot x + b) \cdot (\text{the function cos})(x)}{(\text{the function sin})(x)^{\mathbf{2}}}$.

(30) Suppose $Z \subseteq \mathrm{dom}((\text{the function ln})\ \mathrm{sec})$. Then

(i) (the function ln) sec is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\text{the function ln})\ \mathrm{sec})'_{\restriction Z}(x) = \frac{\frac{1}{(\text{the function cos})(x)}}{x} + \frac{(\text{the function ln})(x) \cdot (\text{the function sin})(x)}{(\text{the function cos})(x)^{\mathbf{2}}}$.

(31) Suppose $Z \subseteq \mathrm{dom}((\text{the function ln})\ \mathrm{cosec})$. Then

(i) (the function ln) $\cdot$ cosec is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function ln) $\cdot$ cosec)$'_{\restriction Z}(x) =$ $\frac{\frac{1}{(\text{the function sin})(x)}}{x} - \frac{(\text{the function ln})(x) \cdot (\text{the function cos})(x)}{(\text{the function sin})(x)^2}$.

(32) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{f} \sec)$ and for every x such that $x \in Z$ holds $f(x) = x$. Then

(i) $\frac{1}{f} \sec$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{f} \sec)'_{\restriction Z}(x) = -\frac{\frac{1}{(\text{the function cos})(x)}}{x^2} +$ $\frac{\frac{(\text{the function sin})(x)}{x}}{(\text{the function cos})(x)^2}$.

(33) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{f} \mathrm{cosec})$ and for every x such that $x \in Z$ holds $f(x) = x$. Then

(i) $\frac{1}{f} \mathrm{cosec}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{1}{f} \mathrm{cosec})'_{\restriction Z}(x) = -\frac{\frac{1}{(\text{the function sin})(x)}}{x^2} -$ $\frac{\frac{(\text{the function cos})(x)}{x}}{(\text{the function sin})(x)^2}$.

(34) Suppose $Z \subseteq \mathrm{dom}(\sec \cdot(\text{the function sin}))$. Then

(i) $\sec \cdot(\text{the function sin})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\sec \cdot(\text{the function sin}))'_{\restriction Z}(x) =$ $\frac{(\text{the function cos})(x) \cdot (\text{the function sin})((\text{the function sin})(x))}{(\text{the function cos})((\text{the function sin})(x))^2}$.

(35) Suppose $Z \subseteq \mathrm{dom}(\sec \cdot(\text{the function cos}))$. Then

(i) $\sec \cdot(\text{the function cos})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\sec \cdot(\text{the function cos}))'_{\restriction Z}(x) =$ $-\frac{(\text{the function sin})(x) \cdot (\text{the function sin})((\text{the function cos})(x))}{(\text{the function cos})((\text{the function cos})(x))^2}$.

(36) Suppose $Z \subseteq \mathrm{dom}(\mathrm{cosec} \cdot(\text{the function sin}))$. Then

(i) $\mathrm{cosec} \cdot(\text{the function sin})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\mathrm{cosec} \cdot(\text{the function sin}))'_{\restriction Z}(x) =$ $-\frac{(\text{the function cos})(x) \cdot (\text{the function cos})((\text{the function sin})(x))}{(\text{the function sin})((\text{the function sin})(x))^2}$.

(37) Suppose $Z \subseteq \mathrm{dom}(\mathrm{cosec} \cdot(\text{the function cos}))$. Then

(i) $\mathrm{cosec} \cdot(\text{the function cos})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\mathrm{cosec} \cdot(\text{the function cos}))'_{\restriction Z}(x) =$ $\frac{(\text{the function sin})(x) \cdot (\text{the function cos})((\text{the function cos})(x))}{(\text{the function sin})((\text{the function cos})(x))^2}$.

(38) Suppose $Z \subseteq \mathrm{dom}(\sec \cdot(\text{the function tan}))$. Then

(i) $\sec \cdot(\text{the function tan})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\sec \cdot(\text{the function tan}))'_{\restriction Z}(x) =$ $\frac{\frac{(\text{the function sin})((\text{the function tan})(x))}{(\text{the function cos})(x)^2}}{(\text{the function cos})((\text{the function tan})(x))^2}$.

(39) Suppose $Z \subseteq \mathrm{dom}(\sec \cdot(\text{the function cot}))$. Then

(i) $\sec \cdot(\text{the function cot})$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\sec \cdot(\text{the function } \cot))'_{\restriction Z}(x) =$

$$-\frac{\frac{(\text{the function } \sin)((\text{the function } \cot)(x))}{(\text{the function } \sin)(x)^{2}}}{(\text{the function } \cos)((\text{the function } \cot)(x))^{2}}.$$

(40)   Suppose $Z \subseteq \text{dom}(\text{cosec} \cdot(\text{the function } \tan))$. Then

 (i) $\text{cosec} \cdot(\text{the function } \tan)$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\text{cosec} \cdot(\text{the function } \tan))'_{\restriction Z}(x) =$

$$-\frac{\frac{(\text{the function } \cos)((\text{the function } \tan)(x))}{(\text{the function } \cos)(x)^{2}}}{(\text{the function } \sin)((\text{the function } \tan)(x))^{2}}.$$

(41)   Suppose $Z \subseteq \text{dom}(\text{cosec} \cdot(\text{the function } \cot))$. Then

 (i) $\text{cosec} \cdot(\text{the function } \cot)$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $(\text{cosec} \cdot(\text{the function } \cot))'_{\restriction Z}(x) =$

$$\frac{\frac{(\text{the function } \cos)((\text{the function } \cot)(x))}{(\text{the function } \sin)(x)^{2}}}{(\text{the function } \sin)((\text{the function } \cot)(x))^{2}}.$$

(42)   Suppose $Z \subseteq \text{dom}((\text{the function } \tan) \ \sec)$. Then

 (i) $(\text{the function } \tan) \ \sec$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $((\text{the function } \tan) \ \sec)'_{\restriction Z}(x) =$

$$\frac{\frac{1}{(\text{the function } \cos)(x)^{2}}}{(\text{the function } \cos)(x)} + \frac{(\text{the function } \tan)(x) \cdot (\text{the function } \sin)(x)}{(\text{the function } \cos)(x)^{2}}.$$

(43)   Suppose $Z \subseteq \text{dom}((\text{the function } \cot) \ \sec)$. Then

 (i) $(\text{the function } \cot) \ \sec$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $((\text{the function } \cot) \ \sec)'_{\restriction Z}(x) =$

$$-\frac{\frac{1}{(\text{the function } \sin)(x)^{2}}}{(\text{the function } \cos)(x)} + \frac{(\text{the function } \cot)(x) \cdot (\text{the function } \sin)(x)}{(\text{the function } \cos)(x)^{2}}.$$

(44)   Suppose $Z \subseteq \text{dom}((\text{the function } \tan) \ \text{cosec})$. Then

 (i) $(\text{the function } \tan) \ \text{cosec}$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $((\text{the function } \tan) \ \text{cosec})'_{\restriction Z}(x) =$

$$\frac{\frac{1}{(\text{the function } \cos)(x)^{2}}}{(\text{the function } \sin)(x)} - \frac{(\text{the function } \tan)(x) \cdot (\text{the function } \cos)(x)}{(\text{the function } \sin)(x)^{2}}.$$

(45)   Suppose $Z \subseteq \text{dom}((\text{the function } \cot) \ \text{cosec})$. Then

 (i) $(\text{the function } \cot) \ \text{cosec}$ is differentiable on Z, and

(ii)   for every x such that $x \in Z$ holds $((\text{the function } \cot) \ \text{cosec})'_{\restriction Z}(x) =$

$$-\frac{\frac{1}{(\text{the function } \sin)(x)^{2}}}{(\text{the function } \sin)(x)} - \frac{(\text{the function } \cot)(x) \cdot (\text{the function } \cos)(x)}{(\text{the function } \sin)(x)^{2}}.$$

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[2] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[3] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[4] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(**4**):697–702, 1990.

[5] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[6] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[7] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[8] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[9] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

[10] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[11] Yasunari Shidama. The Taylor expansions. *Formalized Mathematics*, 12(**2**):195–200, 2004.

[12] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[13] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[14] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[16] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[17] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

The Product Space of Real Normed Spaces and its Properties

Noboru Endou
Gifu National College of Technology
Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Keiichi Miyajima
Ibaraki University
Hitachi, Japan

Summary. In this article, we define the product space of real linear spaces and real normed spaces. We also describe properties of these spaces.

The terminology and notation used here are introduced in the following articles: [20], [9], [22], [2], [1], [19], [5], [23], [7], [10], [8], [4], [13], [12], [21], [14], [3], [6], [16], [11], [15], [17], and [18].

1. The Product Space of Real Linear Spaces

The following propositions are true:

(1) Let s, t be sequences of real numbers and g be a real number. Suppose that for every element n of $\mathbb{N}$ holds $t(n) = |s(n) - g|$. Then s is convergent and $\lim s = g$ if and only if t is convergent and $\lim t = 0$.

(2) Let x, y be finite sequences of elements of $\mathbb{R}$. Suppose $\operatorname{len} x = \operatorname{len} y$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{Seg} \operatorname{len} x$ holds $0 \le x(i)$ and $x(i) \le y(i)$. Then $|x| \le |y|$.

(3) Let F be a finite sequence of elements of $\mathbb{R}$. If for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} F$ holds $F(i) = 0$, then $\sum F = 0$.

Let f be a function and let X be a set. A function is called a multi-operation of X and f if:

(Def. 1) $\operatorname{dom} it = \operatorname{dom} f$ and for every set i such that $i \in \operatorname{dom} f$ holds $it(i)$ is a function from $[\![X,\, f(i)]\!]$ into $f(i)$.

Let F be a sequence of non empty sets and let X be a set. Observe that every multi-operation of X and F is finite sequence-like.

We now state the proposition

(4)   Let X be a set, F be a sequence of non empty sets, and p be a finite sequence. Then p is a multi-operation of X and F if and only if $\operatorname{len} p = \operatorname{len} F$ and for every set i such that $i \in \operatorname{dom} F$ holds $p(i)$ is a function from $[\![X,\, F(i)]\!]$ into $F(i)$.

Let F be a sequence of non empty sets, let X be a set, let p be a multi-operation of X and F, and let i be an element of $\operatorname{dom} F$. Then $p(i)$ is a function from $[\![X,\, F(i)]\!]$ into $F(i)$.

Next we state the proposition

(5)   Let X be a non empty set, F be a sequence of non empty sets, and f, g be functions from $[\![X,\, \prod F]\!]$ into $\prod F$. Suppose that for every element x of X and for every element d of $\prod F$ and for every element i of $\operatorname{dom} F$ holds $f(x, d)(i) = g(x, d)(i)$. Then $f = g$.

Let F be a sequence of non empty sets, let X be a non empty set, and let p be a multi-operation of X and F. The functor $\prod^{\circ} p$ yielding a function from $[\![X,\, \prod F]\!]$ into $\prod F$ is defined as follows:

(Def. 2)   For every element x of X and for every element d of $\prod F$ and for every element i of $\operatorname{dom} F$ holds $(\prod^{\circ} p)(x, d)(i) = p(i)(x, d(i))$.

Let R be a binary relation. We say that R is real-linear-space-yielding if and only if:

(Def. 3)   For every set S such that $S \in \operatorname{rng} R$ holds S is a real linear space.

Let us note that there exists a finite sequence which is non empty and real-linear-space-yielding.

A real linear space-sequence is a non empty real-linear-space-yielding finite sequence.

Let G be a real linear space-sequence and let j be an element of $\operatorname{dom} G$. Then $G(j)$ is a real linear space.

Let G be a real linear space-sequence. The functor $\overline{G}$ yielding a sequence of non empty sets is defined by:

(Def. 4) $\operatorname{len} \overline{G} = \operatorname{len} G$ and for every element j of $\operatorname{dom} G$ holds $\overline{G}(j) =$ the carrier of $G(j)$.

Let G be a real linear space-sequence and let j be an element of $\operatorname{dom} \overline{G}$. Then $G(j)$ is a real linear space.

Let G be a real linear space-sequence. The functor $\langle +_{G_i} \rangle_i$ yielding a family of binary operations of $\overline{G}$ is defined as follows:

(Def. 5) $\text{len}(\langle +_{G_i} \rangle_i) = \text{len}\,\overline{G}$ and for every element j of $\text{dom}\,\overline{G}$ holds $\langle +_{G_i} \rangle_i(j) =$ the addition of $G(j)$.

The functor $\langle -_{G_i} \rangle_i$ yields a family of unary operations of $\overline{G}$ and is defined as follows:

(Def. 6) $\text{len}(\langle -_{G_i} \rangle_i) = \text{len}\,\overline{G}$ and for every element j of $\text{dom}\,\overline{G}$ holds $\langle -_{G_i} \rangle_i(j) = \text{comp}\,G(j)$.

The functor $\langle 0_{G_i} \rangle_i$ yielding an element of $\prod \overline{G}$ is defined by:

(Def. 7)   For every element j of $\text{dom}\,\overline{G}$ holds $\langle 0_{G_i} \rangle_i(j) =$ the zero of $G(j)$.

The functor $\text{multop}\,G$ yields a multi-operation of $\mathbb{R}$ and $\overline{G}$ and is defined by:

(Def. 8) $\text{len}\,\text{multop}\,G = \text{len}\,\overline{G}$ and for every element j of $\text{dom}\,\overline{G}$ holds $(\text{multop}\,G)(j) =$ the external multiplication of $G(j)$.

Let G be a real linear space-sequence. The functor $\prod G$ yielding a strict non empty RLS structure is defined by:

(Def. 9) $\prod G = \langle \prod \overline{G}, \langle 0_{G_i} \rangle_i, \prod^\circ(\langle +_{G_i} \rangle_i), \prod^\circ \text{multop}\,G \rangle$.

Let G be a real linear space-sequence. One can check that $\prod G$ is Abelian, add-associative, right zeroed, right complementable, and real linear space-like.

2. The Product Space of Real Normed Spaces

Let R be a binary relation. We say that R is real-norm-space-yielding if and only if:

(Def. 10)   For every set x such that $x \in \text{rng}\,R$ holds x is a real normed space.

One can check that there exists a finite sequence which is non empty and real-norm-space-yielding.

A real norm space-sequence is a non empty real-norm-space-yielding finite sequence.

Let G be a real norm space-sequence and let j be an element of $\text{dom}\,G$. Then $G(j)$ is a real normed space.

Let us note that every finite sequence which is real-norm-space-yielding is also real-linear-space-yielding.

Let G be a real norm space-sequence and let x be an element of $\prod \overline{G}$. The functor $\text{normsequence}(G, x)$ yields an element of $\mathcal{R}^{\text{len}\,G}$ and is defined as follows:

(Def. 11) $\text{len}\,\text{normsequence}(G, x) = \text{len}\,G$ and for every element j of $\text{dom}\,G$ holds $(\text{normsequence}(G, x))(j) = (\text{the norm of }G(j))(x(j))$.

Let G be a real norm space-sequence. The functor $\text{productnorm}\,G$ yields a function from $\prod (G \textbf{ qua }\text{real linear space-sequence})$ into $\mathbb{R}$ and is defined by:

(Def. 12)   For every element x of $\prod \overline{G}$ holds
$(\text{productnorm}\,G)(x) = |\,\text{normsequence}(G, x)\,|$.

Let G be a real norm space-sequence. The functor $\prod G$ yielding a strict non empty normed structure is defined as follows:

(Def. 13)   The RLS structure of $\prod G = \prod(G \textbf{ qua}$ real linear space-sequence) and the norm of $\prod G = \text{productnorm } G$.

In the sequel G is a real norm space-sequence.

We now state four propositions:

(6) $\prod G = \langle \prod \overline{G}, \langle 0_{G_i} \rangle_i, \prod^\circ(\langle +_{G_i} \rangle_i), \prod^\circ \text{multop } G, \text{productnorm } G \rangle$.

(7)   For every vector x of $\prod G$ and for every element y of $\prod \overline{G}$ such that $x = y$ holds $\|x\| = |\text{normsequence}(G, y)|$.

(8)   For all elements x, y, z of $\prod \overline{G}$ and for every element i of $\mathbb{N}$ such that $i \in \text{dom } x$ and $z = (\prod^\circ(\langle +_{G_i} \rangle_i))(x, y)$ holds $(\text{normsequence}(G, z))(i) \leq (\text{normsequence}(G, x) + \text{normsequence}(G, y))(i)$.

(9)   For every element x of $\prod \overline{G}$ and for every element i of $\mathbb{N}$ such that $i \in \text{dom } x$ holds $0 \leq (\text{normsequence}(G, x))(i)$.

Let G be a real norm space-sequence. Observe that $\prod G$ is real normed space-like, real linear space-like, Abelian, add-associative, right zeroed, and right complementable.

One can prove the following propositions:

(10)   Let G be a real norm space-sequence, i be an element of $\text{dom } G$, x be a point of $\prod G$, y be an element of $\prod \overline{G}$, and x_1 be a point of $G(i)$. If $y = x$ and $x_1 = y(i)$, then $\|x_1\| \leq \|x\|$.

(11)   Let G be a real norm space-sequence, i be an element of $\text{dom } G$, x, y be points of $\prod G$, x_1, y_1 be points of $G(i)$, and z_1, z_2 be elements of $\prod \overline{G}$. If $x_1 = z_1(i)$ and $z_1 = x$ and $y_1 = z_2(i)$ and $z_2 = y$, then $\|y_1 - x_1\| \leq \|y - x\|$.

(12)   Let G be a real norm space-sequence, s_1 be a sequence of $\prod G$, x_0 be a point of $\prod G$, and y_0 be an element of $\prod \overline{G}$. Suppose $x_0 = y_0$ and s_1 is convergent and $\lim s_1 = x_0$. Let i be an element of $\text{dom } G$. Then there exists a sequence s_2 of $G(i)$ such that s_2 is convergent and $y_0(i) = \lim s_2$ and for every element m of $\mathbb{N}$ there exists an element s_3 of $\prod \overline{G}$ such that $s_3 = s_1(m)$ and $s_2(m) = s_3(i)$.

(13)   Let G be a real norm space-sequence, s_1 be a sequence of $\prod G$, x_0 be a point of $\prod G$, and y_0 be an element of $\prod \overline{G}$. Suppose that

(i) $x_0 = y_0$, and

(ii)   for every element i of $\text{dom } G$ there exists a sequence s_2 of $G(i)$ such that s_2 is convergent and $y_0(i) = \lim s_2$ and for every element m of $\mathbb{N}$ there exists an element s_3 of $\prod \overline{G}$ such that $s_3 = s_1(m)$ and $s_2(m) = s_3(i)$. Then s_1 is convergent and $\lim s_1 = x_0$.

(14)   For every real norm space-sequence G such that for every element i of $\text{dom } G$ holds $G(i)$ is complete holds $\prod G$ is complete.

References

[1] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[5] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[11] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

[12] Jarosław Kotowicz. Convergent sequences and the limit of sequences. *Formalized Mathematics*, 1(**2**):273–275, 1990.

[13] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[15] Anna Lango and Grzegorz Bancerek. Product of families of groups and vector spaces. *Formalized Mathematics*, 3(**2**):235–240, 1992.

[16] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[17] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[18] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

[19] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[20] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[21] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[22] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[23] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Mizar Analysis of Algorithms: Preliminaries[1]

Grzegorz Bancerek
Department of Theoretical Computer Science
Białystok Technical University
Poland

Summary. Algorithms and its parts – instructions – are formalized as elements of if-while algebras. An if-while algebra is a (1-sorted) universal algebra which has 4 operations: a constant – the empty instruction, a binary catenation of instructions, a ternary conditional instruction, and a binary while instruction. An execution function is defined on pairs (s, I), where s is a state (an element of certain set of states) and I is an instruction, and results in states. The execution function obeys control structures using the set of distinguished true states, i.e. a condition instruction is executed and the continuation of execution depends on if the resulting state is in true states or not. Termination is also defined for pairs (s, I) and depends on the execution function. The existence of execution function determined on elementary instructions and its uniqueness for terminating instructions are shown.

MML identifier: `AOFA_000`, version: `7.8.05 4.84.971`

The articles [42], [26], [47], [36], [6], [45], [49], [22], [50], [25], [23], [19], [29], [28], [11], [34], [33], [20], [1], [5], [41], [21], [43], [12], [39], [4], [7], [8], [3], [31], [16], [30], [40], [24], [2], [15], [27], [48], [35], [18], [32], [37], [10], [14], [17], [9], [13], [44], [38], and [46] provide the terminology and notation for this paper.

1. BINARY OPERATIONS, ORBITS, AND ITERATIONS

(1) Let f, g, h be functions and A be a set. Suppose $A \subseteq \operatorname{dom} f$ and $A \subseteq \operatorname{dom} g$ and $\operatorname{rng} h \subseteq A$ and for every set x such that $x \in A$ holds $f(x) = g(x)$. Then $f \cdot h = g \cdot h$.

Let x, y be non empty sets. Observe that $\langle x, y \rangle$ is non-empty.

Let p, q be non-empty finite sequences. One can check that $p \frown q$ is non-empty.

Let f be a homogeneous function and let x be a set. We say that x is a unity w.r.t. f if and only if:

(Def. 1) For all sets y, z such that $\langle y, z \rangle \in \operatorname{dom} f$ or $\langle z, y \rangle \in \operatorname{dom} f$ holds $\langle x, y \rangle \in \operatorname{dom} f$ and $f(\langle x, y \rangle) = y$ and $\langle y, x \rangle \in \operatorname{dom} f$ and $f(\langle y, x \rangle) = y$.

Let f be a homogeneous function. We say that f is associative if and only if:

(Def. 2) For all sets x, y, z such that $\langle x, y \rangle \in \operatorname{dom} f$ and $\langle y, z \rangle \in \operatorname{dom} f$ and $\langle f(\langle x, y \rangle), z \rangle \in \operatorname{dom} f$ and $\langle x, f(\langle y, z \rangle) \rangle \in \operatorname{dom} f$ holds $f(\langle f(\langle x, y \rangle), z \rangle) = f(\langle x, f(\langle y, z \rangle) \rangle)$.

We say that f is unital if and only if:

(Def. 3) There exists a set which is a unity w.r.t. f.

Let X be a set, let Y be a non empty set, let Z be a set of finite sequences of X, and let y be an element of Y. Then $Z \longmapsto y$ is a partial function from X^* to Y.

Let X be a non empty set, let x be an element of X, and let n be a natural number. Observe that $X^n \longmapsto x$ is non empty, quasi total, and homogeneous.

One can prove the following proposition

(2) For every non empty set X and for every element x of X and for every natural number n holds $\operatorname{arity}(X^n \longmapsto x) = n$.

Let X be a non empty set and let x be an element of X. One can check the following observations:

∗ $X^0 \longmapsto x$ is nullary,

∗ $X^1 \longmapsto x$ is unary,

∗ $X^2 \longmapsto x$ is binary, and

∗ $X^3 \longmapsto x$ is ternary.

Let X be a non empty set. One can check the following observations:

∗ there exists a non empty quasi total homogeneous partial function from X^* to X which is binary, associative, and unital,

∗ there exists a non empty quasi total homogeneous partial function from X^* to X which is nullary, and

∗   there exists a non empty quasi total homogeneous partial function from X^* to X which is ternary.

Next we state the proposition

(3)   Let X be a non empty set, p be a finite sequence of elements of FinTrees(X), and x, t be sets. If $t \in \operatorname{rng} p$, then $t \neq x\text{-tree}(p)$.

Let f, g be functions and let X be a set. The functor $f+\cdot^X g$ yields a function and is defined as follows:

(Def. 4) $f+\cdot^X g = g+\cdot f{\restriction}X$.

We now state two propositions:

(4)   For all functions f, g and for all sets x, X such that $x \in X$ and $X \subseteq \operatorname{dom} f$ holds $(f+\cdot^X g)(x) = f(x)$.

(5)   For all functions f, g and for all sets x, X such that $x \notin X$ and $x \in \operatorname{dom} g$ holds $(f+\cdot^X g)(x) = g(x)$.

Let X, Y be non empty sets, let f, g be elements of Y^X, and let A be a set. Then $f+\cdot^A g$ is an element of Y^X.

Let X, Y, Z be non empty sets, let f be an element of Y^X, and let g be an element of Z^Y. Then $g \cdot f$ is an element of Z^X.

Let f be a function and let x be a set. The functor $f\text{-orbit}(x)$ is defined by:

(Def. 5) $f\text{-orbit}(x) = \{f^n(x); n \text{ ranges over elements of } \mathbb{N}: x \in \operatorname{dom}(f^n)\}$.

We now state four propositions:

(6)   For every function f and for every set x such that $x \in \operatorname{dom} f$ holds $x \in f\text{-orbit}(x)$.

(7)   For every function f and for all sets x, y such that $\operatorname{rng} f \subseteq \operatorname{dom} f$ and $y \in f\text{-orbit}(x)$ holds $f(y) \in f\text{-orbit}(x)$.

(8)   For every function f and for every set x such that $x \in \operatorname{dom} f$ holds $f(x) \in f\text{-orbit}(x)$.

(9)   For every function f and for every set x such that $x \in \operatorname{dom} f$ and $f(x) \in \operatorname{dom} f$ holds $f\text{-orbit}(f(x)) \subseteq f\text{-orbit}(x)$.

Let f be a function. Let us assume that $\operatorname{rng} f \subseteq \operatorname{dom} f$. Let A be a set and let x be a set. The functor $f^*_{A \to x}$ yielding a function is defined by the conditions (Def. 6).

(Def. 6)(i) $\operatorname{dom}(f^*_{A \to x}) = \operatorname{dom} f$, and

(ii)   for every set a such that $a \in \operatorname{dom} f$ holds if $f\text{-orbit}(a) \subseteq A$, then $f^*_{A \to x}(a) = x$ and for every natural number n such that $f^n(a) \notin A$ and for every natural number i such that $i < n$ holds $f^i(a) \in A$ holds $f^*_{A \to x}(a) = f^n(a)$.

Let f be a function. Let us assume that $\operatorname{rng} f \subseteq \operatorname{dom} f$. Let A be a set and let g be a function. The functor $f^*_{A \to g}$ yields a function and is defined by the conditions (Def. 7).

(Def. 7)(i) $\dom(f^*_{A\to g}) = \dom f$, and

    (ii)   for every set a such that $a \in \dom f$ holds if f-orbit$(a) \subseteq A$, then $f^*_{A\to g}(a) = g(a)$ and for every natural number n such that $f^n(a) \notin A$ and for every natural number i such that $i < n$ holds $f^i(a) \in A$ holds $f^*_{A\to g}(a) = f^n(a)$.

The following propositions are true:

(10)   Let f, g be functions and a, A be sets. Suppose $\rng f \subseteq \dom f$ and $a \in \dom f$. Suppose f-orbit$(a) \nsubseteq A$. Then there exists a natural number n such that $f^*_{A\to g}(a) = f^n(a)$ and $f^n(a) \notin A$ and for every natural number i such that $i < n$ holds $f^i(a) \in A$.

(11)   Let f, g be functions and a, A be sets. If $\rng f \subseteq \dom f$ and $a \in \dom f$ and $g \cdot f = g$, then if $a \in A$, then $f^*_{A\to g}(a) = f^*_{A\to g}(f(a))$.

(12)   For all functions f, g and for all sets a, A such that $\rng f \subseteq \dom f$ and $a \in \dom f$ holds if $a \notin A$, then $f^*_{A\to g}(a) = a$.

Let X be a non empty set, let f be an element of X^X, let A be a set, and let g be an element of X^X. Then $f^*_{A\to g}$ is an element of X^X.

2. Free Universal Algebras

We now state three propositions:

(13)   Let X be a non empty set and S be a non empty finite sequence of elements of $\mathbb{N}$. Then there exists a universal algebra A such that the carrier of $A = X$ and signature $A = S$.

(14)   Let S be a non empty finite sequence of elements of $\mathbb{N}$. Then there exists a universal algebra A such that

    (i)   the carrier of $A = \mathbb{N}$,

    (ii)   signature $A = S$, and

    (iii)   for all natural numbers i, j such that $i \in \dom S$ and $j = S(i)$ holds (the characteristic of $A)(i) = \mathbb{N}^j \longmapsto i$.

(15)   Let S be a non empty finite sequence of elements of $\mathbb{N}$ and i, j be natural numbers. Suppose $i \in \dom S$ and $j = S(i)$. Let X be a non empty set and f be a function from X^j into X. Then there exists a universal algebra A such that the carrier of $A = X$ and signature $A = S$ and (the characteristic of $A)(i) = f$.

Let f be a non empty finite sequence of elements of $\mathbb{N}$ and let D be a non empty missing $\mathbb{N}$ set. Observe that every element of FreeUnivAlgNSG(f, D) is relation-like and function-like.

Let f be a non empty finite sequence of elements of $\mathbb{N}$ and let D be a non empty missing $\mathbb{N}$ set. One can verify that every element of FreeUnivAlgNSG(f, D)

is decorated tree-like and every finite sequence of elements of $\text{FreeUnivAlgNSG}(f, D)$ is decorated tree yielding.

We now state two propositions:

(16) Let G be a non empty tree construction structure and t be a set. Suppose $t \in \text{TS}(G)$. Then

(i) there exists a symbol d of G such that $d \in$ the terminals of G and $t = $ the root tree of d, or

(ii) there exists a symbol o of G and there exists a finite sequence p of elements of $\text{TS}(G)$ such that $o \Rightarrow$ the roots of p and $t = o\text{-tree}(p)$.

(17) Let X be a missing $\mathbb{N}$ non empty set, S be a non empty finite sequence of elements of $\mathbb{N}$, and i be a natural number. Suppose $i \in \text{dom}\, S$. Let p be a finite sequence of elements of $\text{FreeUnivAlgNSG}(S, X)$. If $\text{len}\, p = S(i)$, then $(\text{Den}(i(\in \text{dom}\,(\text{the characteristic of } \text{FreeUnivAlgNSG}(S, X))), \text{FreeUnivAlgNSG}(S, X)))(p) = i\text{-tree}(p)$.

Let A be a non-empty universal algebra structure, let B be a subset of A, and let n be a natural number. The functor B^n yielding a subset of A is defined by the condition (Def. 8).

(Def. 8) There exists a function F from $\mathbb{N}$ into $2^{\text{the carrier of } A}$ such that

(i) $B^n = F(n)$,

(ii) $F(0) = B$, and

(iii) for every natural number n holds $F(n+1) = F(n) \cup \{(\text{Den}(o, A))(p); o$ ranges over elements of $\text{dom}\,(\text{the characteristic of } A)$, p ranges over elements of $(\text{the carrier of } A)^*$: $p \in \text{dom}\,\text{Den}(o, A) \wedge \text{rng}\, p \subseteq F(n)\}$.

Next we state several propositions:

(18) For every universal algebra A and for every subset B of A holds $B^0 = B$.

(19) Let A be a universal algebra, B be a subset of A, and n be a natural number. Then $B^{n+1} = B^n \cup \{(\text{Den}(o, A))(p); o$ ranges over elements of $\text{dom}\,(\text{the characteristic of } A)$, p ranges over elements of $(\text{the carrier of } A)^*$: $p \in \text{dom}\,\text{Den}(o, A) \wedge \text{rng}\, p \subseteq B^n\}$.

(20) Let A be a universal algebra, B be a subset of A, n be a natural number, and x be a set. Then $x \in B^{n+1}$ if and only if one of the following conditions is satisfied:

(i) $x \in B^n$, or

(ii) there exists an element o of $\text{dom}\,(\text{the characteristic of } A)$ and there exists an element p of $(\text{the carrier of } A)^*$ such that $x = (\text{Den}(o, A))(p)$ and $p \in \text{dom}\,\text{Den}(o, A)$ and $\text{rng}\, p \subseteq B^n$.

(21) Let A be a universal algebra, B be a subset of A, and n, m be natural numbers. If $n \leq m$, then $B^n \subseteq B^m$.

(22) Let A be a universal algebra and B_1, B_2 be subsets of A. If $B_1 \subseteq B_2$, then for every natural number n holds $B_1{}^n \subseteq B_2{}^n$.

(23) Let A be a universal algebra, B be a subset of A, n be a natural number, and x be a set. Then $x \in B^{n+1}$ if and only if one of the following conditions is satisfied:

(i) $x \in B$, or

(ii) there exists an element o of dom (the characteristic of A) and there exists an element p of (the carrier of $A)^*$ such that $x = (\mathrm{Den}(o, A))(p)$ and $p \in \mathrm{dom}\,\mathrm{Den}(o, A)$ and $\mathrm{rng}\,p \subseteq B^n$.

The scheme *MaxVal* deals with a non empty set $\mathcal{A}$, a set $\mathcal{B}$, and a binary predicate $\mathcal{P}$, and states that:

There exists a natural number n such that for every element x of $\mathcal{A}$ such that $x \in \mathcal{B}$ holds $\mathcal{P}[x, n]$

provided the following conditions are satisfied:

- $\mathcal{B}$ is finite,
- For every element x of $\mathcal{A}$ such that $x \in \mathcal{B}$ there exists a natural number n such that $\mathcal{P}[x, n]$, and
- For every element x of $\mathcal{A}$ and for all natural numbers n, m such that $\mathcal{P}[x, n]$ and $n \leq m$ holds $\mathcal{P}[x, m]$.

We now state two propositions:

(24) Let A be a universal algebra and B be a subset of A. Then there exists a subset C of A such that $C = \bigcup\{B^n : n \text{ ranges over elements of } \mathbb{N}\}$ and C is operations closed.

(25) Let A be a universal algebra and B, C be subsets of A. Suppose C is operations closed and $B \subseteq C$. Then $\bigcup\{B^n : n \text{ ranges over elements of } \mathbb{N}\} \subseteq C$.

Let A be a universal algebra. The functor Generators A yielding a subset of A is defined by:

(Def. 9) Generators $A = $ (the carrier of A) $\setminus \bigcup\{\mathrm{rng}\,o : o \text{ ranges over elements of } \mathrm{Operations}(A)\}$.

Next we state several propositions:

(26) Let A be a universal algebra and a be an element of A. Then $a \in$ Generators A if and only if it is not true that there exists an element o of $\mathrm{Operations}(A)$ such that $a \in \mathrm{rng}\,o$.

(27) For every universal algebra A and for every subset B of A such that B is operations closed holds $\mathrm{Constants}(A) \subseteq B$.

(28) For every universal algebra A such that $\mathrm{Constants}(A) = \emptyset$ holds $\emptyset_A$ is operations closed.

(29) For every universal algebra A such that $\mathrm{Constants}(A) = \emptyset$ and for every generator set G of A holds $G \neq \emptyset$.

(30) Let A be a universal algebra and G be a subset of A. Then G is a generator set of A if and only if for every element I of A there exists a

natural number n such that $I \in G^n$.

(31) Let A be a universal algebra, B be a subset of A, and G be a generator set of A. If $G \subseteq B$, then B is a generator set of A.

(32) Let A be a universal algebra, G be a generator set of A, and a be an element of A. If it is not true that there exists an element o of Operations(A) such that $a \in \operatorname{rng} o$, then $a \in G$.

(33) For every universal algebra A and for every generator set G of A holds Generators $A \subseteq G$.

(34) For every free universal algebra A and for every free generator set G of A holds $G = $ Generators A.

Let A be a free universal algebra. Note that Generators A is free.

Let A be a free universal algebra. Then Generators A is a generator set of A.

Let A, B be sets. Note that $[\![A, B]\!]$ is missing $\mathbb{N}$.

One can prove the following propositions:

(35) Let A be a free universal algebra, G be a generator set of A, B be a universal algebra, and h_1, h_2 be functions from A into B. Suppose h_1 is a homomorphism of A into B and h_2 is a homomorphism of A into B and $h_1 \upharpoonright G = h_2 \upharpoonright G$. Then $h_1 = h_2$.

(36) Let A be a free universal algebra, o_1, o_2 be operation symbols of A, and p_1, p_2 be finite sequences. If $p_1 \in \operatorname{dom} \operatorname{Den}(o_1, A)$ and $p_2 \in \operatorname{dom} \operatorname{Den}(o_2, A)$, then if $(\operatorname{Den}(o_1, A))(p_1) = (\operatorname{Den}(o_2, A))(p_2)$, then $o_1 = o_2$ and $p_1 = p_2$.

(37) Let A be a free universal algebra, o_1, o_2 be elements of Operations(A), and p_1, p_2 be finite sequences. If $p_1 \in \operatorname{dom} o_1$ and $p_2 \in \operatorname{dom} o_2$, then if $o_1(p_1) = o_2(p_2)$, then $o_1 = o_2$ and $p_1 = p_2$.

(38) Let A be a free universal algebra, o be an operation symbol of A, and p be a finite sequence. If $p \in \operatorname{dom} \operatorname{Den}(o, A)$, then for every set a such that $a \in \operatorname{rng} p$ holds $a \neq (\operatorname{Den}(o, A))(p)$.

(39) Let A be a free universal algebra, G be a generator set of A, and o be an operation symbol of A. Suppose that for every operation symbol o' of A and for every finite sequence p such that $p \in \operatorname{dom} \operatorname{Den}(o', A)$ and $(\operatorname{Den}(o', A))(p) \in G$ holds $o' \neq o$. Let p be a finite sequence. Suppose $p \in \operatorname{dom} \operatorname{Den}(o, A)$. Let n be a natural number. If $(\operatorname{Den}(o, A))(p) \in G^{n+1}$, then $\operatorname{rng} p \subseteq G^n$.

(40) Let A be a free universal algebra, o be an operation symbol of A, and p be a finite sequence. Suppose $p \in \operatorname{dom} \operatorname{Den}(o, A)$. Let n be a natural number. If $(\operatorname{Den}(o, A))(p) \in (\text{Generators } A)^{n+1}$, then $\operatorname{rng} p \subseteq (\text{Generators } A)^n$.

3. IF-WHILE ALGEBRA

Let S be a non empty universal algebra structure. We say that S has empty-instruction if and only if the conditions (Def. 10) are satisfied.

(Def. 10)(i) $1 \in \operatorname{dom}$ (the characteristic of S), and

(ii) (the characteristic of S)(1) is a nullary non empty homogeneous quasi total partial function from (the carrier of S)* to the carrier of S.

We say that S has catenation if and only if the conditions (Def. 11) are satisfied.

(Def. 11)(i) $2 \in \operatorname{dom}$ (the characteristic of S), and

(ii) (the characteristic of S)(2) is a binary non empty homogeneous quasi total partial function from (the carrier of S)* to the carrier of S.

We say that S has if-instruction if and only if the conditions (Def. 12) are satisfied.

(Def. 12)(i) $3 \in \operatorname{dom}$ (the characteristic of S), and

(ii) (the characteristic of S)(3) is a ternary non empty homogeneous quasi total partial function from (the carrier of S)* to the carrier of S.

We say that S has while-instruction if and only if the conditions (Def. 13) are satisfied.

(Def. 13)(i) $4 \in \operatorname{dom}$ (the characteristic of S), and

(ii) (the characteristic of S)(4) is a binary non empty homogeneous quasi total partial function from (the carrier of S)* to the carrier of S.

We say that S is associative if and only if the condition (Def. 14) is satisfied.

(Def. 14) (The characteristic of S)(2) is a binary associative non empty homogeneous quasi total partial function from (the carrier of S)* to the carrier of S.

Let S be a non-empty universal algebra structure. We say that S is unital if and only if the condition (Def. 15) is satisfied.

(Def. 15) There exists a binary non empty homogeneous quasi total partial function f from (the carrier of S)* to the carrier of S such that $f = $ (the characteristic of S)(2) and $(\operatorname{Den}(1(\in \operatorname{dom}$ (the characteristic of S)), S))(\emptyset)$ is a unity w.r.t. f.

One can prove the following proposition

(41) Let X be a non empty set, x be an element of X, and c be a binary associative unital non empty quasi total homogeneous partial function from X^* to X. Suppose x is a unity w.r.t. c. Let i be a ternary non empty quasi total homogeneous partial function from X^* to X and w be a binary non empty quasi total homogeneous partial function from X^* to X. Then there exists a non-empty strict universal algebra structure S such that

(i) the carrier of $S = X$,

(ii)   the characteristic of $S = \langle X^0 \longmapsto x, c \rangle ^\frown \langle i, w \rangle$, and

(iii) S is unital, associative, quasi total, and partial and has empty-instruction, catenation, if-instruction, and while-instruction.

Let us note that there exists a quasi total partial non-empty strict universal algebra structure which is unital and associative and has empty-instruction, catenation, if-instruction, and while-instruction.

A pre-if-while algebra is a universal algebra with empty-instruction, catenation, if-instruction, and while-instruction.

For simplicity, we use the following convention: A is a pre-if-while algebra, C, I, J are elements of A, S is a non empty set, T is a subset of S, and s is an element of S.

Let A be a non empty universal algebra structure. An algorithm of A is an element of A.

The following proposition is true

(42)   Let A be a non-empty universal algebra structure with empty-instruction. Then $\operatorname{dom} \operatorname{Den}(1(\in \operatorname{dom}(\text{the characteristic of } A)), A) = \{\emptyset\}$.

Let A be a non-empty universal algebra structure with empty-instruction. The functor $\operatorname{EmptyIns}_A$ yielding an algorithm of A is defined as follows:

(Def. 16) $\operatorname{EmptyIns}_A = (\operatorname{Den}(1(\in \operatorname{dom}(\text{the characteristic of } A)), A))(\emptyset)$.

The following two propositions are true:

(43)   Let A be a universal algebra with empty-instruction and o be an element of $\operatorname{Operations}(A)$. If $o = \operatorname{Den}(1(\in \operatorname{dom}(\text{the characteristic of } A)), A)$, then arity $o = 0$ and $\operatorname{EmptyIns}_A \in \operatorname{rng} o$.

(44)   Let A be a non-empty universal algebra structure with catenation. Then $\operatorname{dom} \operatorname{Den}(2(\in \operatorname{dom}(\text{the characteristic of } A)), A) = (\text{the carrier of } A)^2$.

Let A be a non-empty universal algebra structure with catenation and let I_1, I_2 be algorithms of A. The functor $I_1; I_2$ yielding an algorithm of A is defined as follows:

(Def. 17) $I_1; I_2 = (\operatorname{Den}(2(\in \operatorname{dom}(\text{the characteristic of } A)), A))(\langle I_1, I_2 \rangle)$.

The following propositions are true:

(45)   Let A be a unital non-empty universal algebra structure with empty-instruction and catenation and I be an element of A. Then $\operatorname{EmptyIns}_A; I = I$ and $I; \operatorname{EmptyIns}_A = I$.

(46)   Let A be an associative non-empty universal algebra structure with catenation and I_1, I_2, I_3 be elements of A. Then $(I_1; I_2); I_3 = I_1; (I_2; I_3)$.

(47)   Let A be a non-empty universal algebra structure with if-instruction. Then $\operatorname{dom} \operatorname{Den}(3(\in \operatorname{dom}(\text{the characteristic of } A)), A) = (\text{the carrier of } A)^3$.

Let A be a non-empty universal algebra structure with if-instruction and let C, I_1, I_2 be algorithms of A. The functor if C then I_1 else I_2 yields an algorithm

of A and is defined as follows:

(Def. 18)   if C then I_1 else $I_2 = (\mathrm{Den}(3(\in \mathrm{dom}\,(\text{the characteristic of } A)), A))(\langle C, I_1, I_2 \rangle)$.

Let A be a non-empty universal algebra structure with empty-instruction and if-instruction and let C, I be algorithms of A. The functor if C then I yields an algorithm of A and is defined as follows:

(Def. 19)   if C then $I =$ if C then I else $(\mathrm{EmptyIns}_A)$.

We now state the proposition

(48)   Let A be a non-empty universal algebra structure with while-instruction. Then $\mathrm{dom}\,\mathrm{Den}(4(\in \mathrm{dom}\,(\text{the characteristic of } A)), A) = (\text{the carrier of } A)^2$.

Let A be a non-empty universal algebra structure with while-instruction and let C, I be algorithms of A. The functor while C do I yields an algorithm of A and is defined as follows:

(Def. 20)   while C do $I = (\mathrm{Den}(4(\in \mathrm{dom}\,(\text{the characteristic of } A)), A))(\langle C, I \rangle)$.

Let A be a pre-if-while algebra and let I_0, C, I, J be elements of A. The functor for I_0 until C step J do I yields an element of A and is defined by:

(Def. 21)   for I_0 until C step J do $I = I_0$; while C do $(I; J)$.

Let A be a pre-if-while algebra. The functor $\mathrm{ElementaryInstructions}_A$ yields a subset of A and is defined by the condition (Def. 22).

(Def. 22) $\mathrm{ElementaryInstructions}_A = (\text{the carrier of } A) \setminus \{\mathrm{EmptyIns}_A\} \setminus \mathrm{rng}\,\mathrm{Den}(3(\in \mathrm{dom}\,(\text{the characteristic of } A)), A) \setminus \mathrm{rng}\,\mathrm{Den}(4(\in \mathrm{dom}\,(\text{the characteristic of } A)), A) \setminus \{I_1; I_2; I_1 \text{ ranges over algorithms of } A, I_2 \text{ ranges over algorithms of } A: I_1 \neq I_1; I_2 \wedge I_2 \neq I_1; I_2\}$.

Next we state several propositions:

(49)   For every pre-if-while algebra A holds $\mathrm{EmptyIns}_A \notin \mathrm{ElementaryInstructions}_A$.

(50)   For every pre-if-while algebra A and for all elements I_1, I_2 of A such that $I_1 \neq I_1; I_2$ and $I_2 \neq I_1; I_2$ holds $I_1; I_2 \notin \mathrm{ElementaryInstructions}_A$.

(51)   For every pre-if-while algebra A and for all elements C, I_1, I_2 of A holds if C then I_1 else $I_2 \notin \mathrm{ElementaryInstructions}_A$.

(52)   For every pre-if-while algebra A and for all elements C, I of A holds while C do $I \notin \mathrm{ElementaryInstructions}_A$.

(53)   Let A be a pre-if-while algebra and I be an element of A. Suppose $I \notin \mathrm{ElementaryInstructions}_A$. Then

(i) $I = \mathrm{EmptyIns}_A$, or

(ii)   there exist elements I_1, I_2 of A such that $I = I_1; I_2$ and $I_1 \neq I_1; I_2$ and $I_2 \neq I_1; I_2$, or

(iii)   there exist elements C, I_1, I_2 of A such that $I =$ if C then I_1 else I_2, or

(iv) there exist elements C, J of A such that $I = $ while C do J.

Let A be a pre-if-while algebra. We say that A is infinite if and only if:

(Def. 23) ElementaryInstructions$_A$ is infinite.

We say that A is degenerated if and only if the conditions (Def. 24) are satisfied.

(Def. 24)(i) There exist elements I_1, I_2 of A such that $I_1 \neq $ EmptyIns$_A$ and $I_1; I_2 = I_2$ or $I_2 \neq $ EmptyIns$_A$ and $I_1; I_2 = I_1$ or $I_1 \neq $ EmptyIns$_A$ or $I_2 \neq $ EmptyIns$_A$ but $I_1; I_2 = $ EmptyIns$_A$, or

(ii) there exist elements C, I_1, I_2 of A such that if C then I_1 else $I_2 = $ EmptyIns$_A$, or

(iii) there exist elements C, I of A such that while C do $I = $ EmptyIns$_A$, or

(iv) there exist elements I_1, I_2, C, J_1, J_2 of A such that $I_1 \neq $ EmptyIns$_A$ and $I_2 \neq $ EmptyIns$_A$ and $I_1; I_2 = $ if C then J_1 else J_2, or

(v) there exist elements I_1, I_2, C, J of A such that $I_1 \neq $ EmptyIns$_A$ and $I_2 \neq $ EmptyIns$_A$ and $I_1; I_2 = $ while C do J, or

(vi) there exist elements C_1, I_1, I_2, C_2, J of A such that if C_1 then I_1 else $I_2 = $ while C_2 do J.

We say that A is well founded if and only if:

(Def. 25) ElementaryInstructions$_A$ is a generator set of A.

The non empty finite sequence ECIW-signature of elements of $\mathbb{N}$ is defined by:

(Def. 26) ECIW-signature $= \langle 0, 2 \rangle \frown \langle 3, 2 \rangle$.

We now state the proposition

(54) len ECIW-signature $= 4$ and dom ECIW-signature $= $ Seg 4 and (ECIW-signature)(1) $= 0$ and (ECIW-signature)(2) $= 2$ and (ECIW-signature)(3) $= 3$ and (ECIW-signature)(4) $= 2$.

Let A be a partial non-empty non empty universal algebra structure. We say that A is E.C.I.W.-strict if and only if:

(Def. 27) signature $A = $ ECIW-signature.

Next we state the proposition

(55) Let A be a partial non-empty non empty universal algebra structure. Suppose A is E.C.I.W.-strict. Let o be an operation symbol of A. Then $o = 1$ or $o = 2$ or $o = 3$ or $o = 4$.

Let X be a missing $\mathbb{N}$ non empty set. One can verify that FreeUnivAlgNSG(ECIW-signature, X) has empty-instruction, catenation, if-instruction, and while-instruction.

We now state a number of propositions:

(56) Let X be a missing $\mathbb{N}$ non empty set and I be an element of FreeUnivAlgNSG(ECIW-signature, X). Then

(i) there exists an element x of X such that $I = $ the root tree of x, or

(ii)   there exists a natural number n and there exists a finite sequence p of elements of FreeUnivAlgNSG(ECIW-signature, X) such that $n \in \operatorname{Seg} 4$ and $I = n\text{-tree}(p)$ and $\operatorname{len} p = (\text{ECIW-signature})(n)$.

(57)   For every missing $\mathbb{N}$ non empty set X holds
$$\text{EmptyIns}_{\text{FreeUnivAlgNSG(ECIW-signature},X)} = 1\text{-tree}(\emptyset).$$

(58)   Let X be a missing $\mathbb{N}$ non empty set and p be a finite sequence of elements of FreeUnivAlgNSG(ECIW-signature, X). If $1\text{-tree}(p)$ is an element of FreeUnivAlgNSG(ECIW-signature, X), then $p = \emptyset$.

(59)   For every missing $\mathbb{N}$ non empty set X and for all elements I_1, I_2 of FreeUnivAlgNSG(ECIW-signature, X) holds $I_1; I_2 = 2\text{-tree}(I_1, I_2)$.

(60)   Let X be a missing $\mathbb{N}$ non empty set and p be a finite sequence of elements of FreeUnivAlgNSG(ECIW-signature, X). Suppose $2\text{-tree}(p)$ is an element of FreeUnivAlgNSG(ECIW-signature, X). Then there exist elements I_1, I_2 of FreeUnivAlgNSG(ECIW-signature, X) such that $p = \langle I_1, I_2 \rangle$.

(61)   For every missing $\mathbb{N}$ non empty set X and for all elements I_1, I_2 of FreeUnivAlgNSG(ECIW-signature, X) holds $I_1; I_2 \neq I_1$ and $I_1; I_2 \neq I_2$.

(62)   Let X be a missing $\mathbb{N}$ non empty set and I_1, I_2, J_1, J_2 be elements of FreeUnivAlgNSG(ECIW-signature, X). If $I_1; I_2 = J_1; J_2$, then $I_1 = J_1$ and $I_2 = J_2$.

(63)   For every missing $\mathbb{N}$ non empty set X and for all elements C, I_1, I_2 of FreeUnivAlgNSG(ECIW-signature, X) holds if C then I_1 else $I_2 = 3\text{-tree}(\langle C, I_1, I_2 \rangle)$.

(64)   Let X be a missing $\mathbb{N}$ non empty set and p be a finite sequence of elements of FreeUnivAlgNSG(ECIW-signature, X). Suppose $3\text{-tree}(p)$ is an element of FreeUnivAlgNSG(ECIW-signature, X). Then there exist elements C, I_1, I_2 of FreeUnivAlgNSG(ECIW-signature, X) such that $p = \langle C, I_1, I_2 \rangle$.

(65)   Let X be a missing $\mathbb{N}$ non empty set and C_1, C_2, I_1, I_2, J_1, J_2 be elements of FreeUnivAlgNSG(ECIW-signature, X). If if C_1 then I_1 else $I_2 = $ if C_2 then J_1 else J_2, then $C_1 = C_2$ and $I_1 = J_1$ and $I_2 = J_2$.

(66)   For every missing $\mathbb{N}$ non empty set X and for all elements C, I of FreeUnivAlgNSG(ECIW-signature, X) holds while C do $I = 4\text{-tree}(C, I)$.

(67)   Let X be a missing $\mathbb{N}$ non empty set and p be a finite sequence of elements of FreeUnivAlgNSG(ECIW-signature, X). Suppose $4\text{-tree}(p)$ is an element of FreeUnivAlgNSG(ECIW-signature, X).
Then there exist elements C, I of FreeUnivAlgNSG(ECIW-signature, X) such that $p = \langle C, I \rangle$.

(68)   Let X be a missing $\mathbb{N}$ non empty set and I be an element of FreeUnivAlgNSG(ECIW-signature, X).
If $I \in \text{ElementaryInstructions}_{\text{FreeUnivAlgNSG(ECIW-signature},X)}$, then there exists an element x of X such that $I = x\text{-tree}(\emptyset)$.

(69) Let X be a missing $\mathbb{N}$ non empty set, p be a finite sequence of elements of FreeUnivAlgNSG(ECIW-signature, X), and x be an element of X. If x--tree(p) is an element of FreeUnivAlgNSG(ECIW-signature, X), then $p=\emptyset$.

(70) For every missing $\mathbb{N}$ non empty set X holds

ElementaryInstructions$_{\text{FreeUnivAlgNSG(ECIW-signature},X)}$ =
FreeGenSetNSG(ECIW-signature, X) and
$\overline{\overline{X}} = \overline{\overline{\text{FreeGenSetNSG(ECIW-signature}, X)}}$.

Let us observe that there exists a set which is infinite and missing $\mathbb{N}$.

Let X be an infinite missing $\mathbb{N}$ set. One can check that FreeUnivAlgNSG(ECIW-signature, X) is infinite.

Let X be a missing $\mathbb{N}$ non empty set. Note that FreeUnivAlgNSG (ECIW-signature, X) is E.C.I.W.-strict.

The following propositions are true:

(71) For every pre-if-while algebra A holds
Generators $A \subseteq$ ElementaryInstructions$_A$.

(72) Let A be a pre-if-while algebra. Suppose A is free. Let C, I_1, I_2 be elements of A. Then EmptyIns$_A \neq I_1; I_2$ and EmptyIns$_A \neq$ if C then I_1 else I_2 and EmptyIns$_A \neq$ while C do I_1.

(73) Let A be a pre-if-while algebra. Suppose A is free. Let I_1, I_2, C, J_1, J_2 be elements of A. Then $I_1; I_2 \neq I_1$ and $I_1; I_2 \neq I_2$ and if $I_1; I_2 = J_1; J_2$, then $I_1 = J_1$ and $I_2 = J_2$ and $I_1; I_2 \neq$ if C then J_1 else J_2 and $I_1; I_2 \neq$ while C do J_1.

(74) Let A be a pre-if-while algebra. Suppose A is free. Let C, I_1, I_2, D, J_1, J_2 be elements of A. Then if C then I_1 else $I_2 \neq C$ and if C then I_1 else $I_2 \neq I_1$ and if C then I_1 else $I_2 \neq I_2$ and if C then I_1 else $I_2 \neq$ while D do J_1 and if if C then I_1 else $I_2 =$ if D then J_1 else J_2, then $C = D$ and $I_1 = J_1$ and $I_2 = J_2$.

(75) Let A be a pre-if-while algebra. Suppose A is free. Let C, I, D, J be elements of A. Then while C do $I \neq C$ and while C do $I \neq I$ and if while C do $I =$ while D do J, then $C = D$ and $I = J$.

Let us note that every pre-if-while algebra which is free is also well founded and non degenerated.

Let us mention that there exists a pre-if-while algebra which is infinite, non degenerated, well founded, E.C.I.W.-strict, free, and strict.

An if-while algebra is a non degenerated well founded E.C.I.W.-strict pre-if-while algebra.

Let A be an infinite pre-if-while algebra.

Observe that ElementaryInstructions$_A$ is infinite.

One can prove the following four propositions:

(76) Let A be a pre-if-while algebra, B be a subset of A, and n be a natural number. Then

(i) $\mathrm{EmptyIns}_A \in B^{n+1}$, and

(ii)   for all elements C, I_1, I_2 of A such that $C \in B^n$ and $I_1 \in B^n$ and $I_2 \in B^n$ holds $I_1; I_2 \in B^{n+1}$ and if C then I_1 else $I_2 \in B^{n+1}$ and while C do $I_1 \in B^{n+1}$.

(77) Let A be an E.C.I.W.-strict pre-if-while algebra, x be a set, and n be a natural number. Suppose $x \in \mathrm{ElementaryInstructions}_A{}^{n+1}$. Then

(i) $x \in \mathrm{ElementaryInstructions}_A{}^n$, or

(ii) $x = \mathrm{EmptyIns}_A$, or

(iii) there exist elements I_1, I_2 of A such that $x = I_1; I_2$ and $I_1 \in \mathrm{ElementaryInstructions}_A{}^n$ and $I_2 \in \mathrm{ElementaryInstructions}_A{}^n$, or

(iv)   there exist elements C, I_1, I_2 of A such that $x = $ if C then I_1 else I_2 and $C \in \mathrm{ElementaryInstructions}_A{}^n$ and $I_1 \in \mathrm{ElementaryInstructions}_A{}^n$ and $I_2 \in \mathrm{ElementaryInstructions}_A{}^n$, or

(v)   there exist elements C, I of A such that $x = $ while C do I and $C \in \mathrm{ElementaryInstructions}_A{}^n$ and $I \in \mathrm{ElementaryInstructions}_A{}^n$.

(78) For every universal algebra A and for every subset B of A holds $\mathrm{Constants}(A) \subseteq B^1$.

(79) Let A be a pre-if-while algebra. Then A is well founded if and only if for every element I of A there exists a natural number n such that $I \in \mathrm{ElementaryInstructions}_A{}^n$.

The scheme *StructInd* deals with a well founded E.C.I.W.-strict pre-if-while algebra $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:
$$\mathcal{P}[\mathcal{B}]$$
provided the following conditions are satisfied:

- For every element I of $\mathcal{A}$ such that $I \in \mathrm{ElementaryInstructions}_\mathcal{A}$ holds $\mathcal{P}[I]$,
- $\mathcal{P}[\mathrm{EmptyIns}_\mathcal{A}]$,
- For all elements I_1, I_2 of $\mathcal{A}$ such that $\mathcal{P}[I_1]$ and $\mathcal{P}[I_2]$ holds $\mathcal{P}[I_1; I_2]$,
- For all elements C, I_1, I_2 of $\mathcal{A}$ such that $\mathcal{P}[C]$ and $\mathcal{P}[I_1]$ and $\mathcal{P}[I_2]$ holds $\mathcal{P}[$if C then I_1 else $I_2]$, and
- For all elements C, I of $\mathcal{A}$ such that $\mathcal{P}[C]$ and $\mathcal{P}[I]$ holds $\mathcal{P}[$while C do $I]$.

4. Execution Function

Let A be a pre-if-while algebra, let S be a non empty set, and let f be a function from $[\![S$, the carrier of $A]\!]$ into S. We say that f is complying-with-empty-instruction if and only if:

(Def. 28)   For every element s of S holds $f(s, \text{EmptyIns}_A) = s$.

We say that f is complying-with-catenation if and only if:

(Def. 29)   For every element s of S and for all elements I_1, I_2 of A holds $f(s, I_1; I_2) = f(f(s, I_1), I_2)$.

Let A be a pre-if-while algebra, let S be a non empty set, let T be a subset of S, and let f be a function from $[\!: S, \text{the carrier of } A :\!]$ into S. We say that f complies with **if** w.r.t. T if and only if the condition (Def. 30) is satisfied.

(Def. 30)   Let s be an element of S and C, I_1, I_2 be elements of A. Then
   (i)   if $f(s, C) \in T$, then $f(s, \text{if } C \text{ then } I_1 \text{ else } I_2) = f(f(s, C), I_1)$, and
   (ii)   if $f(s, C) \notin T$, then $f(s, \text{if } C \text{ then } I_1 \text{ else } I_2) = f(f(s, C), I_2)$.

We say that f complies with **while** w.r.t. T if and only if the condition (Def. 31) is satisfied.

(Def. 31)   Let s be an element of S and C, I be elements of A. Then
   (i)   if $f(s, C) \in T$, then $f(s, \text{while } C \text{ do } I) = f(f(f(s, C), I), \text{while } C \text{ do } I)$, and
   (ii)   if $f(s, C) \notin T$, then $f(s, \text{while } C \text{ do } I) = f(s, C)$.

One can prove the following two propositions:

(80)   Let f be a function from $[\!: S, \text{the carrier of } A :\!]$ into S. Suppose f is complying-with-empty-instruction and f complies with **if** w.r.t. T. Let s be an element of S. If $f(s, C) \notin T$, then $f(s, \text{if } C \text{ then } I) = f(s, C)$.

(81)(i) $\pi_1(S \times \text{the carrier of } A)$ is complying-with-empty-instruction,
   (ii) $\pi_1(S \times \text{the carrier of } A)$ is complying-with-catenation,
   (iii) $\pi_1(S \times \text{the carrier of } A)$ complies with **if** w.r.t. T, and
   (iv) $\pi_1(S \times \text{the carrier of } A)$ complies with **while** w.r.t. T.

Let A be a pre-if-while algebra, let S be a non empty set, and let T be a subset of S. A function from $[\!: S, \text{the carrier of } A :\!]$ into S is said to be an execution function of A over S and T if it satisfies the conditions (Def. 32).

(Def. 32)(i)   It is complying-with-empty-instruction,
   (ii)   it is complying-with-catenation,
   (iii)   it complies with **if** w.r.t. T, and
   (iv)   it complies with **while** w.r.t. T.

Let A be a pre-if-while algebra, let S be a non empty set, and let T be a subset of S. One can verify that every execution function of A over S and T is complying-with-empty-instruction and complying-with-catenation.

Let A be a pre-if-while algebra, let I be an element of A, let S be a non empty set, let s be an element of S, let T be a subset of S, and let f be an execution function of A over S and T. We say that iteration of f started in I terminates w.r.t. s if and only if the condition (Def. 33) is satisfied.

(Def. 33)   There exists a non empty finite sequence r of elements of S such that $r(1) = s$ and $r(\text{len } r) \notin T$ and for every natural number i such that $1 \leq i$

and $i < \operatorname{len} r$ holds $r(i) \in T$ and $r(i+1) = f(r(i),\, I)$.

Let A be a pre-if-while algebra, let I be an element of A, let S be a non empty set, let s be an element of S, let T be a subset of S, and let f be an execution function of A over S and T. The functor termination-degree(I, s, f) yields an extended real number and is defined by:

(Def. 34)(i)   There exists a non empty finite sequence r of elements of S such that termination-degree$(I, s, f) = \operatorname{len} r - 1$ and $r(1) = s$ and $r(\operatorname{len} r) \notin T$ and for every natural number i such that $1 \leq i$ and $i < \operatorname{len} r$ holds $r(i) \in T$ and $r(i+1) = f(r(i),\, I)$ if iteration of f started in I terminates w.r.t. s,

(ii)   termination-degree$(I, s, f) = +\infty$, otherwise.

In the sequel f denotes an execution function of A over S and T.

We now state four propositions:

(82) Iteration of f started in I terminates w.r.t. s iff termination-degree$(I, s, f) < +\infty$.

(83) If $s \notin T$, then iteration of f started in I terminates w.r.t. s and termination-degree$(I, s, f) = 0$.

(84) Suppose $s \in T$. Then
(i)   iteration of f started in I terminates w.r.t. s iff iteration of f started in I terminates w.r.t. $f(s, I)$, and
(ii)   termination-degree$(I, s, f) = \overline{1} + $ termination-degree$(I, f(s, I), f)$.

(85) termination-degree$(I, s, f) \geq 0$.

Now we present two schemes. The scheme *Termination* deals with a pre-if-while algebra $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, a non empty set $\mathcal{C}$, an element $\mathcal{D}$ of $\mathcal{C}$, a subset $\mathcal{E}$ of $\mathcal{C}$, an execution function $\mathcal{F}$ of $\mathcal{A}$ over $\mathcal{C}$ and $\mathcal{E}$, a unary functor $\mathcal{F}$ yielding a natural number, and a unary predicate $\mathcal{P}$, and states that:

Iteration of $\mathcal{F}$ started in $\mathcal{B}$ terminates w.r.t. $\mathcal{D}$

provided the parameters meet the following requirements:
- $\mathcal{D} \in \mathcal{E}$ iff $\mathcal{P}[\mathcal{D}]$, and
- For every element s of $\mathcal{C}$ such that $\mathcal{P}[s]$ holds $\mathcal{P}[\mathcal{F}(s, \mathcal{B})]$ iff $\mathcal{F}(s, \mathcal{B}) \in \mathcal{E}$ and $\mathcal{F}(\mathcal{F}(s, \mathcal{B})) < \mathcal{F}(s)$.

The scheme *Termination2* deals with a pre-if-while algebra $\mathcal{A}$, an element $\mathcal{B}$ of $\mathcal{A}$, a non empty set $\mathcal{C}$, an element $\mathcal{D}$ of $\mathcal{C}$, a subset $\mathcal{E}$ of $\mathcal{C}$, an execution function $\mathcal{F}$ of $\mathcal{A}$ over $\mathcal{C}$ and $\mathcal{E}$, a unary functor $\mathcal{F}$ yielding a natural number, and two unary predicates $\mathcal{P}$, $\mathcal{Q}$, and states that:

Iteration of $\mathcal{F}$ started in $\mathcal{B}$ terminates w.r.t. $\mathcal{D}$

provided the following requirements are met:
- $\mathcal{P}[\mathcal{D}]$,
- $\mathcal{D} \in \mathcal{E}$ iff $\mathcal{Q}[\mathcal{D}]$, and
- Let s be an element of $\mathcal{C}$. Suppose $\mathcal{P}[s]$ and $s \in \mathcal{E}$ and $\mathcal{Q}[s]$. Then $\mathcal{P}[\mathcal{F}(s, \mathcal{B})]$ and $\mathcal{Q}[\mathcal{F}(s, \mathcal{B})]$ iff $\mathcal{F}(s, \mathcal{B}) \in \mathcal{E}$ and $\mathcal{F}(\mathcal{F}(s, \mathcal{B})) < \mathcal{F}(s)$.

Next we state two propositions:

(86) Let r be a non empty finite sequence of elements of S. Suppose $r(1) = f(s, C)$ and $r(\operatorname{len} r) \notin T$ and for every natural number i such that $1 \leq i$ and $i < \operatorname{len} r$ holds $r(i) \in T$ and $r(i + 1) = f(r(i), I; C)$. Then $f(s, \operatorname{while} C \operatorname{do} I) = r(\operatorname{len} r)$.

(87) Let I be an element of A and s be an element of S. Then iteration of f started in I does not terminate w.r.t. s if and only if $(\operatorname{curry}' f)(I)\text{-orbit}(s) \subseteq T$.

Now we present two schemes. The scheme *InvariantSch* deals with a pre-if-while algebra $\mathcal{A}$, elements $\mathcal{B}$, $\mathcal{C}$ of $\mathcal{A}$, a non empty set $\mathcal{D}$, an element $\mathcal{E}$ of $\mathcal{D}$, a subset $\mathcal{F}$ of $\mathcal{D}$, an execution function $\mathcal{G}$ of $\mathcal{A}$ over $\mathcal{D}$ and $\mathcal{F}$, and two unary predicates $\mathcal{P}$, $\mathcal{Q}$, and states that:

$$\mathcal{P}[\mathcal{G}(\mathcal{E}, \operatorname{while} \mathcal{B} \operatorname{do} \mathcal{C})] \text{ and not } \mathcal{Q}[\mathcal{G}(\mathcal{E}, \operatorname{while} \mathcal{B} \operatorname{do} \mathcal{C})]$$

provided the following conditions are met:

- $\mathcal{P}[\mathcal{E}]$,
- Iteration of $\mathcal{G}$ started in $\mathcal{C}; \mathcal{B}$ terminates w.r.t. $\mathcal{G}(\mathcal{E}, \mathcal{B})$,
- For every element s of $\mathcal{D}$ such that $\mathcal{P}[s]$ and $s \in \mathcal{F}$ and $\mathcal{Q}[s]$ holds $\mathcal{P}[\mathcal{G}(s, \mathcal{C})]$, and
- For every element s of $\mathcal{D}$ such that $\mathcal{P}[s]$ holds $\mathcal{P}[\mathcal{G}(s, \mathcal{B})]$ and $\mathcal{G}(s, \mathcal{B}) \in \mathcal{F}$ iff $\mathcal{Q}[\mathcal{G}(s, \mathcal{B})]$.

The scheme *coInvariantSch* deals with a pre-if-while algebra $\mathcal{A}$, elements $\mathcal{B}$, $\mathcal{C}$ of $\mathcal{A}$, a non empty set $\mathcal{D}$, an element $\mathcal{E}$ of $\mathcal{D}$, a subset $\mathcal{F}$ of $\mathcal{D}$, an execution function $\mathcal{G}$ of $\mathcal{A}$ over $\mathcal{D}$ and $\mathcal{F}$, and a unary predicate $\mathcal{P}$, and states that:

$$\mathcal{P}[\mathcal{E}]$$

provided the following conditions are met:

- $\mathcal{P}[\mathcal{G}(\mathcal{E}, \operatorname{while} \mathcal{B} \operatorname{do} \mathcal{C})]$,
- Iteration of $\mathcal{G}$ started in $\mathcal{C}; \mathcal{B}$ terminates w.r.t. $\mathcal{G}(\mathcal{E}, \mathcal{B})$,
- For every element s of $\mathcal{D}$ such that $\mathcal{P}[\mathcal{G}(\mathcal{G}(s, \mathcal{B}), \mathcal{C})]$ and $\mathcal{G}(s, \mathcal{B}) \in \mathcal{F}$ holds $\mathcal{P}[\mathcal{G}(s, \mathcal{B})]$, and
- For every element s of $\mathcal{D}$ such that $\mathcal{P}[\mathcal{G}(s, \mathcal{B})]$ holds $\mathcal{P}[s]$.

Next we state three propositions:

(88) Let A be a free pre-if-while algebra, I_1, I_2 be elements of A, and n be a natural number. Suppose $I_1; I_2 \in \operatorname{ElementaryInstructions}_A{}^n$. Then there exists a natural number i such that $n = i + 1$ and $I_1 \in \operatorname{ElementaryInstructions}_A{}^i$ and $I_2 \in \operatorname{ElementaryInstructions}_A{}^i$.

(89) Let A be a free pre-if-while algebra, C, I_1, I_2 be elements of A, and n be a natural number. Suppose if C then I_1 else $I_2 \in \operatorname{ElementaryInstructions}_A{}^n$. Then there exists a natural number i such that $n = i + 1$ and $C \in \operatorname{ElementaryInstructions}_A{}^i$ and $I_1 \in \operatorname{ElementaryInstructions}_A{}^i$ and $I_2 \in \operatorname{ElementaryInstructions}_A{}^i$.

(90)   Let A be a free pre-if-while algebra, C, I be elements of A, and n be a natural number. Suppose $\text{while}\, C\,\text{do}\, I \in \text{ElementaryInstructions}_A{}^n$. Then there exists a natural number i such that $n = i + 1$ and $C \in \text{ElementaryInstructions}_A{}^i$ and $I \in \text{ElementaryInstructions}_A{}^i$.

5. Existence and Uniqueness of Execution Function and Termination

The scheme *IndDef* deals with a free E.C.I.W.-strict pre-if-while algebra $\mathcal{A}$, a non empty set $\mathcal{B}$, an element $\mathcal{C}$ of $\mathcal{B}$, a unary functor $\mathcal{F}$ yielding a set, two binary functors $\mathcal{G}$ and $\mathcal{H}$ yielding elements of $\mathcal{B}$, and a ternary functor $\mathcal{I}$ yielding an element of $\mathcal{B}$, and states that:

There exists a function f from the carrier of $\mathcal{A}$ into $\mathcal{B}$ such that

(i)   for every element I of $\mathcal{A}$ such that $I \in \text{ElementaryInstructions}_{\mathcal{A}}$ holds $f(I) = \mathcal{F}(I)$,

(ii) $f(\text{EmptyIns}_{\mathcal{A}}) = \mathcal{C}$,

(iii)   for all elements I_1, I_2 of $\mathcal{A}$ holds $f(I_1; I_2) = \mathcal{G}(f(I_1), f(I_2))$,

(iv)   for all elements C, I_1, I_2 of $\mathcal{A}$ holds $f(\text{if}\, C\,\text{then}\, I_1\,\text{else}\, I_2) = \mathcal{I}(f(C), f(I_1), f(I_2))$, and

(v)   for all elements C, I of $\mathcal{A}$ holds $f(\text{while}\, C\,\text{do}\, I) = \mathcal{H}(f(C), f(I))$

provided the following requirement is met:

- For every element I of $\mathcal{A}$ such that $I \in \text{ElementaryInstructions}_{\mathcal{A}}$ holds $\mathcal{F}(I) \in \mathcal{B}$.

We now state three propositions:

(91)   Let A be a free E.C.I.W.-strict pre-if-while algebra, g be a function from $[\![\, S,\, \text{ElementaryInstructions}_A\,]\!]$ into S, and s_0 be an element of S. Then there exists an execution function f of A over S and T such that

(i) $f{\upharpoonright}[\![\, S,\, \text{ElementaryInstructions}_A\,]\!] = g$, and

(ii)   for every element s of S and for all elements C, I of A such that iteration of f started in $I; C$ does not terminate w.r.t. $f(s, C)$ holds $f(s, \text{while}\, C\,\text{do}\, I) = s_0$.

(92)   Let A be a free E.C.I.W.-strict pre-if-while algebra, g be a function from $[\![\, S,\, \text{ElementaryInstructions}_A\,]\!]$ into S, and F be a function from S^S into S^S. Suppose that for every element h of S^S holds $F(h) \cdot h = F(h)$. Then there exists an execution function f of A over S and T such that

(i) $f{\upharpoonright}[\![\, S,\, \text{ElementaryInstructions}_A\,]\!] = g$, and

(ii)   for all elements C, I of A and for every element s of S such that iteration of f started in $I; C$ does not terminate w.r.t. $f(s, C)$ holds $f(s, \text{while}\, C\,\text{do}\, I) = F((\text{curry}'\, f)(I; C))(f(s, C))$.

(93)   Let A be a free E.C.I.W.-strict pre-if-while algebra and f_1, f_2 be execu-
tion functions of A over S and T. Suppose that

(i) $f_1 {\restriction} [: S, \text{ElementaryInstructions}_A :] = f_2 {\restriction} [: S, \text{ElementaryInstructions}_A :]$,
and

(ii)   for every element s of S and for all elements C, I of A such that
iteration of f_1 started in $I; C$ does not terminate w.r.t. $f_1(s, C)$ holds
$f_1(s, \text{while } C \text{ do } I) = f_2(s, \text{while } C \text{ do } I)$.
Then $f_1 = f_2$.

Let A be a pre-if-while algebra, let S be a non empty set, let T be a subset
of S, and let f be an execution function of A over S and T. The functor
$\text{TerminatingPrograms}(A, S, T, f)$ yielding a subset of $[: S, \text{the carrier of } A :]$ is
defined by the conditions (Def. 35).

(Def. 35)(i) $[: S, \text{ElementaryInstructions}_A :] \subseteq \text{TerminatingPrograms}(A, S, T, f)$,

(ii) $[: S, \{\text{EmptyIns}_A\} :] \subseteq \text{TerminatingPrograms}(A, S, T, f)$,

(iii)   for every element s of S and for all elements C, I,
J of A holds if $\langle s, I \rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and
$\langle f(s, I), J \rangle \in \text{TerminatingPrograms}(A, S, T, f)$, then $\langle s, I; J \rangle \in$
$\text{TerminatingPrograms}(A, S, T, f)$ and if $\langle s, C \rangle \in \text{TerminatingPrograms}(A,$
$S, T, f)$ and $\langle f(s, C), I \rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and $f(s,$
$C) \in T$, then $\langle s, \text{if } C \text{ then } I \text{ else } J \rangle \in \text{TerminatingPrograms}(A, S, T, f)$
and if $\langle s, C \rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and $\langle f(s, C),$
$J \rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and $f(s, C) \notin T$, then $\langle s,$
$\text{if } C \text{ then } I \text{ else } J \rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and if $\langle s, C \rangle \in$
$\text{TerminatingPrograms}(A, S, T, f)$ and there exists a non empty finite se-
quence r of elements of S such that $r(1) = f(s, C)$ and $r(\text{len } r) \notin T$ and
for every natural number i such that $1 \leq i$ and $i < \text{len } r$ holds $r(i) \in T$
and $\langle r(i), I; C \rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and $r(i+1) = f(r(i),$
$I; C)$, then $\langle s, \text{while } C \text{ do } I \rangle \in \text{TerminatingPrograms}(A, S, T, f)$, and

(iv)   for every subset P of $[: S, \text{the carrier of } A :]$ such that $[: S,$
$\text{ElementaryInstructions}_A :] \subseteq P$ and $[: S, \{\text{EmptyIns}_A\} :] \subseteq P$ and for ev-
ery element s of S and for all elements C, I, J of A holds if $\langle s, I \rangle \in P$
and $\langle f(s, I), J \rangle \in P$, then $\langle s, I; J \rangle \in P$ and if $\langle s, C \rangle \in P$ and $\langle f(s, C),$
$I \rangle \in P$ and $f(s, C) \in T$, then $\langle s, \text{if } C \text{ then } I \text{ else } J \rangle \in P$ and if $\langle s, C \rangle \in P$
and $\langle f(s, C), J \rangle \in P$ and $f(s, C) \notin T$, then $\langle s, \text{if } C \text{ then } I \text{ else } J \rangle \in P$
and if $\langle s, C \rangle \in P$ and there exists a non empty finite sequence r of el-
ements of S such that $r(1) = f(s, C)$ and $r(\text{len } r) \notin T$ and for every
natural number i such that $1 \leq i$ and $i < \text{len } r$ holds $r(i) \in T$ and $\langle r(i),$
$I; C \rangle \in P$ and $r(i+1) = f(r(i), I; C)$, then $\langle s, \text{while } C \text{ do } I \rangle \in P$ holds
$\text{TerminatingPrograms}(A, S, T, f) \subseteq P$.

Let A be a pre-if-while algebra and let I be an element of A. We say that I
is absolutely-terminating if and only if the condition (Def. 36) is satisfied.

(Def. 36)   Let S be a non empty set, s be an element of S, T be a subset of S, and f be an execution function of A over S and T. Then $\langle s, I \rangle \in$ TerminatingPrograms(A, S, T, f).

Let A be a pre-if-while algebra, let S be a non empty set, let T be a subset of S, let I be an element of A, and let f be an execution function of A over S and T. We say that I is terminating w.r.t. f if and only if:

(Def. 37)   For every element s of S holds $\langle s, I \rangle \in$ TerminatingPrograms(A, S, T, f).

Let A be a pre-if-while algebra, let S be a non empty set, let T be a subset of S, let I be an element of A, let f be an execution function of A over S and T, and let Z be a set. We say that I is terminating w.r.t. f and Z if and only if:

(Def. 38)   For every element s of S such that $s \in Z$ holds $\langle s, I \rangle \in$ TerminatingPrograms(A, S, T, f).

We say that Z is invariant w.r.t. I and f if and only if:

(Def. 39)   For every element s of S such that $s \in Z$ holds $f(s, I) \in Z$.

One can prove the following propositions:

(94)   If $I \in$ ElementaryInstructions$_A$, then
$\langle s, I \rangle \in$ TerminatingPrograms(A, S, T, f).

(95)   If $I \in$ ElementaryInstructions$_A$, then I is absolutely-terminating.

(96) $\langle s, \text{EmptyIns}_A \rangle \in$ TerminatingPrograms(A, S, T, f).

Let us consider A. Observe that EmptyIns$_A$ is absolutely-terminating.

Let us consider A. Observe that there exists an element of A which is absolutely-terminating.

Next we state the proposition

(97)   If A is free and $\langle s, I; J \rangle \in$ TerminatingPrograms(A, S, T, f), then $\langle s, I \rangle \in$ TerminatingPrograms(A, S, T, f) and $\langle f(s, I), J \rangle \in$ TerminatingPrograms(A, S, T, f).

Let us consider A and let I, J be absolutely-terminating elements of A. One can verify that $I; J$ is absolutely-terminating.

We now state the proposition

(98)   Suppose A is free and
$\langle s, \text{if } C \text{ then } I \text{ else } J \rangle \in$ TerminatingPrograms(A, S, T, f). Then $\langle s, C \rangle \in$ TerminatingPrograms(A, S, T, f) and if $f(s, C) \in T$, then $\langle f(s, C), I \rangle \in$ TerminatingPrograms(A, S, T, f) and if $f(s, C) \notin T$, then $\langle f(s, C), J \rangle \in$ TerminatingPrograms(A, S, T, f).

Let us consider A and let C, I, J be absolutely-terminating elements of A. Note that if C then I else J is absolutely-terminating.

Let us consider A and let C, I be absolutely-terminating elements of A. Note that if C then I is absolutely-terminating.

The following propositions are true:

(99)   Suppose A is free and $\langle s, \text{while}\,C\,\text{do}\,I\rangle \in \text{TerminatingPrograms}(A, S, T, f)$. Then

(i) $\langle s, C\rangle \in \text{TerminatingPrograms}(A, S, T, f)$, and

(ii)   there exists a non empty finite sequence r of elements of S such that $r(1) = f(s, C)$ and $r(\text{len}\,r) \notin T$ and for every natural number i such that $1 \leq i$ and $i < \text{len}\,r$ holds $r(i) \in T$ and $\langle r(i), I;C\rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and $r(i+1) = f(r(i), I;C)$.

(100)   If A is free and $\langle s, \text{while}\,C\,\text{do}\,I\rangle \in \text{TerminatingPrograms}(A, S, T, f)$ and $f(s, C) \in T$, then $\langle f(s, C), I\rangle \in \text{TerminatingPrograms}(A, S, T, f)$.

(101)   Let C, I be absolutely-terminating elements of A. Suppose iteration of f started in $I;C$ terminates w.r.t. $f(s, C)$. Then $\langle s, \text{while}\,C\,\text{do}\,I\rangle \in \text{TerminatingPrograms}(A, S, T, f)$.

(102)   Let A be a free E.C.I.W.-strict pre-if-while algebra and f_1, f_2 be execution functions of A over S and T. If $f_1 {\upharpoonright} [\![\,S, \text{ElementaryInstructions}_A\,]\!] = f_2 {\upharpoonright} [\![\,S, \text{ElementaryInstructions}_A\,]\!]$, then $\text{TerminatingPrograms}(A, S, T, f_1) = \text{TerminatingPrograms}(A, S, T, f_2)$.

(103)   Let A be a free E.C.I.W.-strict pre-if-while algebra and f_1, f_2 be execution functions of A over S and T. Suppose $f_1 {\upharpoonright} [\![\,S, \text{ElementaryInstructions}_A\,]\!] = f_2 {\upharpoonright} [\![\,S, \text{ElementaryInstructions}_A\,]\!]$. Let s be an element of S and I be an element of A. If $\langle s, I\rangle \in \text{TerminatingPrograms}(A, S, T, f_1)$, then $f_1(s, I) = f_2(s, I)$.

(104)   Every absolutely-terminating element of A is terminating w.r.t. f.

(105)   For every element I of A holds I is terminating w.r.t. f iff I is terminating w.r.t. f and S.

(106)   Let I be an element of A. Suppose I is terminating w.r.t. f. Let P be a set. Then I is terminating w.r.t. f and P.

(107)   For every absolutely-terminating element I of A and for every set P holds I is terminating w.r.t. f and P.

(108)   For every element I of A holds S is invariant w.r.t. I and f.

(109)   Let P be a set and I, J be elements of A. Suppose P is invariant w.r.t. I and f and invariant w.r.t. J and f. Then P is invariant w.r.t. $I;J$ and f.

(110)   Let I, J be elements of A. Suppose I is terminating w.r.t. f and J is terminating w.r.t. f. Then $I;J$ is terminating w.r.t. f.

(111)   Let P be a set and I, J be elements of A. Suppose I is terminating w.r.t. f and P and J is terminating w.r.t. f and P and P is invariant w.r.t. I and f. Then $I;J$ is terminating w.r.t. f and P.

(112)   Let C, I, J be elements of A. Suppose C is terminating w.r.t. f and I is terminating w.r.t. f and J is terminating w.r.t. f. Then if C then I else J is terminating w.r.t. f.

(113)   Let P be a set and C, I, J be elements of A. Suppose that
   (i) C is terminating w.r.t. f and P,
   (ii) I is terminating w.r.t. f and P,
   (iii) J is terminating w.r.t. f and P, and
   (iv) P is invariant w.r.t. C and f.
       Then if C then I else J is terminating w.r.t. f and P.

(114)   Let C, I be elements of A. Suppose that
   (i) C is terminating w.r.t. f,
   (ii) I is terminating w.r.t. f, and
   (iii) iteration of f started in I; C terminates w.r.t. $f(s, C)$.
       Then $\langle s, \text{while } C \text{ do } I \rangle \in \text{TerminatingPrograms}(A, S, T, f)$.

(115)   Let P be a set and C, I be elements of A. Suppose that
   (i) C is terminating w.r.t. f and P,
   (ii) I is terminating w.r.t. f and P,
   (iii) P is invariant w.r.t. C and f and invariant w.r.t. I and f,
   (iv)   iteration of f started in I; C terminates w.r.t. $f(s, C)$, and
   (v) $s \in P$.
       Then $\langle s, \text{while } C \text{ do } I \rangle \in \text{TerminatingPrograms}(A, S, T, f)$.

(116)   Let P be a set and C, I be elements of A. Suppose that
   (i) C is terminating w.r.t. f,
   (ii) I is terminating w.r.t. f and P,
   (iii) P is invariant w.r.t. C and f,
   (iv)   for every s such that $s \in P$ and $f(f(s, I), C) \in T$ holds $f(s, I) \in P$,
   (v)   iteration of f started in I; C terminates w.r.t. $f(s, C)$, and
   (vi) $s \in P$.
       Then $\langle s, \text{while } C \text{ do } I \rangle \in \text{TerminatingPrograms}(A, S, T, f)$.

(117)   Let C, I be elements of A. Suppose that
   (i) C is terminating w.r.t. f,
   (ii) I is terminating w.r.t. f, and
   (iii) for every s holds iteration of f started in I; C terminates w.r.t. s.
       Then while C do I is terminating w.r.t. f.

(118)   Let P be a set and C, I be elements of A. Suppose that
   (i) C is terminating w.r.t. f,
   (ii) I is terminating w.r.t. f and P,
   (iii) P is invariant w.r.t. C and f,
   (iv)   for every s such that $s \in P$ and $f(f(s, I), C) \in T$ holds $f(s, I) \in P$,
          and
   (v)   for every s such that $f(s, C) \in P$ holds iteration of f started in I; C
          terminates w.r.t. $f(s, C)$.
       Then while C do I is terminating w.r.t. f and P.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**):537–541, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. Introduction to trees. *Formalized Mathematics*, 1(**2**):421–427, 1990.

[5] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[6] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[7] Grzegorz Bancerek. König's lemma. *Formalized Mathematics*, 2(**3**):397–402, 1991.

[8] Grzegorz Bancerek. Sets and functions of trees and joining operations of trees. *Formalized Mathematics*, 3(**2**):195–204, 1992.

[9] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.

[10] Grzegorz Bancerek. Minimal signature for partial algebra. *Formalized Mathematics*, 5(**3**):405–414, 1996.

[11] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[12] Grzegorz Bancerek and Yatsuka Nakamura. Full adder circuit. Part I. *Formalized Mathematics*, 5(**3**):367–380, 1996.

[13] Grzegorz Bancerek and Piotr Rudnicki. On defining functions on trees. *Formalized Mathematics*, 4(**1**):91–101, 1993.

[14] Grzegorz Bancerek and Piotr Rudnicki. The set of primitive recursive functions. *Formalized Mathematics*, 9(**4**):705–720, 2001.

[15] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[16] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):163–171, 1991.

[17] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[18] Ewa Burakowska. Subalgebras of the universal algebra. Lattices of subalgebras. *Formalized Mathematics*, 4(**1**):23–27, 1993.

[19] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.

[20] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[21] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[22] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[23] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[24] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[25] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[26] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[27] Czesław Byliński. Subcategories and products of categories. *Formalized Mathematics*, 1(**4**):725–732, 1990.

[28] Patricia L. Carlson and Grzegorz Bancerek. Context-free grammar – part 1. *Formalized Mathematics*, 2(**5**):683–687, 1991.

[29] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[30] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.

[31] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[32] Małgorzata Korolkiewicz. Homomorphisms of algebras. Quotient universal algebra. *Formalized Mathematics*, 4(**1**):109–113, 1993.

[33] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.

[34] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[35] Jarosław Kotowicz, Beata Madras, and Małgorzata Korolkiewicz. Basic notation of universal algebra. *Formalized Mathematics*, 3(**2**):251–253, 1992.

[36] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[37] Beata Perkowska. Free universal algebra construction. *Formalized Mathematics*, 4(**1**):115–120, 1993.

[38] Beata Perkowska. Free many sorted universal algebra. *Formalized Mathematics*, 5(**1**):67–74, 1996.

[39] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[40] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[41] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

[42] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[43] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[44] Andrzej Trybulec. Many sorted algebras. *Formalized Mathematics*, 5(**1**):37–42, 1996.

[45] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.

[46] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[47] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[48] Edmund Woronowicz. Many–argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

[49] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[50] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Definition and some Properties of Information Entropy

Bo Zhang
Shinshu University
Nagano, Japan

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Summary. In this article we mainly define the information entropy [3], [11] and prove some its basic properties. First, we discuss some properties on four kinds of transformation functions between vector and matrix. The transformation functions are LineVec2Mx, ColVec2Mx, Vec2DiagMx and Mx2FinS. Mx2FinS is a horizontal concatenation operator for a given matrix, treating rows of the given matrix as finite sequences, yielding a new finite sequence by horizontally joining each row of the given matrix in order to index. Then we define each concept of information entropy for a probability sequence and two kinds of probability matrices, joint and conditional, that are defined in article [25]. Further, we discuss some properties of information entropy including Shannon's lemma, maximum property, additivity and super-additivity properties.

The papers [21], [23], [1], [20], [24], [6], [14], [8], [4], [22], [17], [7], [9], [2], [5], [15], [16], [12], [10], [13], [18], [25], and [19] provide the terminology and notation for this paper.

1. Preliminaries

For simplicity, we use the following convention: D denotes a non empty set, i, j, k, l denote elements of $\mathbb{N}$, n denotes a natural number, a, b, c, r, r_1, r_2 denote real numbers, p, q denote finite sequences of elements of $\mathbb{R}$, and M_1, M_2 denote matrices over $\mathbb{R}$.

Next we state several propositions:

(1) If $k \neq 0$ and $i < l$ and $l \leq j$ and $k \mid l$, then $i \div k < j \div k$.

(2) If $r > 0$, then $(\log_-(e))(r) \leq r - 1$ and $r = 1$ iff $(\log_-(e))(r) = r - 1$ and $r \neq 1$ iff $(\log_-(e))(r) < r - 1$.

(3) If $r > 0$, then $\log_e r \leq r - 1$ and $r = 1$ iff $\log_e r = r - 1$ and $r \neq 1$ iff $\log_e r < r - 1$.

(4) If $a > 1$ and $b > 1$, then $\log_a b > 0$.

(5) If $a > 0$ and $a \neq 1$ and $b > 0$, then $-\log_a b = \log_a(\frac{1}{b})$.

(6) If $a > 0$ and $a \neq 1$ and $b \geq 0$ and $c \geq 0$, then $b \cdot c \cdot \log_a(b \cdot c) = b \cdot c \cdot \log_a b + b \cdot c \cdot \log_a c$.

(7) Let q, q_1, q_2 be finite sequences of elements of $\mathbb{R}$. Suppose $\operatorname{len} q_1 = \operatorname{len} q$ and $\operatorname{len} q_1 = \operatorname{len} q_2$ and for every k such that $k \in \operatorname{dom} q_1$ holds $q(k) = q_1(k) + q_2(k)$. Then $\sum q = \sum q_1 + \sum q_2$.

(8) Let q, q_1, q_2 be finite sequences of elements of $\mathbb{R}$. Suppose $\operatorname{len} q_1 = \operatorname{len} q$ and $\operatorname{len} q_1 = \operatorname{len} q_2$ and for every k such that $k \in \operatorname{dom} q_1$ holds $q(k) = q_1(k) - q_2(k)$. Then $\sum q = \sum q_1 - \sum q_2$.

(9) Suppose $\operatorname{len} p \geq 1$. Then there exists q such that $\operatorname{len} q = \operatorname{len} p$ and $q(1) = p(1)$ and for every k such that $0 \neq k$ and $k < \operatorname{len} p$ holds $q(k + 1) = q(k) + p(k + 1)$ and $\sum p = q(\operatorname{len} p)$.

Let us consider p. Let us observe that p is non-negative if and only if:

(Def. 1) For every i such that $i \in \operatorname{dom} p$ holds $p(i) \geq 0$.

Let us note that there exists a finite sequence of elements of $\mathbb{R}$ which is non-negative.

The following proposition is true

(10) If p is non-negative and $r \geq 0$, then $r \cdot p$ is non-negative.

Let us consider p, k. We say that p has only one value in k if and only if:

(Def. 2) $k \in \operatorname{dom} p$ and for every i such that $i \in \operatorname{dom} p$ and $i \neq k$ holds $p(i) = 0$.

Next we state four propositions:

(11) If p has only one value in k and $i \neq k$, then $p(i) = 0$.

(12) If $\operatorname{len} p = \operatorname{len} q$ and p has only one value in k, then $p \bullet q$ has only one value in k and $(p \bullet q)(k) = p(k) \cdot q(k)$.

(13) If p has only one value in k, then $\sum p = p(k)$.

(14) If p is non-negative, then for every k such that $k \in \operatorname{dom} p$ and $p(k) = \sum p$ holds p has only one value in k.

Let us observe that every finite sequence of elements of $\mathbb{R}$ which is finite probability distribution is also non empty and non-negative.

One can prove the following propositions:

(15) Let p be finite probability distribution finite sequence of elements of $\mathbb{R}$ and given k such that $k \in \operatorname{dom} p$ and $p(k) = 1$. Then p has only one value in k.

(16)   Let i be a non empty natural number. Then $i \mapsto \frac{1}{i}$ is finite probability distribution finite sequence of elements of $\mathbb{R}$.

One can check that every matrix over $\mathbb{R}$ which is summable-to-1 is also non empty yielding and every matrix over $\mathbb{R}$ which is joint probability is also non empty yielding.

The following propositions are true:

(17)   For every matrix M over $\mathbb{R}$ such that $M = \emptyset$ holds $\operatorname{SumAll} M = 0$.

(18)   For every matrix M over D and for every i such that $i \in \operatorname{dom} M$ holds $\operatorname{dom} M(i) = \operatorname{Seg} \operatorname{width} M$.

(19) M_1 is nonnegative iff for every i such that $i \in \operatorname{dom} M_1$ holds $\operatorname{Line}(M_1, i)$ is non-negative.

2. Properties of Transformations between Vector and Matrix

Next we state four propositions:

(20)   For every j such that $j \in \operatorname{dom} p$ holds $(\operatorname{LineVec2Mx} p)_{\square,j} = \langle p(j) \rangle$.

(21)   Let p be a non empty finite sequence of elements of $\mathbb{R}$, q be a finite sequence of elements of $\mathbb{R}$, and M be a matrix over $\mathbb{R}$. Then $M = \operatorname{ColVec2Mx} p \cdot \operatorname{LineVec2Mx} q$ if and only if the following conditions are satisfied:

(i) $\operatorname{len} M = \operatorname{len} p$,

(ii) $\operatorname{width} M = \operatorname{len} q$, and

(iii)   for all i, j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} = p(i) \cdot q(j)$.

(22)   Let p be a non empty finite sequence of elements of $\mathbb{R}$, q be a finite sequence of elements of $\mathbb{R}$, and M be a matrix over $\mathbb{R}$. Then $M = \operatorname{ColVec2Mx} p \cdot \operatorname{LineVec2Mx} q$ if and only if the following conditions are satisfied:

(i) $\operatorname{len} M = \operatorname{len} p$,

(ii) $\operatorname{width} M = \operatorname{len} q$, and

(iii)   for every i such that $i \in \operatorname{dom} M$ holds $\operatorname{Line}(M, i) = p(i) \cdot q$.

(23)   Let p, q be finite probability distribution finite sequences of elements of $\mathbb{R}$. Then $\operatorname{ColVec2Mx} p \cdot \operatorname{LineVec2Mx} q$ is joint probability.

Let us consider n and let M_1 be a matrix over $\mathbb{R}$ of dimension n. We say that M_1 is diagonal if and only if:

(Def. 3)   For all i, j such that $\langle i, j \rangle \in$ the indices of M_1 and $(M_1)_{i,j} \neq 0$ holds $i = j$.

Let us consider n. Observe that there exists a matrix over $\mathbb{R}$ of dimension n which is diagonal.

The following proposition is true

(24)   Let M_1 be a matrix over $\mathbb{R}$ of dimension n. Then M_1 is diagonal if and only if for every i such that $i \in \operatorname{dom} M_1$ holds $\operatorname{Line}(M_1, i)$ has only one value in i.

Let us consider p. The functor $\operatorname{Vec2DiagMx} p$ yielding a diagonal matrix over $\mathbb{R}$ of dimension $\operatorname{len} p$ is defined as follows:

(Def. 4)   For every j such that $j \in \operatorname{dom} p$ holds $(\operatorname{Vec2DiagMx} p)_{j,j} = p(j)$.

One can prove the following propositions:

(25) $M_1 = \operatorname{Vec2DiagMx} p$ iff $\operatorname{len} M_1 = \operatorname{len} p$ and $\operatorname{width} M_1 = \operatorname{len} p$ and for every i such that $i \in \operatorname{dom} M_1$ holds $\operatorname{Line}(M_1, i)$ has only one value in i and $\operatorname{Line}(M_1, i)(i) = p(i)$.

(26)   Suppose $\operatorname{len} p = \operatorname{len} M_1$. Then $M_2 = \operatorname{Vec2DiagMx} p \cdot M_1$ if and only if the following conditions are satisfied:
   (i) $\operatorname{len} M_2 = \operatorname{len} p$,
   (ii) $\operatorname{width} M_2 = \operatorname{width} M_1$, and
   (iii)   for all i, j such that $\langle i, j \rangle \in$ the indices of M_2 holds $(M_2)_{i,j} = p(i) \cdot (M_1)_{i,j}$.

(27)   If $\operatorname{len} p = \operatorname{len} M_1$, then $M_2 = \operatorname{Vec2DiagMx} p \cdot M_1$ iff $\operatorname{len} M_2 = \operatorname{len} p$ and $\operatorname{width} M_2 = \operatorname{width} M_1$ and for every i such that $i \in \operatorname{dom} M_2$ holds $\operatorname{Line}(M_2, i) = p(i) \cdot \operatorname{Line}(M_1, i)$.

(28)   Let p be finite probability distribution finite sequence of elements of $\mathbb{R}$ and M be a non empty yielding conditional probability matrix over $\mathbb{R}$. If $\operatorname{len} p = \operatorname{len} M$, then $\operatorname{Vec2DiagMx} p \cdot M$ is joint probability.

(29)   Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given k. If $k \in \operatorname{dom} p$, then $\operatorname{len} p(k) = k \cdot \operatorname{width} M$.

(30)   Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k + 1) = p(k) \frown M(k + 1)$. Let given i, j. If $i \in \operatorname{dom} p$ and $j \in \operatorname{dom} p$ and $i \leq j$, then $\operatorname{dom} p(i) \subseteq \operatorname{dom} p(j)$.

(31)   Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Then $\operatorname{len} p(1) = \operatorname{width} M$ and for every j such that $\langle 1, j \rangle \in$ the indices of M holds $j \in \operatorname{dom} p(1)$ and $p(1)(j) = M_{1,j}$.

(32)   Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given j. If $j \geq 1$ and $j < \operatorname{len} p$, then for every l such that $l \in \operatorname{dom} p(j)$ holds $p(j)(l) = p(j+1)(l)$.

(33)   Let M be a matrix over D and p be a finite sequence of elements of D^*.

Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given i, j. Suppose $i \in \operatorname{dom} p$ and $j \in \operatorname{dom} p$ and $i \leq j$. Let given l. If $l \in \operatorname{dom} p(i)$, then $p(i)(l) = p(j)(l)$.

(34) Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given j. Suppose $j \geq 1$ and $j < \operatorname{len} p$. Let given l. If $l \in \operatorname{Seg} \operatorname{width} M$, then $j \cdot \operatorname{width} M + l \in \operatorname{dom} p(j+1)$ and $p(j+1)(j \cdot \operatorname{width} M + l) = M(j+1)(l)$.

(35) Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given i, j. Suppose $\langle i, j \rangle \in$ the indices of M. Then $(i-1) \cdot \operatorname{width} M + j \in \operatorname{dom} p(i)$ and $M_{i,j} = p(i)((i-1) \cdot \operatorname{width} M + j)$.

(36) Let M be a matrix over D and p be a finite sequence of elements of D^*. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given i, j. Suppose $\langle i, j \rangle \in$ the indices of M. Then $(i-1) \cdot \operatorname{width} M + j \in \operatorname{dom} p(\operatorname{len} M)$ and $M_{i,j} = p(\operatorname{len} M)((i-1) \cdot \operatorname{width} M + j)$.

(37) Let M be a matrix over $\mathbb{R}$ and p be a finite sequence of elements of $\mathbb{R}^*$. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Let given k. If $k \geq 1$ and $k < \operatorname{len} M$, then $\sum p(k+1) = \sum p(k) + \sum M(k+1)$.

(38) Let M be a matrix over $\mathbb{R}$ and p be a finite sequence of elements of $\mathbb{R}^*$. Suppose $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$. Then $\operatorname{SumAll} M = \sum p(\operatorname{len} M)$.

Let D be a non empty set and let M be a matrix over D. The functor $\operatorname{Mx2FinS} M$ yields a finite sequence of elements of D and is defined by:

(Def. 5)(i) $\operatorname{Mx2FinS} M = \emptyset$ if $\operatorname{len} M = 0$,

(ii) there exists a finite sequence p of elements of D^* such that $\operatorname{Mx2FinS} M = p(\operatorname{len} M)$ and $\operatorname{len} p = \operatorname{len} M$ and $p(1) = M(1)$ and for every k such that $k \geq 1$ and $k < \operatorname{len} M$ holds $p(k+1) = p(k) \frown M(k+1)$, otherwise.

We now state several propositions:

(39) For every matrix M over D holds $\operatorname{len} \operatorname{Mx2FinS} M = \operatorname{len} M \cdot \operatorname{width} M$.

(40) Let M be a matrix over D and given i, j. If $\langle i, j \rangle \in$ the indices of M, then $(i-1) \cdot \operatorname{width} M + j \in \operatorname{dom} \operatorname{Mx2FinS} M$ and $M_{i,j} = (\operatorname{Mx2FinS} M)((i-1) \cdot \operatorname{width} M + j)$.

(41) Let M be a matrix over D and given k, l. Suppose $k \in \operatorname{dom} \operatorname{Mx2FinS} M$

and $l = k - 1$. Then $\langle (l \div \text{width } M) + 1,\ (l \bmod \text{width } M) + 1 \rangle \in$ the indices of M and $(\text{Mx2FinS } M)(k) = M_{(l \div \text{width } M)+1,(l \bmod \text{width } M)+1}$.

(42) $\text{SumAll } M_1 = \sum \text{Mx2FinS } M_1$.

(43) M_1 is nonnegative iff $\text{Mx2FinS } M_1$ is non-negative.

(44) M_1 is joint probability iff $\text{Mx2FinS } M_1$ is finite probability distribution.

(45)   Let p, q be finite probability distribution finite sequences of elements of $\mathbb{R}$. Then $\text{Mx2FinS}(\text{ColVec2Mx } p \cdot \text{LineVec2Mx } q)$ is finite probability distribution.

(46)   Let p be finite probability distribution finite sequence of elements of $\mathbb{R}$ and M be a non empty yielding conditional probability matrix over $\mathbb{R}$. If $\text{len } p = \text{len } M$, then $\text{Mx2FinS}(\text{Vec2DiagMx } p \cdot M)$ is finite probability distribution.

3. Information Entropy

Let us consider a, p. Let us assume that $a > 0$ and $a \neq 1$ and p is non-negative. The functor $\overrightarrow{\log}_a p$ yields a finite sequence of elements of $\mathbb{R}$ and is defined by:

(Def. 6) $\text{len } \overrightarrow{\log}_a p = \text{len } p$ and for every k such that $k \in \text{dom } \overrightarrow{\log}_a p$ holds if $p(k) > 0$, then $(\overrightarrow{\log}_a p)(k) = \log_a p(k)$ and if $p(k) = 0$, then $(\overrightarrow{\log}_a p)(k) = 0$.

Let us consider p. The functor $\overrightarrow{\text{id log}} \, p$ yields a finite sequence of elements of $\mathbb{R}$ and is defined by:

(Def. 7) $\overrightarrow{\text{id log}} \, p = p \bullet \overrightarrow{\log}_2 p$.

The following propositions are true:

(47)   Let p be a non-negative finite sequence of elements of $\mathbb{R}$ and given q. Then $q = \overrightarrow{\text{id log}} \, p$ if and only if the following conditions are satisfied:
   (i) $\text{len } q = \text{len } p$, and
   (ii)   for every k such that $k \in \text{dom } q$ holds $q(k) = p(k) \cdot \log_2 p(k)$.

(48)   Let p be a non-negative finite sequence of elements of $\mathbb{R}$ and given k such that $k \in \text{dom } p$. Then
   (i)   if $p(k) = 0$, then $(\overrightarrow{\text{id log}} \, p)(k) = 0$, and
   (ii)   if $p(k) > 0$, then $(\overrightarrow{\text{id log}} \, p)(k) = p(k) \cdot \log_2 p(k)$.

(49)   Let p be a non-negative finite sequence of elements of $\mathbb{R}$ and given q. Then $q = -\overrightarrow{\text{id log}} \, p$ if and only if the following conditions are satisfied:
   (i) $\text{len } q = \text{len } p$, and
   (ii)   for every k such that $k \in \text{dom } q$ holds $q(k) = p(k) \cdot \log_2(\frac{1}{p(k)})$.

(50)   Let p be a non-negative finite sequence of elements of $\mathbb{R}$. Suppose $r_1 \geq 0$ and $r_2 \geq 0$. Let given i. If $i \in \text{dom } p$ and $p(i) = r_1 \cdot r_2$, then $(\overrightarrow{\text{id log}} \, p)(i) = r_1 \cdot r_2 \cdot \log_2 r_1 + r_1 \cdot r_2 \cdot \log_2 r_2$.

(51)   For every non-negative finite sequence p of elements of $\mathbb{R}$ such that $r \geq 0$ holds $\overrightarrow{\text{id log}}\, r \cdot p = r \cdot \log_2 r \cdot p + r \cdot (p \bullet \overrightarrow{\log_2} p)$.

(52)   Let p be a non empty finite probability distribution finite sequence of elements of $\mathbb{R}$ and given k. If $k \in \operatorname{dom} p$, then $(\overrightarrow{\text{id log}}\, p)(k) \leq 0$.

Let us consider M_1. Let us assume that M_1 is nonnegative. The functor $\overrightarrow{\text{id log}}\, M_1$ yields a matrix over $\mathbb{R}$ and is defined as follows:

(Def. 8) $\operatorname{len} \overrightarrow{\text{id log}}\, M_1 = \operatorname{len} M_1$ and $\operatorname{width} \overrightarrow{\text{id log}}\, M_1 = \operatorname{width} M_1$ and for every k such that $k \in \operatorname{dom} \overrightarrow{\text{id log}}\, M_1$ holds $(\overrightarrow{\text{id log}}\, M_1)(k) = \operatorname{Line}(M_1, k) \bullet \overrightarrow{\log_2} \operatorname{Line}(M_1, k)$.

The following two propositions are true:

(53)   For every nonnegative matrix M over $\mathbb{R}$ and for every k such that $k \in \operatorname{dom} M$ holds $\operatorname{Line}(\overrightarrow{\text{id log}}\, M, k) = \overrightarrow{\text{id log}}\, \operatorname{Line}(M, k)$.

(54)   Let M be a nonnegative matrix over $\mathbb{R}$ and M_3 be a matrix over $\mathbb{R}$. Then $M_3 = \overrightarrow{\text{id log}}\, M$ if and only if the following conditions are satisfied:
   (i) $\operatorname{len} M_3 = \operatorname{len} M$,
   (ii) $\operatorname{width} M_3 = \operatorname{width} M$, and
   (iii)   for all i, j such that $\langle i, j \rangle \in$ the indices of M_3 holds $(M_3)_{i,j} = M_{i,j} \cdot \log_2(M_{i,j})$.

Let p be a finite sequence of elements of $\mathbb{R}$. The functor $\operatorname{Entropy} p$ yields a real number and is defined by:

(Def. 9) $\operatorname{Entropy} p = -\sum \overrightarrow{\text{id log}}\, p$.

We now state several propositions:

(55)   For every non empty finite probability distribution finite sequence p of elements of $\mathbb{R}$ holds $\operatorname{Entropy} p \geq 0$.

(56)   Let p be a non empty finite probability distribution finite sequence of elements of $\mathbb{R}$. If there exists k such that $k \in \operatorname{dom} p$ and $p(k) = 1$, then $\operatorname{Entropy} p = 0$.

(57)   Let p, q be non empty finite probability distribution finite sequences of elements of $\mathbb{R}$ and p_1, q_3 be finite sequences of elements of $\mathbb{R}$. Suppose that
   (i) $\operatorname{len} p = \operatorname{len} q$,
   (ii) $\operatorname{len} p_1 = \operatorname{len} p$,
   (iii) $\operatorname{len} q_3 = \operatorname{len} q$, and
   (iv)   for every k such that $k \in \operatorname{dom} p$ holds $p(k) > 0$ and $q(k) > 0$ and $p_1(k) = -p(k) \cdot \log_2 p(k)$ and $q_3(k) = -p(k) \cdot \log_2 q(k)$.
   Then
   (v) $\sum p_1 \leq \sum q_3$,
   (vi)   for every k such that $k \in \operatorname{dom} p$ holds $p(k) = q(k)$ iff $\sum p_1 = \sum q_3$, and
   (vii)   there exists k such that $k \in \operatorname{dom} p$ and $p(k) \neq q(k)$ iff $\sum p_1 < \sum q_3$.

(58)   Let p be a non empty finite probability distribution finite sequence of elements of $\mathbb{R}$. Suppose that for every k such that $k \in \operatorname{dom} p$ holds $p(k) > 0$. Then

   (i)   Entropy $p \leq \log_2 \operatorname{len} p$,

   (ii)   for every k such that $k \in \operatorname{dom} p$ holds $p(k) = \frac{1}{\operatorname{len} p}$ iff Entropy $p = \log_2 \operatorname{len} p$, and

   (iii) there exists k such that $k \in \operatorname{dom} p$ and $p(k) \neq \frac{1}{\operatorname{len} p}$ iff Entropy $p < \log_2 \operatorname{len} p$.

(59)   For every nonnegative matrix M over $\mathbb{R}$ holds Mx2FinS $\overrightarrow{\operatorname{id} \log} M = \overrightarrow{\operatorname{id} \log}$ Mx2FinS M.

(60)   Let p, q be finite probability distribution finite sequences of elements of $\mathbb{R}$ and M be a matrix over $\mathbb{R}$. If $M = \operatorname{ColVec2Mx} p \cdot \operatorname{LineVec2Mx} q$, then SumAll $\overrightarrow{\operatorname{id} \log} M = \sum \overrightarrow{\operatorname{id} \log} p + \sum \overrightarrow{\operatorname{id} \log} q$.

Let us consider M_1. The entropy of joint probability of M_1 yields a real number and is defined as follows:

(Def. 10)   The entropy of joint probability of $M_1 = $ Entropy Mx2FinS M_1.

Next we state the proposition

(61)   Let p, q be finite probability distribution finite sequences of elements of $\mathbb{R}$. Then the entropy of joint probability of $\operatorname{ColVec2Mx} p \cdot \operatorname{LineVec2Mx} q = $ Entropy $p + $ Entropy q.

Let us consider M_1. The entropy of conditional probability of M_1 yields a finite sequence of elements of $\mathbb{R}$ and is defined by the conditions (Def. 11).

(Def. 11)(i)   len (the entropy of conditional probability of M_1) = len M_1, and

   (ii)   for every k such that $k \in \operatorname{dom}$ (the entropy of conditional probability of M_1) holds (the entropy of conditional probability of M_1)$(k) = $ Entropy Line(M_1, k).

One can prove the following propositions:

(62)   Let M be a non empty yielding conditional probability matrix over $\mathbb{R}$ and p be a finite sequence of elements of $\mathbb{R}$. Then $p = $ the entropy of conditional probability of M if and only if len $p = $ len M and for every k such that $k \in \operatorname{dom} p$ holds $p(k) = -\sum (\overrightarrow{\operatorname{id} \log} M)(k)$.

(63)   Let M be a non empty yielding conditional probability matrix over $\mathbb{R}$. Then the entropy of conditional probability of $M = -$LineSum $\overrightarrow{\operatorname{id} \log} M$.

(64)   Let p be finite probability distribution finite sequence of elements of $\mathbb{R}$ and M be a non empty yielding conditional probability matrix over $\mathbb{R}$. Suppose len $p = $ len M. Let M_3 be a matrix over $\mathbb{R}$. If $M_3 = \operatorname{Vec2DiagMx} p \cdot M$, then SumAll $\overrightarrow{\operatorname{id} \log} M_3 = \sum \overrightarrow{\operatorname{id} \log} p + \sum (p \bullet$ LineSum $\overrightarrow{\operatorname{id} \log} M)$.

(65)   Let p be finite probability distribution finite sequence of elements of $\mathbb{R}$ and M be a non empty yielding conditional probability matrix over

$\mathbb{R}$. Suppose $\operatorname{len} p = \operatorname{len} M$. Then the entropy of joint probability of $\operatorname{Vec2DiagMx} p \cdot M = \operatorname{Entropy} p + \sum(p \bullet$ the entropy of conditional probability of $M)$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] P. Billingsley. *Ergodic Theory and Information*. John Wiley & Sons, 1964.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[10] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[11] Shigeichi Hirasawa. *Information Theory*. Baifukan CO., 1996.
[12] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[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] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[16] Yatsuka Nakamura, Nobuyuki Tamaura, and Wenpai Chang. A theory of matrices of real elements. *Formalized Mathematics*, 14(**1**):21–28, 2006.
[17] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics*.
[18] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.
[19] Yasunari Shidama. The Taylor expansions. *Formalized Mathematics*, 12(**2**):195–200, 2004.
[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[21] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[22] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[25] Bo Zhang and Yatsuka Nakamura. The definition of finite sequences and matrices of probability, and addition of matrices of real elements. *Formalized Mathematics*, 14(**3**):101–108, 2006.

String Rewriting Systems

Michał Trybulec
Motorola Software Group
Cracow, Poland

Summary. Basing on the definitions from [15], semi-Thue systems, Thue systems, and direct derivations are introduced. Next, the standard reduction relation is defined that, in turn, is used to introduce derivations using the theory from [1]. Finally, languages generated by rewriting systems are defined as all strings reachable from an initial word. This is followed by the introduction of the equivalence of semi-Thue systems with respect to the initial word.

The notation and terminology used here are introduced in the following papers: [11], [13], [8], [16], [10], [4], [17], [14], [7], [18], [2], [1], [3], [12], [5], [6], and [9].

1. Preliminaries

We adopt the following convention: x denotes a set, k, l denote natural numbers, and p, q denote finite sequences.

Next we state two propositions:

(1)   If $k \notin \operatorname{dom} p$ and $k + 1 \in \operatorname{dom} p$, then $k = 0$.

(2)   If $k > \operatorname{len} p$ and $k \leq \operatorname{len}(p \frown q)$, then there exists l such that $k = \operatorname{len} p + l$ and $l \geq 1$ and $l \leq \operatorname{len} q$.

In the sequel R denotes a binary relation and p, q denote reduction sequences w.r.t. R.

Next we state two propositions:

(3)   If $k \geq 1$, then $p{\restriction}k$ is a reduction sequence w.r.t. R.

(4)   If $k \in \operatorname{dom} p$, then there exists q such that $\operatorname{len} q = k$ and $q(1) = p(1)$ and $q(\operatorname{len} q) = p(k)$.

2. Finite 0-sequence Yielding Functions and Finite Sequences

Let f be a function. We say that f is finite-0-sequence-yielding if and only if:

(Def. 1)   If $x \in \operatorname{dom} f$, then $f(x)$ is a finite 0-sequence.

Let us mention that $\emptyset$ is finite-0-sequence-yielding.

Let f be a finite 0-sequence. Observe that $\langle f \rangle$ is finite-0-sequence-yielding.

Let us observe that there exists a function which is finite-0-sequence-yielding.

Let p be a finite-0-sequence-yielding function and let us consider x. Then $p(x)$ is a finite 0-sequence.

One can verify that there exists a finite sequence which is finite-0-sequence-yielding.

Let E be a set. Note that every finite sequence of elements of E^{ω} is finite-0-sequence-yielding.

Let p, q be finite-0-sequence-yielding finite sequences. Observe that $p \frown q$ is finite-0-sequence-yielding.

3. Concatenation of a Finite 0-sequence with All Elements of a Finite 0-sequence Yielding Function

Let s be a finite 0-sequence and let p be a finite-0-sequence-yielding function. The functor $s + p$ yields a finite-0-sequence-yielding function and is defined by:

(Def. 2) $\operatorname{dom}(s + p) = \operatorname{dom} p$ and for every x such that $x \in \operatorname{dom} p$ holds $(s + p)(x) = s \frown p(x)$.

The functor $p + s$ yielding a finite-0-sequence-yielding function is defined by:

(Def. 3) $\operatorname{dom}(p + s) = \operatorname{dom} p$ and for every x such that $x \in \operatorname{dom} p$ holds $(p + s)(x) = p(x) \frown s$.

Let s be a finite 0-sequence and let p be a finite-0-sequence-yielding finite sequence. Note that $s + p$ is finite sequence-like and $p + s$ is finite sequence-like.

We adopt the following convention: E denotes a set, s, t denote finite 0-sequences, and p, q denote finite-0-sequence-yielding finite sequences.

The following propositions are true:

(5) $\operatorname{len}(s + p) = \operatorname{len} p$ and $\operatorname{len}(p + s) = \operatorname{len} p$.

(6) $\langle\rangle_E + p = p$ and $p + \langle\rangle_E = p$.

(7) $s + (t + p) = s \frown t + p$ and $p + t + s = p + t \frown s$.

(8) $s + (p + t) = (s + p) + t$.

(9) $s + p \frown q = (s + p) \frown (s + q)$ and $p \frown q + s = (p + s) \frown (q + s)$.

4. Semi-Thue Systems and Thue Systems

Let E be a set, let p be a finite sequence of elements of E^ω, and let k be a natural number. Then $p(k)$ is an element of E^ω.

Let E be a set, let k be a natural number, and let s be an element of E^ω. Then $k \mapsto s$ is a finite sequence of elements of E^ω.

Let E be a set, let s be an element of E^ω, and let p be a finite sequence of elements of E^ω. Then $s + p$ is a finite sequence of elements of E^ω. Then $p + s$ is a finite sequence of elements of E^ω.

Let E be a set. A semi-Thue-system of E is a binary relation on E^ω.

In the sequel E is a set and S, T, U are semi-Thue-systems of E.

Let S be a binary relation. Observe that $S \cup S^{\smile}$ is symmetric.

Let us consider E. One can check that there exists a semi-Thue-system of E which is symmetric.

Let E be a set. A Thue-system of E is a symmetric semi-Thue-system of E.

5. Direct Derivations

We follow the rules: s, t, s_1, t_1, u, v, w are elements of E^ω and p is a finite sequence of elements of E^ω.

Let us consider E, S, s, t. The predicate $s \to_S t$ is defined by:

(Def. 4) $\langle s, t \rangle \in S$.

Let us consider E, S, s, t. The predicate $s \Rightarrow_S t$ is defined as follows:

(Def. 5)   There exist v, w, s_1, t_1 such that $s = v \frown s_1 \frown w$ and $t = v \frown t_1 \frown w$ and $s_1 \to_S t_1$.

The following propositions are true:

(10)   If $s \to_S t$, then $s \Rightarrow_S t$.

(11)   If $s \Rightarrow_S s$, then there exist v, w, s_1 such that $s = v \frown s_1 \frown w$ and $s_1 \to_S s_1$.

(12)   If $s \Rightarrow_S t$, then $u \frown s \Rightarrow_S u \frown t$ and $s \frown u \Rightarrow_S t \frown u$.

(13)   If $s \Rightarrow_S t$, then $u \frown s \frown v \Rightarrow_S u \frown t \frown v$.

(14)   If $s \to_S t$, then $u \frown s \Rightarrow_S u \frown t$ and $s \frown u \Rightarrow_S t \frown u$.

(15)   If $s \to_S t$, then $u \frown s \frown v \Rightarrow_S u \frown t \frown v$.

(16)   If S is a Thue-system of E and $s \to_S t$, then $t \to_S s$.

(17)   If S is a Thue-system of E and $s \Rightarrow_S t$, then $t \Rightarrow_S s$.

(18)   If $S \subseteq T$ and $s \to_S t$, then $s \to_T t$.

(19)   If $S \subseteq T$ and $s \Rightarrow_S t$, then $s \Rightarrow_T t$.

(20) $s \not\Rightarrow_{\emptyset_{E^\omega, E^\omega}} t$.

(21)   If $s \Rightarrow_{S \cup T} t$, then $s \Rightarrow_S t$ or $s \Rightarrow_T t$.

6. Reduction Relation

Let us consider E. Then id_E is a binary relation on E.

Let us consider E, S. The functor $\Rightarrow_S$ yielding a binary relation on E^ω is defined as follows:

(Def. 6) $\langle s, t \rangle \in \Rightarrow_S$ iff $s \Rightarrow_S t$.

The following propositions are true:

(22) $S \subseteq \Rightarrow_S$.

(23)   Suppose p is a reduction sequence w.r.t. $\Rightarrow_S$. Then $p + u$ is a reduction sequence w.r.t. $\Rightarrow_S$ and $u + p$ is a reduction sequence w.r.t. $\Rightarrow_S$.

(24)   If p is a reduction sequence w.r.t. $\Rightarrow_S$, then $(t + p) + u$ is a reduction sequence w.r.t. $\Rightarrow_S$.

(25)   If S is a Thue-system of E, then $\Rightarrow_S = (\Rightarrow_S)^\smile$.

(26)   If $S \subseteq T$, then $\Rightarrow_S \subseteq \Rightarrow_T$.

(27) $\Rightarrow_{\mathrm{id}_{E^\omega}} = \mathrm{id}_{E^\omega}$.

(28) $\Rightarrow_{S \cup \mathrm{id}_{E^\omega}} = \Rightarrow_S \cup \mathrm{id}_{E^\omega}$.

(29) $\Rightarrow_{\emptyset_{E^\omega, E^\omega}} = \emptyset_{E^\omega, E^\omega}$.

(30)   If $s \Rightarrow_{\Rightarrow_S} t$, then $s \Rightarrow_S t$.

(31) $\Rightarrow_{\Rightarrow_S} = \Rightarrow_S$.

7. Derivations

Let us consider E, S, s, t. The predicate $s \Rightarrow_S^* t$ is defined by:

(Def. 7) $\Rightarrow_S$ reduces s to t.

One can prove the following propositions:

(32) $s \Rightarrow_S^* s$.

(33)   If $s \Rightarrow_S t$, then $s \Rightarrow_S^* t$.

(34)   If $s \to_S t$, then $s \Rightarrow_S^* t$.

(35)   If $s \Rightarrow_S^* t$ and $t \Rightarrow_S^* u$, then $s \Rightarrow_S^* u$.

(36)   If $s \Rightarrow_S^* t$, then $s \frown u \Rightarrow_S^* t \frown u$ and $u \frown s \Rightarrow_S^* u \frown t$.

(37)   If $s \Rightarrow_S^* t$, then $u \frown s \frown v \Rightarrow_S^* u \frown t \frown v$.

(38)   If $s \Rightarrow_S^* t$ and $u \Rightarrow_S^* v$, then $s \frown u \Rightarrow_S^* t \frown v$ and $u \frown s \Rightarrow_S^* v \frown t$.

(39)   If S is a Thue-system of E and $s \Rightarrow_S^* t$, then $t \Rightarrow_S^* s$.

(40)   If $S \subseteq T$ and $s \Rightarrow_S^* t$, then $s \Rightarrow_T^* t$.

(41) $s \Rightarrow_S^* t$ iff $s \Rightarrow_{S \cup \mathrm{id}_{E^\omega}}^* t$.

(42)   If $s \Rightarrow_{\emptyset_{E^\omega, E^\omega}}^* t$, then $s = t$.

(43)   If $s \Rightarrow_{\Rightarrow_S}^* t$, then $s \Rightarrow_S^* t$.

(44)   If $s \Rightarrow_S^* t$ and $u \Rightarrow_{\{\langle s,t \rangle\}} v$, then $u \Rightarrow_S^* v$.

(45)   If $s \Rightarrow_S^* t$ and $u \Rightarrow_{S \cup \{\langle s,t \rangle\}}^* v$, then $u \Rightarrow_S^* v$.

8. Languages Generated by Semi-Thue Systems

Let us consider E, S, w. The functor $\mathrm{Lang}(w, S)$ yields a subset of E^ω and is defined by:

(Def. 8) $\mathrm{Lang}(w, S) = \{s : w \Rightarrow_S^* s\}$.

Next we state two propositions:

(46) $s \in \mathrm{Lang}(w, S)$ iff $w \Rightarrow_S^* s$.

(47) $w \in \mathrm{Lang}(w, S)$.

Let E be a non empty set, let S be a semi-Thue-system of E, and let w be an element of E^ω. Note that $\mathrm{Lang}(w, S)$ is non empty.

We now state four propositions:

(48)   If $S \subseteq T$, then $\mathrm{Lang}(w, S) \subseteq \mathrm{Lang}(w, T)$.

(49) $\mathrm{Lang}(w, S) = \mathrm{Lang}(w, S \cup \mathrm{id}_{E^\omega})$.

(50) $\mathrm{Lang}(w, \emptyset_{E^\omega, E^\omega}) = \{w\}$.

(51) $\mathrm{Lang}(w, \mathrm{id}_{E^\omega}) = \{w\}$.

9. Equivalence of Semi-Thue Systems

Let us consider E, S, T, w. We say that S and T are equivalent wrt w if and only if:

(Def. 9) $\mathrm{Lang}(w, S) = \mathrm{Lang}(w, T)$.

The following propositions are true:

(52) S and S are equivalent wrt w.

(53)   If S and T are equivalent wrt w, then T and S are equivalent wrt w.

(54)   Suppose S and T are equivalent wrt w and T and U are equivalent wrt w. Then S and U are equivalent wrt w.

(55) S and $S \cup \mathrm{id}_{E^\omega}$ are equivalent wrt w.

(56)   Suppose S and T are equivalent wrt w and $S \subseteq U$ and $U \subseteq T$. Then S and U are equivalent wrt w and U and T are equivalent wrt w.

(57) S and $\Rightarrow_S$ are equivalent wrt w.

(58)   If S and T are equivalent wrt w and $\Rightarrow_{S \cup T}$ reduces w to s, then $\Rightarrow_S$ reduces w to s.

(59)   If S and T are equivalent wrt w and $w \Rightarrow_{S \cup T}^* s$, then $w \Rightarrow_S^* s$.

(60)   If S and T are equivalent wrt w, then S and $S \cup T$ are equivalent wrt w.

(61)   If $s \Rightarrow_S t$, then S and $S \cup \{\langle s, t\rangle\}$ are equivalent wrt w.

(62)   If $s \Rightarrow_S^* t$, then S and $S \cup \{\langle s, t\rangle\}$ are equivalent wrt w.

References

[1]   Grzegorz Bancerek. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.
[2]   Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3]   Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[4]   Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5]   Patricia L. Carlson and Grzegorz Bancerek. Context-free grammar – part 1. *Formalized Mathematics*, 2(**5**):683–687, 1991.
[6]   Markus Moschner. Basic notions and properties of orthoposets. *Formalized Mathematics*, 11(**2**):201–210, 2003.
[7]   Karol Pąk. The Catalan numbers. Part II. *Formalized Mathematics*, 14(**4**):153–159, 2006.
[8]   Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[9]   Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[10] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[12] Michał Trybulec. Formal languages – concatenation and closure. *Formalized Mathematics*, 15(**1**):11–15, 2007.
[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[14] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.
[15] William M. Waite and Gerhard Goos. *Compiler Construction*. Springer-Verlag New York Inc., 1984.
[16] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[17] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[18] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Determinant and Inverse of Matrices of Real Elements

Nobuyuki Tamura
Shinshu University
Nagano, Japan

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Summary. In this paper the classic theory of matrices of real elements (see e.g. [12], [13]) is developed. We prove selected equations that have been proved previously for matrices of field elements. Similarly, we introduce in this special context the determinant of a matrix, the identity and zero matrices, and the inverse matrix. The new concept discussed in the case of matrices of real numbers is the property of matrices as operators acting on finite sequences of real numbers from both sides. The relations of invertibility of matrices and the "onto" property of matrices as operators are discussed.

The articles [24], [30], [9], [2], [22], [31], [7], [4], [5], [8], [3], [6], [28], [26], [21], [14], [29], [32], [23], [25], [27], [15], [34], [33], [19], [16], [11], [18], [20], [10], [17], [1], and [35] provide the terminology and notation for this paper.

1. Preliminaries

We use the following convention: D denotes a non empty set, k, n, m, i, j, l denote elements of $\mathbb{N}$, and K denotes a field.

We now state several propositions:

(1) For all finite sequences x, y of elements of $\mathbb{R}$ such that $\operatorname{len} x = \operatorname{len} y$ and $x + y = \underbrace{\langle 0, \ldots, 0 \rangle}_{\operatorname{len} x}$ holds $x = -y$ and $y = -x$.

(2) Let A be a matrix over D and p be a finite sequence of elements of D. If $p = A(i)$ and $1 \le i$ and $i \le \operatorname{len} A$ and $1 \le j$ and $j \le \operatorname{width} A$ and $\operatorname{len} p = \operatorname{width} A$, then $A_{i,j} = p(j)$.

(3)   Let a be a real number and A be a matrix over $\mathbb{R}$. Suppose $\operatorname{len}(a \cdot A) = \operatorname{len} A$ and $\operatorname{width}(a \cdot A) = \operatorname{width} A$ and $\langle i, j \rangle \in$ the indices of A. Then $(a \cdot A)_{i,j} = a \cdot A_{i,j}$.

(4)   For all matrices A, B over $\mathbb{R}$ of dimension n holds $\operatorname{len}(A \cdot B) = \operatorname{len} A$ and $\operatorname{width}(A \cdot B) = \operatorname{width} B$ and $\operatorname{len}(A \cdot B) = n$ and $\operatorname{width}(A \cdot B) = n$.

(5)   For every real number a and for every matrix A over $\mathbb{R}$ holds $\operatorname{len}(a \cdot A) = \operatorname{len} A$ and $\operatorname{width}(a \cdot A) = \operatorname{width} A$.

2. Calculation of Matrices

We now state the proposition

(6)   Let A, B be matrices over $\mathbb{R}$. Suppose $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$. Then $\operatorname{len}(A - B) = \operatorname{len} A$ and $\operatorname{width}(A - B) = \operatorname{width} A$ and for all i, j such that $\langle i, j \rangle \in$ the indices of A holds $(A - B)_{i,j} = A_{i,j} - B_{i,j}$.

Let us consider n and let A, B be matrices over $\mathbb{R}$ of dimension n. Then $A \cdot B$ is a matrix over $\mathbb{R}$ of dimension n.

The following propositions are true:

(7)   For all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$ holds $A + (B - B) = A$.

(8)   For all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$ holds $(A + B) - B = A$.

(9)   For every matrix A over $\mathbb{R}$ holds $(-1) \cdot A = -A$.

(10)   For every matrix A over $\mathbb{R}$ and for all elements i, j of $\mathbb{N}$ such that $\langle i, j \rangle \in$ the indices of A holds $(-A)_{i,j} = -A_{i,j}$.

(11)   For all real numbers a, b and for every matrix A over $\mathbb{R}$ holds $(a \cdot b) \cdot A = a \cdot (b \cdot A)$.

(12)   For all real numbers a, b and for every matrix A over $\mathbb{R}$ holds $(a + b) \cdot A = a \cdot A + b \cdot A$.

(13)   For all real numbers a, b and for every matrix A over $\mathbb{R}$ holds $(a - b) \cdot A = a \cdot A - b \cdot A$.

(14)   For every matrix A over K such that $n > 0$ and $\operatorname{len} A > 0$ holds
$$\begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_K^{n \times (\operatorname{len} A)} \cdot A = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_K^{n \times (\operatorname{width} A)} .$$

(15)   For all matrices A, C over K such that $\operatorname{len} A = \operatorname{width} C$ and $\operatorname{len} C > 0$ and $\operatorname{len} A > 0$ holds $(-C) \cdot A = -C \cdot A$.

(16)   For all matrices A, B, C over K such that $\operatorname{len} B = \operatorname{len} C$ and $\operatorname{width} B = \operatorname{width} C$ and $\operatorname{len} A = \operatorname{width} B$ and $\operatorname{len} B > 0$ and $\operatorname{len} A > 0$ holds $(B - C) \cdot A = B \cdot A - C \cdot A$.

(17) For all matrices A, B, C over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} C = \operatorname{width} A$ and $\operatorname{len} A > 0$ and $\operatorname{len} C > 0$ holds $(A - B) \cdot C = A \cdot C - B \cdot C$.

(18) For every element m of $\mathbb{N}$ and for all matrices A, C over K such that $\operatorname{width} A > 0$ and $\operatorname{len} A > 0$ holds $A \cdot \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_K^{(\operatorname{width} A) \times m} = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_K^{(\operatorname{len} A) \times m}$.

(19) For all matrices A, C over K such that $\operatorname{width} A = \operatorname{len} C$ and $\operatorname{len} A > 0$ and $\operatorname{len} C > 0$ holds $A \cdot -C = -A \cdot C$.

(20) For all matrices A, B, C over K such that $\operatorname{len} B = \operatorname{len} C$ and $\operatorname{width} B = \operatorname{width} C$ and $\operatorname{len} B = \operatorname{width} A$ and $\operatorname{len} B > 0$ and $\operatorname{len} A > 0$ holds $A \cdot (B - C) = A \cdot B - A \cdot C$.

(21) For all matrices A, B, C over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{width} C = \operatorname{len} A$ and $\operatorname{len} C > 0$ and $\operatorname{len} A > 0$ holds $C \cdot (A - B) = C \cdot A - C \cdot B$.

(22) Let A, B, C be matrices over $\mathbb{R}$. Suppose that
  (i) $\operatorname{len} A = \operatorname{len} B$,
  (ii) $\operatorname{width} A = \operatorname{width} B$,
  (iii) $\operatorname{len} C = \operatorname{len} A$,
  (iv) $\operatorname{width} C = \operatorname{width} A$, and
  (v) for all elements i, j of $\mathbb{N}$ such that $\langle i, j \rangle \in$ the indices of A holds $C_{i,j} = A_{i,j} - B_{i,j}$.
  Then $C = A - B$.

(23) For all finite sequences x_1, x_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} x_1 > 0$ holds $\operatorname{LineVec2Mx}(x_1 - x_2) = \operatorname{LineVec2Mx} x_1 - \operatorname{LineVec2Mx} x_2$.

(24) For all finite sequences x_1, x_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} x_1 > 0$ holds $\operatorname{ColVec2Mx}(x_1 - x_2) = \operatorname{ColVec2Mx} x_1 - \operatorname{ColVec2Mx} x_2$.

(25) Let A, B be matrices over $\mathbb{R}$. Suppose $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$. Let i be a natural number. If $1 \le i$ and $i \le \operatorname{len} A$, then $\operatorname{Line}(A - B, i) = \operatorname{Line}(A, i) - \operatorname{Line}(B, i)$.

(26) Let A, B be matrices over $\mathbb{R}$. Suppose $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$. Let i be a natural number. If $1 \le i$ and $i \le \operatorname{width} A$, then $(A - B)_{\square,i} = A_{\square,i} - B_{\square,i}$.

(27) Let A be a matrix over $\mathbb{R}$ of dimension $n \times k$, B be a matrix over $\mathbb{R}$ of

dimension $k \times m$, and C be a matrix over $\mathbb{R}$ of dimension $m \times l$. If $n > 0$ and $k > 0$ and $m > 0$, then $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

(28) For all matrices A, B, C over $\mathbb{R}$ of dimension n holds $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

(29) For every matrix A over D of dimension n holds $(A^{\mathrm{T}})^{\mathrm{T}} = A$.

(30) For all matrices A, B over $\mathbb{R}$ of dimension n holds $(A \cdot B)^{\mathrm{T}} = B^{\mathrm{T}} \cdot A^{\mathrm{T}}$.

(31) For every matrix A over $\mathbb{R}$ such that $n > 0$ and $\operatorname{len} A = n$ and $\operatorname{width} A = m$ holds $-A + A = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m}$.

3. Determinants

Let us consider n and let A be a matrix over $\mathbb{R}$ of dimension n. Then $(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})A$ is a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n.

Let us consider n and let A be a matrix over $\mathbb{R}$ of dimension n. The functor $\operatorname{Det} A$ yielding a real number is defined as follows:

(Def. 1) $\operatorname{Det} A = \operatorname{Det}(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})A$.

We now state a number of propositions:

(32) For every matrix A over $\mathbb{R}$ of dimension 2 holds $\operatorname{Det} A = A_{1,1} \cdot A_{2,2} - A_{1,2} \cdot A_{2,1}$.

(33) For all finite sequences s_1, s_2, s_3 such that $\operatorname{len} s_1 = n$ and $\operatorname{len} s_2 = n$ and $\operatorname{len} s_3 = n$ holds $\langle s_1, s_2, s_3 \rangle$ is tabular.

(34) Let p_1, p_2, p_3 be finite sequences of elements of D. Suppose $\operatorname{len} p_1 = n$ and $\operatorname{len} p_2 = n$ and $\operatorname{len} p_3 = n$. Then $\langle p_1, p_2, p_3 \rangle$ is a matrix over D of dimension $3 \times n$.

(35) For all elements a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3 of D holds $\langle \langle a_1, a_2, a_3 \rangle, \langle b_1, b_2, b_3 \rangle, \langle c_1, c_2, c_3 \rangle \rangle$ is a matrix over D of dimension 3.

(36) Let A be a matrix over D of dimension n, p be a finite sequence of elements of D, and i be a natural number. If $p = A(i)$ and $i \in \operatorname{Seg} n$, then $\operatorname{len} p = n$.

(37) For every matrix A over D of dimension 3 holds $A = \langle \langle A_{1,1}, A_{1,2}, A_{1,3} \rangle, \langle A_{2,1}, A_{2,2}, A_{2,3} \rangle, \langle A_{3,1}, A_{3,2}, A_{3,3} \rangle \rangle$.

(38) Let A be a matrix over $\mathbb{R}$ of dimension 3. Then $\operatorname{Det} A = (((A_{1,1} \cdot A_{2,2} \cdot A_{3,3} - A_{1,3} \cdot A_{2,2} \cdot A_{3,1} - A_{1,1} \cdot A_{2,3} \cdot A_{3,2}) + A_{1,2} \cdot A_{2,3} \cdot A_{3,1}) - A_{1,2} \cdot A_{2,1} \cdot A_{3,3}) + A_{1,3} \cdot A_{2,1} \cdot A_{3,2}$.

(39) For every permutation f of $\operatorname{Seg} 0$ holds $f = \varepsilon_{\mathbb{N}}$.

(40) The permutations of 0-element set $= \{\varepsilon_{\mathbb{N}}\}$.

(41) For every matrix A over K of dimension 0 holds $\operatorname{Det} A = 1_K$.

(42) For every matrix A over $\mathbb{R}$ of dimension 0 holds $\operatorname{Det} A = 1$.

(43) For every natural number n and for every matrix A over K of dimension n holds $\operatorname{Det} A = \operatorname{Det}(A^{\mathrm{T}})$.

(44) For every matrix A over $\mathbb{R}$ of dimension n holds $\operatorname{Det} A = \operatorname{Det}(A^{\mathrm{T}})$.

(45) For all matrices A, B over K of dimension n holds $\operatorname{Det}(A \cdot B) = \operatorname{Det} A \cdot \operatorname{Det} B$.

(46) For all matrices A, B over $\mathbb{R}$ of dimension n holds $\operatorname{Det}(A \cdot B) = \operatorname{Det} A \cdot \operatorname{Det} B$.

4. Matrix as Operator

We now state a number of propositions:

(47) Let x, y be finite sequences of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{len} A$ and $\operatorname{len} y = \operatorname{len} x$ and $\operatorname{len} x > 0$ and $\operatorname{len} A > 0$, then $(x - y) \cdot A = x \cdot A - y \cdot A$.

(48) Let x, y be finite sequences of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{width} A$ and $\operatorname{len} y = \operatorname{len} x$ and $\operatorname{len} x > 0$ and $\operatorname{len} A > 0$, then $A \cdot (x - y) = A \cdot x - A \cdot y$.

(49) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} A = \operatorname{len} x$ and $\operatorname{len} x > 0$ and $\operatorname{width} A > 0$, then $(-x) \cdot A = -x \cdot A$.

(50) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{width} A$ and $\operatorname{len} A > 0$ and $\operatorname{len} x > 0$, then $A \cdot -x = -A \cdot x$.

(51) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{len} A$ and $\operatorname{len} x > 0$ and $\operatorname{width} A > 0$, then $x \cdot -A = -x \cdot A$.

(52) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{width} A$ and $\operatorname{len} A > 0$ and $\operatorname{len} x > 0$, then $(-A) \cdot x = -A \cdot x$.

(53) Let a be a real number, x be a finite sequence of elements of $\mathbb{R}$, and A be a matrix over $\mathbb{R}$. If $\operatorname{width} A = \operatorname{len} x$ and $\operatorname{len} x > 0$ and $\operatorname{len} A > 0$, then $A \cdot (a \cdot x) = a \cdot (A \cdot x)$.

(54) Let x be a finite sequence of elements of $\mathbb{R}$ and A, B be matrices over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{len} A$ and $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$, then $x \cdot (A - B) = x \cdot A - x \cdot B$.

(55) Let x be a finite sequence of elements of $\mathbb{R}$ and A, B be matrices over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{width} A$ and $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} x > 0$ and $\operatorname{len} A > 0$, then $(A - B) \cdot x = A \cdot x - B \cdot x$.

(56) For every finite sequence x of elements of $\mathbb{R}$ and for every matrix A over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} x$ holds $\operatorname{LineVec2Mx} x \cdot A = \operatorname{LineVec2Mx}(x \cdot A)$.

(57) Let x be a finite sequence of elements of $\mathbb{R}$ and A, B be matrices over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{len} A$ and $\operatorname{width} A = \operatorname{len} B$, then $x \cdot (A \cdot B) = (x \cdot A) \cdot B$.

(58)   Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If width $A = \operatorname{len} x$ and $\operatorname{len} x > 0$ and $\operatorname{len} A > 0$, then $A \cdot \operatorname{ColVec2Mx} x = \operatorname{ColVec2Mx}(A \cdot x)$.

(59)   Let x be a finite sequence of elements of $\mathbb{R}$ and A, B be matrices over $\mathbb{R}$. If $\operatorname{len} x = \operatorname{width} B$ and $\operatorname{width} A = \operatorname{len} B$ and $\operatorname{len} x > 0$ and $\operatorname{len} B > 0$, then $(A \cdot B) \cdot x = A \cdot (B \cdot x)$.

(60)   Let B be a matrix over $\mathbb{R}$ of dimension $n \times m$ and A be a matrix over $\mathbb{R}$ of dimension $m \times k$. Suppose $n > 0$. Let given i, j. If $\langle i,\, j \rangle \in$ the indices of $B \cdot A$, then $(B \cdot A)_{i,j} = (\operatorname{Line}(B, i) \cdot A)(j)$.

(61)   Let A, B be matrices over $\mathbb{R}$ of dimension n and given i, j. If $\langle i,\, j \rangle \in$ the indices of $B \cdot A$, then $(B \cdot A)_{i,j} = (\operatorname{Line}(B, i) \cdot A)(j)$.

(62)   Let A, B be matrices over $\mathbb{R}$ of dimension n. Suppose $n > 0$. Let given i, j. If $\langle i,\, j \rangle \in$ the indices of $A \cdot B$, then $(A \cdot B)_{i,j} = (A \cdot B_{\square,j})(i)$.

5. Identity and Zero of Matrix of $\mathbb{R}$

Let n be an element of $\mathbb{N}$. The functor $1_{\mathbb{R}} \operatorname{matrix}(n)$ yields a matrix over $\mathbb{R}$ of dimension n and is defined as follows:

(Def. 2) $1_{\mathbb{R}} \operatorname{matrix}(n) = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})\left(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_{\mathbb{R}_{\mathrm{F}}}\right)$.

One can prove the following propositions:

(63)(i)   For every i such that $\langle i,\, i \rangle \in$ the indices of $1_{\mathbb{R}} \operatorname{matrix}(n)$ holds $(1_{\mathbb{R}} \operatorname{matrix}(n))_{i,i} = 1$, and

(ii)   for all i, j such that $\langle i,\, j \rangle \in$ the indices of $1_{\mathbb{R}} \operatorname{matrix}(n)$ and $i \neq j$ holds $(1_{\mathbb{R}} \operatorname{matrix}(n))_{i,j} = 0$.

(64) $(1_{\mathbb{R}} \operatorname{matrix}(n))^{\mathrm{T}} = 1_{\mathbb{R}} \operatorname{matrix}(n)$.

(65)   For all elements n, m of $\mathbb{N}$ such that $n > 0$ holds $\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}^{n \times m}_{\mathbb{R}} + \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}^{n \times m}_{\mathbb{R}} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}^{n \times m}_{\mathbb{R}}$.

(66)   For every real number a such that $n > 0$ holds $a \cdot \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}^{n \times m}_{\mathbb{R}} =$

$$\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m}.$$

(67) For every field K and for every matrix A over K holds $A \cdot$
$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_{K}^{\text{width } A \times \text{width } A} = A.$$

(68) For every matrix A over K holds $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_{K}^{\text{len } A \times \text{len } A} \cdot A = A$.

(69) For every matrix A over $\mathbb{R}$ holds if $n = \text{width } A$, then $A \cdot 1_{\mathbb{R}} \text{matrix}(n) = A$ and if $m = \text{len } A$, then $1_{\mathbb{R}} \text{matrix}(m) \cdot A = A$.

(70) For every matrix A over $\mathbb{R}$ of dimension n holds $1_{\mathbb{R}} \text{matrix}(n) \cdot A = A$.

(71) For every matrix A over $\mathbb{R}$ of dimension n holds $A \cdot 1_{\mathbb{R}} \text{matrix}(n) = A$.

(72) Det $1_{\mathbb{R}} \text{matrix}(n) = 1$.

Let n be an element of $\mathbb{N}$. The functor $0_{\mathbb{R}} \text{matrix}(n)$ yields a matrix over $\mathbb{R}$ of dimension n and is defined by:

(Def. 3) $0_{\mathbb{R}} \text{matrix}(n) = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times n}.$

One can prove the following proposition

(73) If $n > 0$, then Det $0_{\mathbb{R}} \text{matrix}(n) = 0$.

Let us consider n and let us consider i. The base fin seq(n, i) yielding a finite sequence of elements of $\mathbb{R}$ is defined by:

(Def. 4)   The base fin seq(n, i) = Replace($n \mapsto (0 \textbf{ qua }$ element of $\mathbb{R}), i, 1$).

We now state several propositions:

(74) len (the base fin seq(n, i)) $= n$.

(75) If $1 \le i$ and $i \le n$, then (the base fin seq(n, i))$(i) = 1$.

(76) If $1 \le i$ and $i \le n$ and $1 \le j$ and $j \le n$ and $i \ne j$, then (the base fin seq(n, i))$(j) = 0$.

(77)(i)   The base fin seq(1, 1) $= \langle 1 \rangle$,
  (ii)   the base fin seq(2, 1) $= \langle 1, 0 \rangle$,
  (iii)   the base fin seq(2, 2) $= \langle 0, 1 \rangle$,
  (iv)   the base fin seq(3, 1) $= \langle 1, 0, 0 \rangle$,
  (v)   the base fin seq(3, 2) $= \langle 0, 1, 0 \rangle$, and
  (vi)   the base fin seq(3, 3) $= \langle 0, 0, 1 \rangle$.

(78) If $1 \le i$ and $i \le n$, then $(1_{\mathbb{R}} \text{matrix}(n))(i) =$ the base fin seq(n, i).

6. Inverse of Matrix

Let n be an element of $\mathbb{N}$ and let A be a matrix over $\mathbb{R}$ of dimension n. We say that A is invertible if and only if:

(Def. 5) There exists a matrix B over $\mathbb{R}$ of dimension n such that $B \cdot A = 1_{\mathbb{R}} \operatorname{matrix}(n)$ and $A \cdot B = 1_{\mathbb{R}} \operatorname{matrix}(n)$.

Let n be an element of $\mathbb{N}$ and let A be a matrix over $\mathbb{R}$ of dimension n. Let us assume that A is invertible. The functor $\operatorname{Inv} A$ yields a matrix over $\mathbb{R}$ of dimension n and is defined as follows:

(Def. 6) $\operatorname{Inv} A \cdot A = 1_{\mathbb{R}} \operatorname{matrix}(n)$ and $A \cdot \operatorname{Inv} A = 1_{\mathbb{R}} \operatorname{matrix}(n)$.

Let us consider n. Note that $1_{\mathbb{R}} \operatorname{matrix}(n)$ is invertible.

We now state a number of propositions:

(79) $\operatorname{Inv} 1_{\mathbb{R}} \operatorname{matrix}(n) = 1_{\mathbb{R}} \operatorname{matrix}(n)$.

(80) For all matrices A, B_1, B_2 over $\mathbb{R}$ of dimension n such that $B_1 \cdot A = 1_{\mathbb{R}} \operatorname{matrix}(n)$ and $A \cdot B_2 = 1_{\mathbb{R}} \operatorname{matrix}(n)$ holds $B_1 = B_2$ and A is invertible.

(81) For every matrix A over $\mathbb{R}$ of dimension n such that A is invertible holds $\operatorname{Det} \operatorname{Inv} A = \operatorname{Det} A^{-1}$.

(82) For every matrix A over $\mathbb{R}$ of dimension n such that A is invertible holds $\operatorname{Det} A \neq 0$.

(83) Let A, B be matrices over $\mathbb{R}$ of dimension n. Suppose A is invertible and B is invertible. Then $A \cdot B$ is invertible and $\operatorname{Inv} A \cdot B = \operatorname{Inv} B \cdot \operatorname{Inv} A$.

(84) For every matrix A over $\mathbb{R}$ of dimension n such that A is invertible holds $\operatorname{Inv} \operatorname{Inv} A = A$.

(85) $1_{\mathbb{R}} \operatorname{matrix}(0) = 0_{\mathbb{R}} \operatorname{matrix}(0)$ and $1_{\mathbb{R}} \operatorname{matrix}(0) = \emptyset$.

(86) For every finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x = n$ and $n > 0$ holds $1_{\mathbb{R}} \operatorname{matrix}(n) \cdot x = x$.

(87) Let n be an element of $\mathbb{N}$, x, y be finite sequences of elements of $\mathbb{R}$, and A be a matrix over $\mathbb{R}$ of dimension n. Suppose A is invertible and $\operatorname{len} x = n$ and $\operatorname{len} y = n$ and $n > 0$. Then $A \cdot x = y$ if and only if $x = \operatorname{Inv} A \cdot y$.

(88) For every finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x = n$ holds $x \cdot 1_{\mathbb{R}} \operatorname{matrix}(n) = x$.

(89) Let x, y be finite sequences of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$ of dimension n. Suppose A is invertible and $\operatorname{len} x = n$ and $\operatorname{len} y = n$. Then $x \cdot A = y$ if and only if $x = y \cdot \operatorname{Inv} A$.

(90) Let A be a matrix over $\mathbb{R}$ of dimension n. Suppose $n > 0$ and A is invertible. Let y be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} y = n$. Then there exists a finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x = n$ and $A \cdot x = y$.

(91)   Let A be a matrix over $\mathbb{R}$ of dimension n. Suppose A is invertible. Let y be a finite sequence of elements of $\mathbb{R}$. Suppose $\operatorname{len} y = n$. Then there exists a finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x = n$ and $x \cdot A = y$.

(92)   Let A be a matrix over $\mathbb{R}$ of dimension n and x, y be finite sequences of elements of $\mathbb{R}$. Suppose $\operatorname{len} x = n$ and $\operatorname{len} y = n$ and $x \cdot A = y$. Let j be an element of $\mathbb{N}$. If $1 \leq j$ and $j \leq n$, then $y(j) = |(x, A_{\square, j})|$.

(93)   Let A be a matrix over $\mathbb{R}$ of dimension n. Suppose that for every finite sequence y of elements of $\mathbb{R}$ such that $\operatorname{len} y = n$ there exists a finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x = n$ and $x \cdot A = y$. Then there exists a matrix B over $\mathbb{R}$ of dimension n such that $B \cdot A = 1_{\mathbb{R}} \operatorname{matrix}(n)$.

(94)   Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$ of dimension n. If $n > 0$ and $\operatorname{len} x = n$, then $A^{\mathrm{T}} \cdot x = x \cdot A$.

(95)   Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$ of dimension n. If $n > 0$ and $\operatorname{len} x = n$, then $x \cdot A^{\mathrm{T}} = A \cdot x$.

(96)   Let A be a matrix over $\mathbb{R}$ of dimension n. Suppose that

(i) $n > 0$, and

(ii)   for every finite sequence y of elements of $\mathbb{R}$ such that $\operatorname{len} y = n$ there exists a finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x = n$ and $A \cdot x = y$. Then there exists a matrix B over $\mathbb{R}$ of dimension n such that $A \cdot B = 1_{\mathbb{R}} \operatorname{matrix}(n)$.

(97)   Let A be a matrix over $\mathbb{R}$ of dimension n. Suppose that

(i) $n > 0$, and

(ii)   for every finite sequence y of elements of $\mathbb{R}$ such that $\operatorname{len} y = n$ there exist finite sequences x_1, x_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 = n$ and $\operatorname{len} x_2 = n$ and $A \cdot x_1 = y$ and $x_2 \cdot A = y$.
Then A is invertible.

References

[1] Kanchun   and Yatsuka Nakamura. The inner product of finite sequences and of points of n-dimensional topological space. *Formalized Mathematics*, 11(**2**):179–183, 2003.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[5] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[11] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[12] Shigeru Furuya. *Matrix and Determinant*. Baifuukan (in Japanese), 1957.
[13] Felix R. Gantmacher. *The Theory of Matrices*. AMS Chelsea Publishing, 1959.
[14] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[15] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[16] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[17] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[18] Yatsuka Nakamura. Determinant of some matrices of field elements. *Formalized Mathematics*, 14(**1**):1–5, 2006.
[19] Yatsuka Nakamura, Nobuyuki Tamaura, and Wenpai Chang. A theory of matrices of real elements. *Formalized Mathematics*, 14(**1**):21–28, 2006.
[20] Yatsuka Nakamura and Hiroshi Yamazaki. Calculation of matrices of field elements. Part I. *Formalized Mathematics*, 11(**4**):385–391, 2003.
[21] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics*.
[22] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[23] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[24] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[25] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.
[26] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[27] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[28] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[30] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[31] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[32] Hiroshi Yamazaki, Yoshinori Fujisawa, and Yatsuka Nakamura. On replace function and swap function for finite sequences. *Formalized Mathematics*, 9(**3**):471–474, 2001.
[33] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.
[34] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.
[35] Bo Zhang and Yatsuka Nakamura. The definition of finite sequences and matrices of probability, and addition of matrices of real elements. *Formalized Mathematics*, 14(**3**):101–108, 2006.

The Rank+Nullity Theorem

Jesse Alama
Department of Philosophy
Stanford University
USA

Summary. The rank+nullity theorem states that, if T is a linear transformation from a finite-dimensional vector space V to a finite-dimensional vector space W, then $\dim(V) = \operatorname{rank}(T) + \operatorname{nullity}(T)$, where $\operatorname{rank}(T) = \dim(\operatorname{im}(T))$ and $\operatorname{nullity}(T) = \dim(\ker(T))$. The proof treated here is standard; see, for example, [14]: take a basis A of $\ker(T)$ and extend it to a basis B of V, and then show that $\dim(\operatorname{im}(T))$ is equal to $|B - A|$, and that T is one-to-one on $B - A$.

The articles [21], [11], [32], [22], [19], [33], [34], [7], [2], [17], [10], [18], [8], [9], [20], [1], [12], [3], [5], [6], [27], [29], [24], [31], [25], [13], [4], [30], [28], [26], [23], [15], [16], and [35] provide the notation and terminology for this paper.

1. Preliminaries

One can prove the following three propositions:

(1)   For all functions f, g such that g is one-to-one and $f {\restriction} \operatorname{rng} g$ is one-to-one and $\operatorname{rng} g \subseteq \operatorname{dom} f$ holds $f \cdot g$ is one-to-one.

(2)   For every function f and for all sets X, Y such that $X \subseteq Y$ and $f{\restriction}Y$ is one-to-one holds $f{\restriction}X$ is one-to-one.

(3)   Let V be a 1-sorted structure and X, Y be subsets of V. Then X meets Y if and only if there exists an element v of V such that $v \in X$ and $v \in Y$.

In the sequel F is a field and V, W are vector spaces over F.

Let F be a field and let V be a finite dimensional vector space over F. One can verify that there exists a basis of V which is finite.

137

Let F be a field and let V, W be vector spaces over F. Note that there exists a function from V into W which is linear.

Next we state three propositions:

(4)   If Ω_V is finite, then V is finite dimensional.

(5)   For every finite dimensional vector space V over F such that $\overline{\overline{\Omega_V}} = 1$ holds $\dim(V) = 0$.

(6)   If $\overline{\overline{\Omega_V}} = 2$, then $\dim(V) = 1$.

2. BASIC FACTS OF LINEAR TRANSFORMATIONS

Let F be a field and let V, W be vector spaces over F. A linear transformation from V to W is a linear function from V into W.

In the sequel T is a linear transformation from V to W.

One can prove the following propositions:

(7)   For all non empty 1-sorted structures V, W and for every function T from V into W holds $\operatorname{dom} T = \Omega_V$ and $\operatorname{rng} T \subseteq \Omega_W$.

(8)   For all elements x, y of V holds $T(x) - T(y) = T(x - y)$.

(9) $T(0_V) = 0_W$.

Let F be a field, let V, W be vector spaces over F, and let T be a linear transformation from V to W. The functor $\ker T$ yielding a strict subspace of V is defined as follows:

(Def. 1) $\Omega_{\ker T} = \{u; u \text{ ranges over elements of } V\colon T(u) = 0_W\}$.

We now state the proposition

(10)   For every element x of V holds $x \in \ker T$ iff $T(x) = 0_W$.

Let V, W be non empty 1-sorted structures, let T be a function from V into W, and let X be a subset of V. Then $T°X$ is a subset of W.

Let F be a field, let V, W be vector spaces over F, and let T be a linear transformation from V to W. The functor $\operatorname{im} T$ yielding a strict subspace of W is defined as follows:

(Def. 2) $\Omega_{\operatorname{im} T} = T°(\Omega_V)$.

The following propositions are true:

(11) $0_V \in \ker T$.

(12)   For every subset X of V holds $T°X$ is a subset of $\operatorname{im} T$.

(13)   For every element y of W holds $y \in \operatorname{im} T$ iff there exists an element x of V such that $y = T(x)$.

(14)   For every element x of $\ker T$ holds $T(x) = 0_W$.

(15)   If T is one-to-one, then $\ker T = \mathbf{0}_V$.

(16)   For every finite dimensional vector space V over F holds $\dim(\mathbf{0}_V) = 0$.

(17)   For all elements x, y of V such that $T(x) = T(y)$ holds $x - y \in \ker T$.

(18)   For every subset A of V and for all elements x, y of V such that $x - y \in$ $\mathrm{Lin}(A)$ holds $x \in \mathrm{Lin}(A \cup \{y\})$.

3. Some Lemmas on Linearly Independent Subsets, Linear Combinations, and Linear Transformations

One can prove the following propositions:

(19)   For every subset X of V such that V is a subspace of W holds X is a subset of W.

(20)   For every subset A of V such that A is linearly independent holds A is a basis of $\mathrm{Lin}(A)$.

(21)   For every subset A of V and for every element x of V such that $x \in$ $\mathrm{Lin}(A)$ and $x \notin A$ holds $A \cup \{x\}$ is linearly dependent.

(22)   For every subset A of V and for every basis B of V such that A is a basis of $\ker T$ and $A \subseteq B$ holds $T{\restriction}(B \setminus A)$ is one-to-one.

(23)   Let A be a subset of V, l be a linear combination of A, x be an element of V, and a be an element of F. Then $l +\cdot (x, a)$ is a linear combination of $A \cup \{x\}$.

Let V be a 1-sorted structure and let X be a subset of V. The functor $V \setminus X$ yields a subset of V and is defined by:

(Def. 3) $V \setminus X = \Omega_V \setminus X$.

Let F be a field, let V be a vector space over F, let l be a linear combination of V, and let X be a subset of V. Then $l^\circ X$ is a subset of F.

In the sequel l is a linear combination of V.

Let F be a field and let V be a vector space over F. Note that there exists a subset of V which is linearly dependent.

Let F be a field, let V be a vector space over F, let l be a linear combination of V, and let A be a subset of V. The functor $l[A]$ yields a linear combination of A and is defined by:

(Def. 4) $l[A] = l{\restriction}A +\cdot (V \setminus A \longmapsto 0_F)$.

The following propositions are true:

(24) $l = l[\text{the support of } l]$.

(25)   For every subset A of V and for every element v of V such that $v \in A$ holds $l[A](v) = l(v)$.

(26)   For every subset A of V and for every element v of V such that $v \notin A$ holds $l[A](v) = 0_F$.

(27)   For all subsets A, B of V and for every linear combination l of B such that $A \subseteq B$ holds $l = l[A] + l[B \setminus A]$.

Let F be a field, let V be a vector space over F, let l be a linear combination of V, and let X be a subset of V. Observe that $l°X$ is finite.

Let V, W be non empty 1-sorted structures, let T be a function from V into W, and let X be a subset of W. Then $T^{-1}(X)$ is a subset of V.

We now state the proposition

(28)   For every subset X of V such that X misses the support of l holds $l°X \subseteq \{0_F\}$.

Let F be a field, let V, W be vector spaces over F, let l be a linear combination of V, and let T be a linear transformation from V to W. The functor $T^{@}l$ yielding a linear combination of W is defined by:

(Def. 5)   For every element w of W holds $(T^{@}l)(w) = \sum(l°T^{-1}(\{w\}))$.

One can prove the following propositions:

(29) $T^{@}l$ is a linear combination of $T°$(the support of l).

(30)   The support of $T^{@}l \subseteq T°$(the support of l).

(31)   Let l, m be linear combinations of V. Suppose the support of l misses the support of m. Then the support of $l + m =$ (the support of l) $\cup$ (the support of m).

(32)   Let l, m be linear combinations of V. Suppose the support of l misses the support of m. Then the support of $l - m =$ (the support of l) $\cup$ (the support of m).

(33)   For all subsets A, B of V such that $A \subseteq B$ and B is a basis of V holds V is the direct sum of $\mathrm{Lin}(A)$ and $\mathrm{Lin}(B \setminus A)$.

(34)   Let A be a subset of V, l be a linear combination of A, and v be an element of V. Suppose $T{\restriction}A$ is one-to-one and $v \in A$. Then there exists a subset X of V such that X misses A and $T^{-1}(\{T(v)\}) = \{v\} \cup X$.

(35)   For every subset X of V such that X misses the support of l and $X \neq \emptyset$ holds $l°X = \{0_F\}$.

(36)   For every element w of W such that $w \in$ the support of $T^{@}l$ holds $T^{-1}(\{w\})$ meets the support of l.

(37)   Let v be an element of V. Suppose $T{\restriction}$(the support of l) is one-to-one and $v \in$ the support of l. Then $(T^{@}l)(T(v)) = l(v)$.

(38)   Let G be a finite sequence of elements of V. Suppose $\mathrm{rng}\,G =$ the support of l and $T{\restriction}$(the support of l) is one-to-one. Then $T \cdot (l\,G) = (T^{@}l)(T \cdot G)$.

(39)   If $T{\restriction}$(the support of l) is one-to-one, then $T°$(the support of l) $=$ the support of $T^{@}l$.

(40)   Let A be a subset of V, B be a basis of V, and l be a linear combination of $B \setminus A$. If A is a basis of $\ker T$ and $A \subseteq B$, then $T(\sum l) = \sum(T^{@}l)$.

(41)   Let X be a subset of V. Suppose X is linearly dependent. Then there exists a linear combination l of X such that the support of $l \neq \emptyset$ and

$\sum l = 0_V$.

Let F be a field, let V, W be vector spaces over F, let X be a subset of V, let T be a linear transformation from V to W, and let l be a linear combination of $T^\circ X$. Let us assume that $T{\upharpoonright}X$ is one-to-one. The functor $T\#l$ yields a linear combination of X and is defined as follows:

(Def. 6) $T\#l = l \cdot T + \cdot(V \setminus X \longmapsto 0_F)$.

We now state two propositions:

(42)   Let X be a subset of V, l be a linear combination of $T^\circ X$, and v be an element of V. If $v \in X$ and $T{\upharpoonright}X$ is one-to-one, then $(T\#l)(v) = l(T(v))$.

(43)   For every subset X of V and for every linear combination l of $T^\circ X$ such that $T{\upharpoonright}X$ is one-to-one holds $T^{\,@} T\#l = l$.

4. THE RANK+NULLITY THEOREM

Let F be a field, let V, W be finite dimensional vector spaces over F, and let T be a linear transformation from V to W. The functor $\operatorname{rank} T$ yielding a natural number is defined by:

(Def. 7) $\operatorname{rank} T = \dim(\operatorname{im} T)$.

The functor $\operatorname{nullity} T$ yields a natural number and is defined by:

(Def. 8) $\operatorname{nullity} T = \dim(\ker T)$.

Next we state two propositions:

(44)   Let V, W be finite dimensional vector spaces over F and T be a linear transformation from V to W. Then $\dim(V) = \operatorname{rank} T + \operatorname{nullity} T$.

(45)   Let V, W be finite dimensional vector spaces over F and T be a linear transformation from V to W. If T is one-to-one, then $\dim(V) = \operatorname{rank} T$.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[5] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[10] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[14] Serge Lang. *Algebra*. Springer, 3rd edition, 2005.

[15] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.

[16] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.

[17] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[18] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[20] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

[21] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[22] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[23] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.

[24] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[25] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.

[26] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.

[27] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[28] Wojciech A. Trybulec. Operations on subspaces in vector space. *Formalized Mathematics*, 1(**5**):871–876, 1990.

[29] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[30] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.

[31] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[32] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[33] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[34] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[35] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

Laplace Expansion

Karol Pąk
Institute of Computer Science
University of Białystok
Poland

Andrzej Trybulec
Institute of Computer Science
University of Białystok
Poland

Summary. In the article the formula for Laplace expansion is proved.

MML identifier: `LAPLACE`, version: `7.8.05 4.87.985`

The notation and terminology used in this paper are introduced in the following articles: [23], [11], [29], [20], [12], [30], [31], [6], [9], [7], [3], [4], [21], [28], [26], [15], [22], [10], [5], [13], [24], [14], [33], [25], [18], [34], [1], [8], [2], [16], [17], [27], [19], and [32].

1. Preliminaries

For simplicity, we follow the rules: x, y are sets, N is an element of $\mathbb{N}$, c, i, j, k, m, n are natural numbers, D is a non empty set, s is an element of $2\text{Set Seg}(n+2)$, p is an element of the permutations of n-element set, p_1, q_1 are elements of the permutations of $(n+1)$-element set, p_2 is an element of the permutations of $(n+2)$-element set, K is a field, a, b are elements of K, f is a finite sequence of elements of K, A is a matrix over K, A_1 is a matrix over D of dimension $n \times m$, p_3 is a finite sequence of elements of D, and M is a matrix over K of dimension n.

The following propositions are true:

(1) For every finite sequence f and for every natural number i such that $i \in \text{dom } f$ holds $\text{len}(f_{\upharpoonright i}) = \text{len } f -' 1$.

(2) Let i, j, n be natural numbers and M be a matrix over K of dimension n. If $i \in \text{dom } M$, then $\text{len }(\text{the deleting of } i\text{-row and } j\text{-column in } M) = n -' 1$.

(3) If $j \in \text{Seg width } A$, then $\text{width}(\text{the deleting of } j\text{-column in } A) = \text{width } A -' 1$.

(4) For every natural number i such that $\operatorname{len} A > 1$ holds $\operatorname{width} A = \operatorname{width}$ (the deleting of i-row in A).

(5) For every natural number i such that $j \in \operatorname{Seg} \operatorname{width} M$ holds width (the deleting of i-row and j-column in M) $= n -' 1$.

Let G be a non empty groupoid, let B be a function from $[:$ the carrier of G, $\mathbb{N}\,$:$]$ into the carrier of G, let g be an element of G, and let i be a natural number. Then $B(g, i)$ is an element of G.

One can prove the following propositions:

(6) $\overline{\overline{\text{the permutations of } n\text{-element set}}} = n!$.

(7) For all i, j such that $i \in \operatorname{Seg}(n + 1)$ and $j \in \operatorname{Seg}(n + 1)$ holds $\overline{\overline{\{p_1 : p_1(i) = j\}}} = n!$.

(8) Let K be a Fanoian field, given p_2, and X, Y be elements of $\operatorname{Fin} 2\operatorname{Set} \operatorname{Seg}(n + 2)$. Suppose $Y = \{s \ : \ s \ \in X \ \wedge \ (\text{Part-sgn}(p_2, K))(s) = -\mathbf{1}_K\}$. Then (the multiplication of K)-$\sum_X \text{Part-sgn}(p_2, K) = \text{power}_K(-\mathbf{1}_K, \operatorname{card} Y)$.

(9) Let K be a Fanoian field and given p_2, i, j. Suppose $i \in \operatorname{Seg}(n + 2)$ and $p_2(i) = j$. Then there exists an element X of $\operatorname{Fin} 2\operatorname{Set} \operatorname{Seg}(n+2)$ such that $X = \{\{N, i\} : \{N, i\} \in 2\operatorname{Set} \operatorname{Seg}(n + 2)\}$ and (the multiplication of K)-$\sum_X \text{Part-sgn}(p_2, K) = \text{power}_K(-\mathbf{1}_K, i + j)$.

(10) Let given i, j. Suppose $i \in \operatorname{Seg}(n + 1)$ and $j \in \operatorname{Seg}(n + 1)$ and $n \geq 2$. Then there exists a function P_1 from $2\operatorname{Set} \operatorname{Seg} n$ into $2\operatorname{Set} \operatorname{Seg}(n + 1)$ such that

   (i) $\operatorname{rng} P_1 = 2\operatorname{Set} \operatorname{Seg}(n + 1) \setminus \{\{N, i\} : \{N, i\} \in 2\operatorname{Set} \operatorname{Seg}(n + 1)\}$,

   (ii) P_1 is one-to-one, and

   (iii) for all k, m such that $k < m$ and $\{k, m\} \in 2\operatorname{Set} \operatorname{Seg} n$ holds if $m < i$ and $k < i$, then $P_1(\{k, m\}) = \{k, m\}$ and if $m \geq i$ and $k < i$, then $P_1(\{k, m\}) = \{k, m + 1\}$ and if $m \geq i$ and $k \geq i$, then $P_1(\{k, m\}) = \{k + 1, m + 1\}$.

(11) If $n < 2$, then for every element p of the permutations of n-element set holds p is even and $p = \operatorname{idseq}(n)$.

(12) Let X, Y, D be non empty sets, f be a function from X into $\operatorname{Fin} Y$, g be a function from $\operatorname{Fin} Y$ into D, and F be a binary operation on D. Suppose that

   (i) for all elements A, B of $\operatorname{Fin} Y$ such that A misses B holds $F(g(A), g(B)) = g(A \cup B)$,

   (ii) F is commutative and associative and has a unity, and

   (iii) $g(\emptyset) = \mathbf{1}_F$.

   Let I be an element of $\operatorname{Fin} X$. Suppose that for all x, y such that $x \in I$ and $y \in I$ and $f(x)$ meets $f(y)$ holds $x = y$. Then F-$\sum_I g \cdot f = F$-$\sum_{f \circ I} g$ and F-$\sum_{f \circ I} g = g(\bigcup(f^\circ I))$ and $\bigcup(f^\circ I)$ is an element of $\operatorname{Fin} Y$.

2. Auxiliary Notions

Let i, j, n be natural numbers, let us consider K, and let M be a matrix over K of dimension n. Let us assume that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} n$. The functor $\operatorname{Delete}(M, i, j)$ yielding a matrix over K of dimension $n -' 1$ is defined as follows:

(Def. 1) $\operatorname{Delete}(M, i, j) =$ the deleting of i-row and j-column in M.

The following propositions are true:

(13)   Let given i, j. Suppose $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} n$. Let given k, m such that $k \in \operatorname{Seg}(n -' 1)$ and $m \in \operatorname{Seg}(n -' 1)$. Then

  (i)   if $k < i$ and $m < j$, then $(\operatorname{Delete}(M, i, j))_{k,m} = M_{k,m}$,

  (ii)   if $k < i$ and $m \geq j$, then $(\operatorname{Delete}(M, i, j))_{k,m} = M_{k,m+1}$,

  (iii) if $k \geq i$ and $m < j$, then $(\operatorname{Delete}(M, i, j))_{k,m} = M_{k+1,m}$, and

  (iv)   if $k \geq i$ and $m \geq j$, then $(\operatorname{Delete}(M, i, j))_{k,m} = M_{k+1,m+1}$.

(14)   For all i, j such that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} n$ holds $(\operatorname{Delete}(M, i, j))^{\mathrm{T}} = \operatorname{Delete}(M^{\mathrm{T}}, j, i)$.

(15)   For every finite sequence f of elements of K and for all i, j such that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} n$ holds $\operatorname{Delete}(M, i, j) = \operatorname{Delete}(\operatorname{RLine}(M, i, f), i, j)$.

Let us consider c, n, m, D, let M be a matrix over D of dimension $n \times m$, and let p_3 be a finite sequence of elements of D. The functor $\operatorname{ReplaceCol}(M, c, p_3)$ yielding a matrix over D of dimension $n \times m$ is defined by:

(Def. 2)(i) $\operatorname{len} \operatorname{ReplaceCol}(M, c, p_3) = \operatorname{len} M$ and $\operatorname{width} \operatorname{ReplaceCol}(M, c, p_3) = \operatorname{width} M$ and for all i, j such that $\langle i, j \rangle \in$ the indices of M holds if $j \neq c$, then $(\operatorname{ReplaceCol}(M, c, p_3))_{i,j} = M_{i,j}$ and if $j = c$, then $(\operatorname{ReplaceCol}(M, c, p_3))_{i,c} = p_3(i)$ if $\operatorname{len} p_3 = \operatorname{len} M$,

  (ii) $\operatorname{ReplaceCol}(M, c, p_3) = M$, otherwise.

Let us consider c, n, m, D, let M be a matrix over D of dimension $n \times m$, and let p_3 be a finite sequence of elements of D. We introduce $\operatorname{RCol}(M, c, p_3)$ as a synonym of $\operatorname{ReplaceCol}(M, c, p_3)$.

We now state four propositions:

(16)   For every i such that $i \in \operatorname{Seg} \operatorname{width} A_1$ holds if $i = c$ and $\operatorname{len} p_3 = \operatorname{len} A_1$, then $(\operatorname{RCol}(A_1, c, p_3))_{\square,i} = p_3$ and if $i \neq c$, then $(\operatorname{RCol}(A_1, c, p_3))_{\square,i} = (A_1)_{\square,i}$.

(17)   If $c \notin \operatorname{Seg} \operatorname{width} A_1$, then $\operatorname{RCol}(A_1, c, p_3) = A_1$.

(18) $\operatorname{RCol}(A_1, c, (A_1)_{\square,c}) = A_1$.

(19)   Let A be a matrix over D of dimension $n \times m$ and A' be a matrix over D of dimension $m \times n$. If $A' = A^{\mathrm{T}}$ and if $m = 0$, then $n = 0$, then $\operatorname{ReplaceCol}(A, c, p_3) = (\operatorname{ReplaceLine}(A', c, p_3))^{\mathrm{T}}$.

3. Permutations

Let us consider i, n and let p_4 be an element of the permutations of $(n+1)$-element set. Let us assume that $i \in \operatorname{Seg}(n+1)$. The functor $\operatorname{Rem}(p_4, i)$ yielding an element of the permutations of n-element set is defined by the condition (Def. 3).

(Def. 3)   Let given k such that $k \in \operatorname{Seg} n$. Then
   (i)   if $k < i$, then if $p_4(k) < p_4(i)$, then $(\operatorname{Rem}(p_4, i))(k) = p_4(k)$ and if $p_4(k) \geq p_4(i)$, then $(\operatorname{Rem}(p_4, i))(k) = p_4(k) - 1$, and
   (ii)   if $k \geq i$, then if $p_4(k+1) < p_4(i)$, then $(\operatorname{Rem}(p_4, i))(k) = p_4(k+1)$ and if $p_4(k+1) \geq p_4(i)$, then $(\operatorname{Rem}(p_4, i))(k) = p_4(k+1) - 1$.

One can prove the following three propositions:

(20)   Let given i, j. Suppose $i \in \operatorname{Seg}(n+1)$ and $j \in \operatorname{Seg}(n+1)$. Let P be a set. Suppose $P = \{p_1 : p_1(i) = j\}$. Then there exists a function P_1 from P into the permutations of n-element set such that P_1 is bijective and for every q_1 such that $q_1(i) = j$ holds $P_1(q_1) = \operatorname{Rem}(q_1, i)$.

(21)   For all i, j such that $i \in \operatorname{Seg}(n+1)$ and $p_1(i) = j$ holds $(-1)^{\operatorname{sgn}(p_1)} a = \operatorname{power}_K(-\mathbf{1}_K, i+j) \cdot (-1)^{\operatorname{sgn}(\operatorname{Rem}(p_1, i))} a$.

(22)   Let given i, j. Suppose $i \in \operatorname{Seg}(n+1)$ and $p_1(i) = j$. Let M be a matrix over K of dimension $n+1$ and D_1 be a matrix over K of dimension n. Suppose $D_1 = \operatorname{Delete}(M, i, j)$. Then (the product on paths of M)(p_1) = $\operatorname{power}_K(-\mathbf{1}_K, i+j) \cdot M_{i,j} \cdot$ (the product on paths of D_1)$(\operatorname{Rem}(p_1, i))$.

4. Minors and Cofactors

Let i, j, n be natural numbers, let us consider K, and let M be a matrix over K of dimension n. The functor $\operatorname{Minor}(M, i, j)$ yielding an element of K is defined by:

(Def. 4) $\operatorname{Minor}(M, i, j) = \operatorname{Det} \operatorname{Delete}(M, i, j)$.

Let i, j, n be natural numbers, let us consider K, and let M be a matrix over K of dimension n. The functor $\operatorname{Cofactor}(M, i, j)$ yielding an element of K is defined as follows:

(Def. 5) $\operatorname{Cofactor}(M, i, j) = \operatorname{power}_K(-\mathbf{1}_K, i+j) \cdot \operatorname{Minor}(M, i, j)$.

The following propositions are true:

(23)   Let given i, j. Suppose $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} n$. Let P be an element of Fin (the permutations of n-element set). Suppose $P = \{p : p(i) = j\}$. Let M be a matrix over K of dimension n. Then (the addition of K)-$\sum_P$ (the product on paths of M) = $M_{i,j} \cdot \operatorname{Cofactor}(M, i, j)$.

(24)   For all i, j such that $i \in \operatorname{Seg} n$ and $j \in \operatorname{Seg} n$ holds $\operatorname{Minor}(M, i, j) = \operatorname{Minor}(M^{\mathrm{T}}, j, i)$.

Let us consider n, K and let M be a matrix over K of dimension n. The matrix of cofactor M yielding a matrix over K of dimension n is defined by the condition (Def. 6).

(Def. 6)   Let i, j be natural numbers. Suppose $\langle i, j \rangle \in$ the indices of the matrix of cofactor M. Then (the matrix of cofactor $M)_{i,j} = \text{Cofactor}(M, i, j)$.

5. Laplace Expansion

Let us consider n, i, K and let M be a matrix over K of dimension n. The functor $\text{LaplaceExpL}(M, i)$ yields a finite sequence of elements of K and is defined as follows:

(Def. 7) $\text{len}\,\text{LaplaceExpL}(M, i) = n$ and for every j such that $j \in \text{dom}\,\text{LaplaceExpL}(M, i)$ holds
$(\text{LaplaceExpL}(M, i))(j) = M_{i,j} \cdot \text{Cofactor}(M, i, j)$.

Let us consider n, let j be a natural number, let us consider K, and let M be a matrix over K of dimension n. The functor $\text{LaplaceExpC}(M, j)$ yields a finite sequence of elements of K and is defined by:

(Def. 8) $\text{len}\,\text{LaplaceExpC}(M, j) = n$ and for every i such that $i \in \text{dom}\,\text{LaplaceExpC}(M, j)$ holds $(\text{LaplaceExpC}(M, j))(i) = M_{i,j} \cdot \text{Cofactor}(M, i, j)$.

One can prove the following propositions:

(25)   For every natural number i and for every matrix M over K of dimension n such that $i \in \text{Seg}\,n$ holds $\text{Det}\,M = \sum \text{LaplaceExpL}(M, i)$.

(26)   For every i such that $i \in \text{Seg}\,n$ holds $\text{LaplaceExpC}(M, i) = \text{LaplaceExpL}(M^{\text{T}}, i)$.

(27)   For every natural number j and for every matrix M over K of dimension n such that $j \in \text{Seg}\,n$ holds $\text{Det}\,M = \sum \text{LaplaceExpC}(M, j)$.

(28)   For all p, i such that $\text{len}\,f = n$ and $i \in \text{Seg}\,n$ holds $\text{Line}(\text{the matrix of cofactor }M, i) \bullet f = \text{LaplaceExpL}(\text{RLine}(M, i, f), i)$.

(29)   If $i \in \text{Seg}\,n$, then $\text{Line}(M, j) \cdot ((\text{the matrix of cofactor }M)^{\text{T}})_{\square,i} = \text{Det}\,\text{RLine}(M, i, \text{Line}(M, j))$.

(30)   If $\text{Det}\,M \neq 0_K$, then $M \cdot (\text{Det}\,M^{-1} \cdot (\text{the matrix of cofactor }M)^{\text{T}}) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K \cdot$

(31)   For all f, i such that $\text{len}\,f = n$ and $i \in \text{Seg}\,n$ holds (the matrix of cofactor $M)_{\square,i} \bullet f = \text{LaplaceExpL}(\text{RLine}(M^{\text{T}}, i, f), i)$.

(32)   If $i \in \text{Seg}\,n$ and $j \in \text{Seg}\,n$, then $\text{Line}((\text{the matrix of cofactor }M)^{\text{T}}, i) \cdot M_{\square,j} = \text{Det}\,\text{RLine}(M^{\text{T}}, i, \text{Line}(M^{\text{T}}, j))$.

(33) If $\text{Det } M \neq 0_K$, then $\text{Det } M^{-1} \cdot (\text{the matrix of cofactor } M)^{\text{T}} \cdot M =$
$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}.$$

(34) M is invertible iff $\text{Det } M \neq 0_K$.

(35) If $\text{Det } M \neq 0_K$, then $M^{\smile} = \text{Det } M^{-1} \cdot (\text{the matrix of cofactor } M)^{\text{T}}$.

(36) Let M be a matrix over K of dimension n. Suppose M is invertible. Let given i, j. If $\langle i, j \rangle \in$ the indices of $M^{\smile}$, then $M^{\smile}_{i,j} = \text{Det } M^{-1} \cdot \text{power}_K(-\mathbf{1}_K, i + j) \cdot \text{Minor}(M, j, i)$.

(37) Let A be a matrix over K of dimension n. Suppose $\text{Det } A \neq 0_K$. Let x, b be matrices over K. Suppose $\text{len } x = n$ and $A \cdot x = b$. Then $x = A^{\smile} \cdot b$ and for all i, j such that $\langle i, j \rangle \in$ the indices of x holds $x_{i,j} = \text{Det } A^{-1} \cdot \text{Det ReplaceCol}(A, i, b_{\square,j})$.

(38) Let A be a matrix over K of dimension n. Suppose $\text{Det } A \neq 0_K$. Let x, b be matrices over K. Suppose $\text{width } x = n$ and $x \cdot A = b$. Then $x = b \cdot A^{\smile}$ and for all i, j such that $\langle i, j \rangle \in$ the indices of x holds $x_{i,j} = \text{Det } A^{-1} \cdot \text{Det ReplaceLine}(A, j, \text{Line}(b, i))$.

6. Product by a Vector

Let D be a non empty set and let f be a finite sequence of elements of D. Then $\langle f \rangle$ is a matrix over D of dimension $1 \times \text{len } f$.

Let us consider K, let M be a matrix over K, and let f be a finite sequence of elements of K. The functor $M \cdot f$ yielding a matrix over K is defined by:

(Def. 9) $M \cdot f = M \cdot \langle f \rangle^{\text{T}}$.

The functor $f \cdot M$ yields a matrix over K and is defined by:

(Def. 10) $f \cdot M = \langle f \rangle \cdot M$.

Next we state two propositions:

(39) Let A be a matrix over K of dimension n. Suppose $\text{Det } A \neq 0_K$. Let x, b be finite sequences of elements of K. Suppose $\text{len } x = n$ and $A \cdot x = \langle b \rangle^{\text{T}}$. Then $\langle x \rangle^{\text{T}} = A^{\smile} \cdot b$ and for every i such that $i \in \text{Seg } n$ holds $x(i) = \text{Det } A^{-1} \cdot \text{Det ReplaceCol}(A, i, b)$.

(40) Let A be a matrix over K of dimension n. Suppose $\text{Det } A \neq 0_K$. Let x, b be finite sequences of elements of K. Suppose $\text{len } x = n$ and $x \cdot A = \langle b \rangle$. Then $\langle x \rangle = b \cdot A^{\smile}$ and for every i such that $i \in \text{Seg } n$ holds $x(i) = \text{Det } A^{-1} \cdot \text{Det ReplaceLine}(A, i, b)$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[8] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Czesław Byliński. Semigroup operations on finite subsets. *Formalized Mathematics*, 1(**4**):651–656, 1990.

[11] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[13] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[14] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.

[15] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[16] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[17] Yatsuka Nakamura. Determinant of some matrices of field elements. *Formalized Mathematics*, 14(**1**):1–5, 2006.

[18] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[19] Karol Pąk. Basic properties of determinants of square matrices over a field. *Formalized Mathematics*, 15(**1**):17–25, 2007.

[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[22] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

[23] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[24] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

[25] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.

[26] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[27] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[28] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[29] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[30] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[31] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[32] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.

[33] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

[34] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Some Properties of Line and Column Operations on Matrices

Xiquan Liang
Qingdao University of Science
and Technology
China

Tao Sun
Qingdao University of Science
and Technology
China

Dahai Hu
Qingdao University of Science
and Technology
China

Summary. This article describes definitions of elementary operations about matrix and their main properties.

The articles [8], [13], [17], [11], [1], [18], [5], [6], [2], [7], [15], [16], [9], [10], [20], [4], [3], [21], [12], [14], and [19] provide the notation and terminology for this paper.

For simplicity, we adopt the following convention: j, k, l, n, m, i are natural numbers, K is a field, a is an element of K, M, M_1 are matrices over K of dimension $n \times m$, and A is a matrix over K of dimension n.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, and let l, k be natural numbers. The functor InterchangeLine(M, l, k) yielding a matrix over K of dimension $n \times m$ is defined by the conditions (Def. 1).

(Def. 1)(i)　len InterchangeLine$(M, l, k) = $ len M, and

(ii)　for all i, j such that $i \in \text{dom } M$ and $j \in \text{Seg width } M$ holds if $i = l$, then (InterchangeLine$(M, l, k))_{i,j} = M_{k,j}$ and if $i = k$, then (InterchangeLine$(M, l, k))_{i,j} = M_{l,j}$ and if $i \neq l$ and $i \neq k$, then (InterchangeLine$(M, l, k))_{i,j} = M_{i,j}$.

The following three propositions are true:

(1)   For all matrices M_1, M_2 over K of dimension $n \times m$ holds width $M_1 =$ width M_2.

(2)   Let given M, M_1, i such that $l \in \text{dom } M$ and $k \in \text{dom } M$ and $i \in \text{dom } M$ and $M_1 = \text{InterchangeLine}(M, l, k)$. Then

(i)   if $i = l$, then $\text{Line}(M_1, i) = \text{Line}(M, k)$,

(ii)   if $i = k$, then $\text{Line}(M_1, i) = \text{Line}(M, l)$, and

(iii)   if $i \neq l$ and $i \neq k$, then $\text{Line}(M_1, i) = \text{Line}(M, i)$.

(3)   For all a, i, j, M such that $i \in \text{dom } M$ and $j \in \text{Seg width } M$ holds $(a \cdot \text{Line}(M, i))(j) = a \cdot M_{i,j}$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l be a natural number, and let a be an element of K. The functor $\text{ScalarXLine}(M, l, a)$ yields a matrix over K of dimension $n \times m$ and is defined by the conditions (Def. 2).

(Def. 2)(i)   len $\text{ScalarXLine}(M, l, a) = \text{len } M$, and

(ii)   for all i, j such that $i \in \text{dom } M$ and $j \in \text{Seg width } M$ holds if $i = l$, then $(\text{ScalarXLine}(M, l, a))_{i,j} = a \cdot M_{l,j}$ and if $i \neq l$, then $(\text{ScalarXLine}(M, l, a))_{i,j} = M_{i,j}$.

We now state the proposition

(4)   If $l \in \text{dom } M$ and $i \in \text{dom } M$ and $a \neq 0_K$ and $M_1 = \text{ScalarXLine}(M, l, a)$, then if $i = l$, then $\text{Line}(M_1, i) = a \cdot \text{Line}(M, l)$ and if $i \neq l$, then $\text{Line}(M_1, i) = \text{Line}(M, i)$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l, k be natural numbers, and let a be an element of K. Let us assume that $l \in \text{dom } M$ and $k \in \text{dom } M$. The functor $\text{RlineXScalar}(M, l, k, a)$ yielding a matrix over K of dimension $n \times m$ is defined by the conditions (Def. 3).

(Def. 3)(i)   len $\text{RlineXScalar}(M, l, k, a) = \text{len } M$, and

(ii)   for all i, j such that $i \in \text{dom } M$ and $j \in \text{Seg width } M$ holds if $i = l$, then $(\text{RlineXScalar}(M, l, k, a))_{i,j} = a \cdot M_{k,j} + M_{l,j}$ and if $i \neq l$, then $(\text{RlineXScalar}(M, l, k, a))_{i,j} = M_{i,j}$.

We now state the proposition

(5)   If $l \in \text{dom } M$ and $k \in \text{dom } M$ and $i \in \text{dom } M$ and $M_1 = \text{RlineXScalar}(M, l, k, a)$, then if $i = l$, then $\text{Line}(M_1, i) = a \cdot \text{Line}(M, k) + \text{Line}(M, l)$ and if $i \neq l$, then $\text{Line}(M_1, i) = \text{Line}(M, i)$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, and let l, k be natural numbers. We introduce $\text{ILine}(M, l, k)$ as a synonym of $\text{InterchangeLine}(M, l, k)$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l be a natural number, and let a be an element of K. We

introduce $\mathrm{SXLine}(M, l, a)$ as a synonym of $\mathrm{ScalarXLine}(M, l, a)$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l, k be natural numbers, and let a be an element of K. We introduce $\mathrm{RLineXS}(M, l, k, a)$ as a synonym of $\mathrm{RlineXScalar}(M, l, k, a)$.

We now state several propositions:

(6) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$, then

$\mathrm{ILine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k) \cdot A = \mathrm{ILine}(A, l, k).$

(7) For all l, a, A such that $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$ and $a \neq 0_K$ holds

$\mathrm{SXLine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, a) \cdot A = \mathrm{SXLine}(A, l, a).$

(8) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$, then

$\mathrm{RLineXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k, a) \cdot A = \mathrm{RLineXS}(A, l, k, a).$

(9) $\mathrm{ILine}(M, k, k) = M.$

(10) $\mathrm{ILine}(M, l, k) = \mathrm{ILine}(M, k, l).$

(11) If $l \in \mathrm{dom}\, M$ and $k \in \mathrm{dom}\, M$, then $\mathrm{ILine}(\mathrm{ILine}(M, l, k), l, k) = M.$

(12) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$, then

$\mathrm{ILine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k)$ is invertible and

$(\mathrm{ILine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k))^{\smile} = \mathrm{ILine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k).$

(13) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$

and $k \neq l$, then $\mathrm{RLineXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k, a)$ is invertible and

$(\mathrm{RLineXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, k, a))^{\smile} = \mathrm{RLineXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K,$

$l, k, -a)$.

(14) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K)$ and $a \neq 0_K$, then

$\mathrm{SXLine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, a)$ is invertible and

$(\mathrm{SXLine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, a))^{\smile} = \mathrm{SXLine}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}^{n \times n}_K, l, a^{-1})$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, and let l, k be natural numbers. Let us assume that $l \in \mathrm{Seg\,width}\,M$ and $k \in \mathrm{Seg\,width}\,M$ and $n > 0$ and $m > 0$. The functor $\mathrm{InterchangeCol}(M, l, k)$ yields a matrix over K of dimension $n \times m$ and is defined by the conditions (Def. 4).

(Def. 4)(i) $\mathrm{len\,InterchangeCol}(M, l, k) = \mathrm{len}\,M$, and

(ii)   for all i, j such that $i \in \mathrm{dom}\,M$ and $j \in \mathrm{Seg\,width}\,M$ holds if $j = l$, then $(\mathrm{InterchangeCol}(M, l, k))_{i,j} = M_{i,k}$ and if $j = k$, then $(\mathrm{InterchangeCol}(M, l, k))_{i,j} = M_{i,l}$ and if $j \neq l$ and $j \neq k$, then $(\mathrm{InterchangeCol}(M, l, k))_{i,j} = M_{i,j}$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l be a natural number, and let a be an element of K. Let us assume that $l \in \mathrm{Seg\,width}\,M$ and $n > 0$ and $m > 0$. The functor $\mathrm{ScalarXCol}(M, l, a)$ yielding a matrix over K of dimension $n \times m$ is defined by the conditions (Def. 5).

(Def. 5)(i) $\mathrm{len\,ScalarXCol}(M, l, a) = \mathrm{len}\,M$, and

(ii)   for all i, j such that $i \in \mathrm{dom}\,M$ and $j \in \mathrm{Seg\,width}\,M$ holds if $j = l$, then $(\mathrm{ScalarXCol}(M, l, a))_{i,j} = a \cdot M_{i,l}$ and if $j \neq l$, then $(\mathrm{ScalarXCol}(M, l, a))_{i,j} = M_{i,j}$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l, k be natural numbers, and let a be an element of K. Let us assume that $l \in \operatorname{Seg} \operatorname{width} M$ and $k \in \operatorname{Seg} \operatorname{width} M$ and $n > 0$ and $m > 0$. The functor $\operatorname{RcolXScalar}(M, l, k, a)$ yielding a matrix over K of dimension $n \times m$ is defined by the conditions (Def. 6).

(Def. 6)(i) $\operatorname{len} \operatorname{RcolXScalar}(M, l, k, a) = \operatorname{len} M$, and

(ii)   for all i, j such that $i \in \operatorname{dom} M$ and $j \in \operatorname{Seg} \operatorname{width} M$ holds if $j = l$, then $(\operatorname{RcolXScalar}(M, l, k, a))_{i,j} = a \cdot M_{i,k} + M_{i,l}$ and if $j \neq l$, then $(\operatorname{RcolXScalar}(M, l, k, a))_{i,j} = M_{i,j}$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, and let l, k be natural numbers. We introduce $\operatorname{ICol}(M, l, k)$ as a synonym of $\operatorname{InterchangeCol}(M, l, k)$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l be a natural number, and let a be an element of K. We introduce $\operatorname{SXCol}(M, l, a)$ as a synonym of $\operatorname{ScalarXCol}(M, l, a)$.

Let us consider n, m, let us consider K, let M be a matrix over K of dimension $n \times m$, let l, k be natural numbers, and let a be an element of K. We introduce $\operatorname{RColXS}(M, l, k, a)$ as a synonym of $\operatorname{RcolXScalar}(M, l, k, a)$.

We now state several propositions:

(15)   If $l \in \operatorname{Seg} \operatorname{width} M$ and $k \in \operatorname{Seg} \operatorname{width} M$ and $n > 0$ and $m > 0$ and $M_1 = M^{\mathrm{T}}$, then $(\operatorname{ILine}(M_1, l, k))^{\mathrm{T}} = \operatorname{ICol}(M, l, k)$.

(16)   If $l \in \operatorname{Seg} \operatorname{width} M$ and $a \neq 0_K$ and $n > 0$ and $m > 0$ and $M_1 = M^{\mathrm{T}}$, then $(\operatorname{SXLine}(M_1, l, a))^{\mathrm{T}} = \operatorname{SXCol}(M, l, a)$.

(17)   If $l \in \operatorname{Seg} \operatorname{width} M$ and $k \in \operatorname{Seg} \operatorname{width} M$ and $n > 0$ and $m > 0$ and $M_1 = M^{\mathrm{T}}$, then $(\operatorname{RLineXS}(M_1, l, k, a))^{\mathrm{T}} = \operatorname{RColXS}(M, l, k, a)$.

(18)   If $l \in \operatorname{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $k \in \operatorname{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $n > 0$, then $A \cdot \operatorname{ICol}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, k) = \operatorname{ICol}(A, l, k)$.

(19)   If $l \in \operatorname{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $a \neq 0_K$ and $n > 0$, then $A \cdot \operatorname{SXCol}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, a) = \operatorname{SXCol}(A, l, a)$.

(20) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and

$n > 0$, then $A \cdot \mathrm{RColXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, k, a) = \mathrm{RColXS}(A, l, k, a)$.

(21) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and

$n > 0$, then $(\mathrm{ICol}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, k))^{\smile} = \mathrm{ICol}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n},$

$l, k)$.

(22) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $k \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$

and $k \neq l$ and $n > 0$, then $(\mathrm{RColXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, k, a))^{\smile} =$

$\mathrm{RColXS}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, k, -a)$.

(23) If $l \in \mathrm{dom}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n})$ and $a \neq 0_K$ and $n > 0$, then

$(\mathrm{SXCol}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, a))^{\smile} = \mathrm{SXCol}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}, l, a^{-1})$.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.
[4] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[8] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[9] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[10] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[11] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[12] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[13] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[14] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.

[15] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[18] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[19] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.

[20] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

[21] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

The Sylow Theorems

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. The goal of this article is to formalize the Sylow theorems closely following the book [4]. Accordingly, the article introduces the group operating on a set, the stabilizer, the orbits, the p-groups and the Sylow subgroups.

The papers [20], [26], [18], [9], [21], [14], [11], [27], [6], [28], [7], [3], [5], [10], [1], [23], [24], [22], [16], [13], [19], [17], [2], [25], [15], [8], and [12] provide the notation and terminology for this paper.

1. Group Operating on a Set

Let S be a non empty 1-sorted structure, let E be a set, let A be an action of the carrier of S on E, and let s be an element of S. We introduce $A \frown s$ as a synonym of $A(s)$.

Let S be a non empty 1-sorted structure, let E be a set, let A be an action of the carrier of S on E, and let s be an element of S. Then $A \frown s$ is a function from E into E.

Let S be a unital non empty groupoid, let E be a set, and let A be an action of the carrier of S on E. We say that A is left-operation if and only if:

(Def. 1) $A \frown (\mathbf{1}_S) = \mathrm{id}_E$ and for all elements s_1, s_2 of S holds $A \frown (s_1 \cdot s_2) = (A \frown s_1) \cdot (A \frown s_2)$.

Let S be a unital non empty groupoid and let E be a set. Note that there exists an action of the carrier of S on E which is left-operation.

Let S be a unital non empty groupoid and let E be a set. A left operation of S on E is a left-operation action of the carrier of S on E.

The scheme *ExLeftOperation* deals with a set $\mathcal{A}$, a group-like non empty groupoid $\mathcal{B}$, and a unary functor $\mathcal{F}$ yielding a function from $\mathcal{A}$ into $\mathcal{A}$, and states that:

There exists a left operation T of $\mathcal{B}$ on $\mathcal{A}$ such that for every element s of $\mathcal{B}$ holds $T(s) = \mathcal{F}(s)$

provided the parameters meet the following requirements:

- $\mathcal{F}(\mathbf{1}_\mathcal{B}) = \mathrm{id}_\mathcal{A}$, and
- For all elements s_1, s_2 of $\mathcal{B}$ holds $\mathcal{F}(s_1 \cdot s_2) = \mathcal{F}(s_1) \cdot \mathcal{F}(s_2)$.

Next we state the proposition

(1) Let E be a non empty set, S be a group-like non empty groupoid, s be an element of S, and L_1 be a left operation of S on E. Then $L_1 \frown s$ is one-to-one.

Let S be a non empty groupoid and let s be an element of S. We introduce $\boldsymbol{\gamma}_s$ as a synonym of s^*.

Let S be a group-like associative non empty groupoid. The functor $\boldsymbol{\Gamma}_S$ yielding a left operation of S on the carrier of S is defined as follows:

(Def. 2) For every element s of S holds $\boldsymbol{\Gamma}_S(s) = \boldsymbol{\gamma}_s$.

Let E be a set and let n be a set. The functor $[E]^n$ yielding a family of subsets of E is defined by:

(Def. 3) $[E]^n = \{X; X \text{ ranges over subsets of } E\colon \overline{\overline{X}} = n\}$.

Let E be a finite set and let n be a set. One can verify that $[E]^n$ is finite.

The following two propositions are true:

(2) For every natural number n and for every non empty set E such that $\overline{\overline{n}} \leq \overline{\overline{E}}$ holds $[E]^n$ is non empty.

(3) For every non empty finite set E and for every element k of $\mathbb{N}$ and for all sets x_1, x_2 such that $x_1 \neq x_2$ holds $\mathrm{card}\,\mathrm{Choose}(E, k, x_1, x_2) = \mathrm{card}([E]^k)$.

Let E be a non empty set, let n be a natural number, let S be a group-like non empty groupoid, let s be an element of S, and let L_1 be a left operation of S on E. Let us assume that $\overline{\overline{n}} \leq \overline{\overline{E}}$. The functor $\boldsymbol{\gamma}_{s,L_1}^n$ yields a function from $[E]^n$ into $[E]^n$ and is defined by:

(Def. 4) For every element X of $[E]^n$ holds $\boldsymbol{\gamma}_{s,L_1}^n(X) = (L_1 \frown s)^\circ X$.

Let E be a non empty set, let n be a natural number, let S be a group-like non empty groupoid, and let L_1 be a left operation of S on E. Let us assume that $\overline{\overline{n}} \leq \overline{\overline{E}}$. The functor $\boldsymbol{\Gamma}_{L_1}^n$ yields a left operation of S on $[E]^n$ and is defined by:

(Def. 5) For every element s of S holds $\boldsymbol{\Gamma}_{L_1}^n(s) = \boldsymbol{\gamma}_{s,L_1}^n$.

Let S be a non empty groupoid, let s be an element of S, and let Z be a non empty set. The functor $\boldsymbol{\gamma}_{s,Z}$ yielding a function from $[\![\text{the carrier of } S,\ Z]\!]$ into $[\![\text{the carrier of } S,\ Z]\!]$ is defined by the condition (Def. 6).

(Def. 6)   Let z_1 be an element of $[\!$ the carrier of S, Z $]\!]$. Then there exists an element z_2 of $[\!$ the carrier of S, Z $]\!]$ and there exist elements s_1, s_2 of S and there exists an element z of Z such that $z_2 = \boldsymbol{\gamma}_{s,Z}(z_1)$ and $s_2 = s \cdot s_1$ and $z_1 = \langle s_1, z \rangle$ and $z_2 = \langle s_2, z \rangle$.

Let S be a group-like associative non empty groupoid and let Z be a non empty set. The functor $\boldsymbol{\Gamma}_{S,Z}$ yields a left operation of S on $[\!$ the carrier of S, Z $]\!]$ and is defined by:

(Def. 7)   For every element s of S holds $\boldsymbol{\Gamma}_{S,Z}(s) = \boldsymbol{\gamma}_{s,Z}$.

Let G be a group, let H, P be subgroups of G, and let h be an element of H. The functor $\boldsymbol{\gamma}_{h,P}$ yields a function from the left cosets of P into the left cosets of P and is defined by the condition (Def. 8).

(Def. 8)   Let P_1 be an element of the left cosets of P. Then there exists an element P_2 of the left cosets of P and there exist subsets A_1, A_2 of G and there exists an element g of G such that $P_2 = \boldsymbol{\gamma}_{h,P}(P_1)$ and $A_2 = g \cdot A_1$ and $A_1 = P_1$ and $A_2 = P_2$ and $g = h$.

Let G be a group and let H, P be subgroups of G. The functor $\boldsymbol{\Gamma}_{H,P}$ yields a left operation of H on the left cosets of P and is defined as follows:

(Def. 9)   For every element h of H holds $\boldsymbol{\Gamma}_{H,P}(h) = \boldsymbol{\gamma}_{h,P}$.

2. Stabilizer and Orbits

Let G be a group, let E be a non empty set, let T be a left operation of G on E, and let A be a subset of E. The functor T_A yields a strict subgroup of G and is defined as follows:

(Def. 10)   The carrier of $T_A = \{g; g$ ranges over elements of G: $(T \frown g)^\circ A = A\}$.

Let G be a group, let E be a non empty set, let T be a left operation of G on E, and let x be an element of E. The functor T_x yielding a strict subgroup of G is defined by:

(Def. 11) $T_x = T_{\{x\}}$.

Let S be a unital non empty groupoid, let E be a set, let T be a left operation of S on E, and let x be an element of E. We say that x is fixed under T if and only if:

(Def. 12)   For every element s of S holds $x = (T \frown s)(x)$.

Let S be a unital non empty groupoid, let E be a set, and let T be a left operation of S on E. The functor T_0 yields a subset of E and is defined by:

(Def. 13) $T_0 = \begin{cases} \{x; x \text{ ranges over elements of } E: x \text{ is fixed under } T\}, \\ \qquad \text{if } E \text{ is non empty,} \\ \emptyset_E, \text{ otherwise.} \end{cases}$

Let S be a unital non empty groupoid, let E be a set, let T be a left operation of S on E, and let x, y be elements of E. We say that x and y are conjugated under T if and only if:

(Def. 14)   There exists an element s of S such that $y = (T \frown s)(x)$.

We now state three propositions:

(4)   Let S be a unital non empty groupoid, E be a non empty set, x be an element of E, and T be a left operation of S on E. Then x and x are conjugated under T.

(5)   Let G be a group, E be a non empty set, x, y be elements of E, and T be a left operation of G on E. Suppose x and y are conjugated under T. Then y and x are conjugated under T.

(6)   Let S be a unital non empty groupoid, E be a non empty set, x, y, z be elements of E, and T be a left operation of S on E. Suppose x and y are conjugated under T and y and z are conjugated under T. Then x and z are conjugated under T.

Let S be a unital non empty groupoid, let E be a non empty set, let T be a left operation of S on E, and let x be an element of E. The functor $T(x)$ yields a subset of E and is defined as follows:

(Def. 15) $T(x) = \{y; y$ ranges over elements of E: x and y are conjugated under $T\}$.

One can prove the following four propositions:

(7)   Let S be a unital non empty groupoid, E be a non empty set, x be an element of E, and T be a left operation of S on E. Then $T(x)$ is non empty.

(8)   Let G be a group, E be a non empty set, x, y be elements of E, and T be a left operation of G on E. Then $T(x)$ misses $T(y)$ or $T(x) = T(y)$.

(9)   Let S be a unital non empty groupoid, E be a non empty finite set, x be an element of E, and T be a left operation of S on E. If x is fixed under T, then $T(x) = \{x\}$.

(10)   Let G be a group, E be a non empty set, a be an element of E, and T be a left operation of G on E. Then $\overline{\overline{T(a)}} = |\bullet : T_a|$.

Let G be a group, let E be a non empty set, and let T be a left operation of G on E. The orbits of T yields a partition of E and is defined by:

(Def. 16)   The orbits of $T = \{X; X$ ranges over subsets of E: $\bigvee_{x:\text{element of } E} X = T(x)\}$.

3. p-GROUPS

Let p be a prime natural number and let G be a group. We say that G is a p-group if and only if:

(Def. 17)   There exists a natural number r such that $\operatorname{ord}(G) = p^r$.

Let p be a prime natural number, let G be a group, and let P be a subgroup of G. We say that P is a p-group if and only if:

(Def. 18)   There exists a finite group H such that $P = H$ and H is a p-group.

One can prove the following proposition

(11)   Let E be a non empty finite set, G be a finite group, p be a prime natural number, and T be a left operation of G on E. If G is a p-group, then $\operatorname{card} T_0 \bmod p = \operatorname{card} E \bmod p$.

4. The Sylow Theorems

Let p be a prime natural number, let G be a group, and let P be a subgroup of G. We say that P is a Sylow p-subgroup if and only if:

(Def. 19) P is a p-group and $p \nmid |\bullet : P|_{\mathbb{N}}$.

We now state three propositions:

(12)   For every finite group G and for every prime natural number p holds there exists a subgroup of G which is a Sylow p-subgroup.

(13)   Let G be a finite group and p be a prime natural number. If $p \mid \operatorname{ord}(G)$, then there exists an element g of G such that $\operatorname{ord}(g) = p$.

(14)   Let G be a finite group and p be a prime natural number. Then
  (i)   for every subgroup H of G such that H is a p-group there exists a subgroup P of G such that P is a Sylow p-subgroup and H is a subgroup of P, and
  (ii)   for all subgroups P_1, P_2 of G such that P_1 is a Sylow p-subgroup and P_2 is a Sylow p-subgroup holds P_1 and P_2 are conjugated.

Let G be a group and let p be a prime natural number. The functor $\mathsf{Syl}_p(G)$ yielding a subset of $\operatorname{SubGr} G$ is defined as follows:

(Def. 20) $\mathsf{Syl}_p(G) = \{H; H \text{ ranges over elements of } \operatorname{SubGr} G :$
$\bigvee_{P:\ \text{strict subgroup of } G} (P = H \ \wedge \ P \text{ is a Sylow } p\text{-subgroup})\}$.

Let G be a finite group and let p be a prime natural number. Note that $\mathsf{Syl}_p(G)$ is non empty and finite.

Let G be a finite group, let p be a prime natural number, let H be a subgroup of G, and let h be an element of H. The functor $\gamma_{h,p}$ yielding a function from $\mathsf{Syl}_p(G)$ into $\mathsf{Syl}_p(G)$ is defined by the condition (Def. 21).

(Def. 21)   Let P_1 be an element of $\mathsf{Syl}_p(G)$. Then there exists an element P_2 of $\mathsf{Syl}_p(G)$ and there exist strict subgroups H_1, H_2 of G and there exists an element g of G such that $P_2 = \gamma_{h,p}(P_1)$ and $P_1 = H_1$ and $P_2 = H_2$ and $h^{-1} = g$ and $H_2 = H_1{}^g$.

Let G be a finite group, let p be a prime natural number, and let H be a subgroup of G. The functor $\mathbf{\Gamma}_{H,p}$ yields a left operation of H on $\mathsf{Syl}_p(G)$ and is defined as follows:

(Def. 22)   For every element h of H holds $\mathbf{\Gamma}_{H,p}(h) = \boldsymbol{\gamma}_{h,p}$.

The following proposition is true

(15)   For every finite group G and for every prime natural number p holds $\mathrm{card}(\mathsf{Syl}_p(G)) \bmod p = 1$ and $\mathrm{card}(\mathsf{Syl}_p(G)) \mid \mathrm{ord}(G)$.

5. Appendix

The following propositions are true:

(16)   For all non empty sets X, Y holds
$$\overline{\overline{\{[: X, \{y\} :] : y \text{ ranges over elements of } Y\}}} = \overline{\overline{Y}}.$$

(17)   For all natural numbers n, m, r and for every prime natural number p such that $n = p^r \cdot m$ and $p \nmid m$ holds $\binom{n}{p^r} \bmod p \neq 0$.

(18)   For every natural number n such that $n > 0$ holds $\mathrm{ord}(\mathbb{Z}_n^+) = n$.

(19)   For every group G and for every non empty subset A of G and for every element g of G holds $\overline{\overline{A}} = \overline{\overline{A \cdot g}}$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3*. Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Artur Korniłowicz. The definition and basic properties of topological groups. *Formalized Mathematics*, 7(**2**):217–225, 1998.

[13] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[15] Karol Pąk. Cardinal numbers and finite sets. *Formalized Mathematics*, 13(**3**):399–406, 2005.

[16] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[17] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.

[18] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[20] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[21] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[22] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.

[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[24] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

[25] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[27] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[28] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.