Evidence Algorithm

By the end of 1960s Academician V. Glushkov advanced a programme on investigating automated theorem proving, which was later called the Evidence Algorithm, EA (first mentioned in "Kibernetika", 2, 1970). V. Glushkov proposed to make investigation simultaneously into formalized languages for presenting mathematical texts in the form most appropriate for a user, formalization and evolutional development of computer-made proof step, EA information environment having an influence on a current evidence of computer-made proof step, and interactive man-assistant search of proof.

- SAD system
- Explanations
- Download
- Our Team

Since then, a lot of investigations were made in all the above spheres. Russian and English versions of the formalized mathematical languages were developed. Their syntactical analyzers were designed. At present time, a translator of the English-based Formal Theory Language (ForTheL) into the first-order language is implemented.

A sequential formalism was developed for construction of an efficient technique of proof search in an initial theory (without preliminary skolemization). A special approach was offered for applying definitions and auxiliary propositions that takes into account the neighbourhood of the proposition to be proved. Basing on this formalism, a first-order prover was implemented.

As a result, the System for Automated Deduction (SAD) appeared.

Theses of the EA programme promise to be helpful in attacking such problems as distributed automated theorem proving, verification of mathematical texts, remote training in mathematical disciplines, and construction of databases for mathematical theories.

---

to Russian Last modified: 8 Oct 2007

THE SYSTEM FOR AUTOMATED DEDUCTION

Evidence Algorithm

SAD system | Explanations | Download | Our Team
Inference Search | Theorem Proving | Text Verification | TPTP Problems

[Help] [Examples]

```
#
# Integers
#

[integer/-s]

Signature Integers. An integer is a notion.

Let a,b,c,d,i,j,k,l,m,n stand for integers.

Signature IntZero.  0 is an integer.
Signature IntOne.   1 is an integer.
Signature IntNeg.   -a is an integer.
Signature IntPlus.  a + b is an integer.
Signature IntMult.  a * b is an integer.

Let a - b stand for a + (-b).

Axiom ZeroOne.      0 != 1.
```

Parse | Verify with Moses | Verify with | SPASS 3.7 | Clear

Time limit (1–600 sec) 3 | 3 Verbosity level (0–6)

to Russian

Last modified: 3 Aug 2008

```
#\newtheorem{signature}{Signature}
#\newtheorem{axiom}{Axiom}
#\newtheorem{signaturep}{Signature}
#\newtheorem{axiomp}{Axiom}
#\newtheorem{definitionp}{Definition}
#\newtheorem{theoremp}{Theorem}
#\newtheorem{lemmap}{Lemma}

#\newcommand{\power}{{\cal P}}
#\newcommand{\preimg}[2]{{#1}^{-1}[#2]}
#\newcommand{\Seq}[2]{{#1,\dots,#2}}
#\newcommand{\Set}[3]{{#1_{#2},\dots,#1_{#3}}}
#\newcommand{\Product}[3]{\prod_{i=#2}^{#3}{#1}_i}
#\newcommand{\subfunc}[2]{{#1}_{#2}}
#\newcommand{\CC}{{\Bbb C}}
#\newcommand{\RR}{{\Bbb R}}
#\newcommand{\QQ}{{\Bbb Q}}
#\newcommand{\ZZ}{{\Bbb Z}}
#\newcommand{\NN}{{\Bbb N}}
#\newcommand{\NNplus}{{\Bbb N}^+}

#\title{There are infinitely many primes}
#\maketitle
#
# Version 18 March 2012
#
#\section{I. Foundations}

#\subsection{1. Sets}

[set/-s] [element/-s] [belong/-s] [subset/-s]

# Signature SetSort.  A set is a notion.
Let A,X,Y,Z denote sets.


# Signature ElmSort.
# An element is a notion.
# Let x,y,z denote elements.


# Signature EOfElem.
# An element of X is an element.
Let x belongs to X stand for x is an element of X.
Let x is in X stand for x belongs to X.
Let x \in X stand for x is in X.


Definition DefEmp.
\emptyset is a set that has no elements.
Let X is empty stand for X = \emptyset.
Let X is nonempty stand for X != \emptyset.


Definition DefSub.
A subset of Y is a set X such that
every element of X belongs to Y.
Let X \subseteq Y stand for X is a subset of Y.


Lemma SubRefl.
X \subseteq X.


Lemma SubTrans.
X \subseteq Y \subseteq Z  =>  X \subseteq Z.
```

```
Axiom SubASymm.
X \subseteq Y \subseteq X  =>  X = Y.



#\subsection{2. Functions}

[function/-s]

# Signature FunSort.
# A function is a notion.
Let f,g,p denote functions.


# Signature DomSet.
# dom f is a set.
# Let the domain of f stand for Dom(f).


# Signature ImgElm.
# Let x \in dom f. f(x) is an element.
Let \subfunc{f}{x} stand for f[x].


Definition DefSImg.
Let X \subseteq Dom(f). f[[X]] = { f[x] | x \in X }.
Let Ran(f) stand for f[[Dom(f)]].
Let the range of f stand for Ran(f).

Let a function from X stand for a function f
such that Dom(f) = X.
Let a function from X to Y stand
for a function f such that Dom(f) = X
and Ran(f) \subseteq Y.

Let f : X stand for f is a function from X.
Let f : X -> Y stand for f is a function from X to Y.


Lemma ImgRng.
Let x \in Dom(f). f[x] belongs to Ran(f).


Definition DefRst.
Let X \subseteq Dom(f).
f \upharpoonright X is a function g from X
such that for every x \in X g[x] = f[x].

#\subsection{3. Numbers}

[number/-s]

Signature NatSort.
A number is a notion.
Let i,j,k,l,m,n,q,r denote numbers.


Definition Nat.
\NN is the set of numbers.


Signature SortsC.
0 is a number.
Let x is nonzero stand for x != 0.
```

```
Signature SortsC.
1 is a nonzero number.


Signature SortsB.
m + n is a number.


Signature SortsB.
m \cdot n is a number.


Axiom AddAsso. (m + n) + l = m + (n + l).
Axiom AddZero.  m + 0 = m = 0 + m.
Axiom AddComm.   m + n = n + m.

Axiom MulAsso.
(m \cdot n) \cdot l = m \cdot (n \cdot l).

Axiom MulUnit.  m \cdot 1 = m = 1 \cdot m.
Axiom MulZero.  m \cdot 0 = 0 = 0 \cdot m.
Axiom MulComm.  m \cdot n = n \cdot m.

Axiom AMDistr.
m \cdot (n + l) = (m \cdot n) + (m \cdot l) and
(n + l) \cdot m = (n \cdot m) + (l \cdot m).

Axiom AddCanc.
If l + m = l + n or m + l = n + l then m = n.

Axiom MulCanc.
Assume that l is nonzero. If
l \cdot m = l \cdot n or m \cdot l = n \cdot l
then m = n.

Axiom ZeroAdd.
If m + n = 0 then m = 0 and n = 0.

Lemma ZeroMul.
If m \cdot n = 0 then m = 0 or n = 0.


Definition DefLE.
m \leq n iff there exists l such that m + l = n.


Definition DefDiff.  Assume that m \leq n.
n - m is a number l such that m + l = n.


Lemma LERefl. m \leq m.
Lemma LETran. m \leq n \leq l  =>  m \leq l.

Lemma LEAsym. m \leq n \leq m  =>  m = n.


Let m < n stand for m != n and m \leq n.

Axiom LETotal. m \leq n or n < m.

Lemma MonAdd. Assume that l < n.
Then m + l < m + n and l + m < n + m.
```

```
Lemma MonMul. Assume that m is nonzero and l < n.
Then m \cdot l < m \cdot n and l \cdot m < n \cdot m.


Axiom LENTr.
n = 0 or n = 1 or 1 < n.


Lemma MonMul2. m != 0 => n \leq n \cdot m.

Proof.
Let m != 0. Then 1 \leq m.
qed.

Signature InbuiltForthelInductionRelation. m -<- n is an atom.


Axiom EmbeddingLessIntoInductionRelation. m < n => m -<- n.

#\subsection{4. Finite Sets and Sequences}

Definition.
\Seq{m}{n} = { i \in \NN | m \leq i \leq n }.


Definition.
Let f be a function such that
\Seq{m}{n} \subseteq Dom(f).
\Set{f}{m}{n} = { f[i] | i \in \NN /\ m \leq i \leq n }.


Definition. f lists X in n steps iff
Dom(f) = \Seq{1}{n} and X = \Set{f}{1}{n}.


Definition. X is finite iff there is a function
f and a number n such that f lists X in n steps.


Definition. X is infinite iff X is not finite.

#\section{II. Prime Numbers}

#\subsection{1. Divisibility}

[divide/-s] [divisor/-s]

Definition DefDiv.
m divides n iff for some l n = m \cdot l.
Let m | n denote m divides n.
Let a divisor of n denote a number that divides n.


Definition DefQuot.
Assume that m is nonzero and m | n.
\frac{n}{m} is a number l such that n = m \cdot l.


Lemma DivTrans. l | m | n => l | n.


Lemma DivSum.
Let l | m and l | n. Then l | m + n.
Indeed if l is nonzero then
m + n = l \cdot (\frac{m}{l} + \frac{n}{l}).
```

```
Lemma DivMin.
Let l | m and l | m + n. Then l | n.

Proof.
Assume that l,n are nonzero.
Take i such that m = l \cdot i.
Take j such that m + n = l \cdot j.

Let us show that i \leq j.
Assume the contrary. Then j < i.
m+n = l \cdot j < l \cdot i = m.
m \leq m+n.
m = m+n. n=0.
Contradiction. end.

Take k = j - i.
We have (l \cdot i) + (l \cdot k) = (l \cdot i) + n.
Hence n = l \cdot k.
qed.

Lemma DivLE.
Let m | n != 0. Then m \leq n.


Lemma DivAsso.
Let l be nonzero and divide m.
Then n \cdot \frac{m}{l} = \frac{n \cdot m}{l}.
Proof.
(l \cdot n) \cdot \frac{m}{l} = l \cdot \frac{n \cdot m}{l}.
qed.

Definition.
\NNplus = {n \in \NN | n != 0 }.

# Lemma. Every element of \NNplus is a number.


Signature.
Let f : \Seq{m}{n} -> \NNplus.
# \Product{f}{m}{n} is an element of \NNplus.
# \Product{f}{m}{n} is an element of \NN. ##
\Product{f}{m}{n} is a number.

Axiom. Let f : \Seq{m}{n} -> \NNplus.
\Product{f}{m}{n} != 0.

Axiom MultProd.
Let f : \Seq{m}{n} -> \NNplus.
Let m \leq j \leq n.
\subfunc{f}{j} divides \Product{f}{m}{n}.

#\subsection{2. Primes}

[prime/-s] [compound/-s] [primenumber/-s]

Let m is trivial stand for m = 0 or m = 1.
Let m is nontrivial stand for m != 0 and m != 1.

Definition DefPrime.
q is prime iff q is nontrivial and
for every divisor m of q m = 1 or m = q.


Let m is compound stand for m is not prime.
```

```
Lemma PrimDiv.
Every nontrivial k has a prime divisor.

Proof by induction on k.
Let k be nontrivial.
Case k is prime. Obvious.
Case k is compound.
Take a divisor m of k such that m != 1 and m != k.
#m != 0.
m is nontrivial and m -<- k.
Take a prime divisor n of m.
n is a prime divisor of k.
end.
qed.

Theorem.
Let P be the set of prime numbers. Then P is infinite.

Proof.
Let A be a finite set of prime numbers.
Take a function p and a number r such that
p lists A in r steps.
Ran(p) \subseteq \NNplus.
\Product{p}{1}{r} != 0.
Take n=\Product{p}{1}{r}+1.
n is nontrivial.
Take a prime divisor q of n (by PrimDiv).

Let us show that q is not an element of A.
Assume the contrary.
Take i such that (1 \leq i \leq r and q=\subfunc{p}{i}).
\subfunc{p}{i} divides \Product{p}{1}{r} (by MultProd).
Then q divides 1 (by DivMin).
Contradiction. qed.

Hence A is not the set of prime numbers.
qed.
```

Let k be nontrivial. Case k is prime. Obvious. Case k is compound. Take a divisor m of k such that $m \neq 1$ and $m \neq k$. m is nontrivial and $m - < -k$. Take a prime divisor n of m. n is a prime divisor of k. end.
qed.

Theorem 1 *Let P be the set of prime numbers. Then P is infinite.*

Proof Let A be a finite set of prime numbers. Take a function p and a number r such that p lists A in r steps. $Ran(p) \subseteq \mathbb{N}^+$. $\prod_{i=1}^{r} p_i \neq 0$. Take $n = \prod_{i=1}^{r} p_i + 1$. n is nontrivial. Take a prime divisor q of n (by PrimDiv).
Let us show that q is not an element of A. Assume the contrary. Take i such that $(1 \leq i \leq r and q = p_i)$. p_i divides $\prod_{i=1}^{r} p_i$ (by MultProd). Then q divides 1 (by DivMin). Contradiction. qed.
Hence A is not the set of prime numbers. $\square$

The Maximum Principle for Holomorphic Functions

1 Preliminaries

[number/-s][ontored on][checkontored on]
Let the *domain* of f stand for $\mathrm{Dom}(f)$. Let z is *in* M stand for z is an element of M. Let M *contains* z stand for z is in M. Let $z \in M$ stand for z is in M.
Let f denote a function. Let M denote a set.

Definition 1. A *subset* of M is a set N such that every element of N is an element of M.

Definition 2. Assume M is a subset of the domain of f. $f[\![M]\!] = \{f[x] \mid x \in M\}$.

Signature 1. A *complex number* is a notion. Let z, w denote complex numbers.

Axiom 1. Every element of $\mathrm{Dom}(f)$ is a complex number and for every element z of $\mathrm{Dom}(f)$ $f[z]$ is a complex number.

Axiom 2. Every element of M is a complex number.

Signature 2. A *real number* is a notion. Let x, y denote real numbers.

Signature 3. $|z|$ is a real number.

Signature 4. x is *positive* is an atom. Let ϵ, δ denote positive real numbers.

Signature 5. $x < y$ is an atom. Let $x \leq y$ stand for $x = y$ or $x < y$.

Axiom 3. $x < y \Rightarrow \neg y < x$.

Signature 6. f is *holomorphic* is an atom.

Signature 7. $B_\epsilon(z)$ is a set that contains z.

Axiom 4. $|z| < |w|$ for some element w of $B_\epsilon(z)$.

Definition 3. M is *open* iff for every element z of M there exists ϵ such that $B_\epsilon(z)$ is a subset of M.

Axiom 5. $B_\epsilon(z)$ is open.

Definition 4. A *local maximal point* of f is an element z of the domain of f such that there exists ϵ such that $B_\epsilon(z)$ is a subset of the domain of f and $|f[w]| \leq |f[z]|$ for every element w of $B_\epsilon(z)$.

Definition 5. Let U be a subset of the domain of f. f is *constant on* U iff there exists z such that $f[w] = z$ for every element w of U. Let f is *constant* stand for f is constant on the domain of f.

Axiom 6. Assume f is holomorphic and $B_\epsilon(z)$ is a subset of the domain of f. If f is not constant on $B_\epsilon(z)$ then $f[\![B_\epsilon(z)]\!]$ is open.

Signature 8. A *region* is an open set.

In: A. Editor, B. Coeditor (eds.): Proceedings of the XYZ Workshop, Location, Country, DD-MMM-YYYY, published at http://ceur-ws.org

Axiom 7 (IdentityTheorem)**.** Assume f is holomorphic and the domain of f is a region. Assume that $B_\epsilon(z)$ is a subset of the domain of f. If f is constant on $B_\epsilon(z)$ then f is constant.

Theorem 1 (MaximumPrinciple)**.** *Assume f is holomorphic and the domain of f is a region. If f has a local maximal point then f is constant.*

Proof. Let z be a local maximal point of f. Take ϵ such that $B_\epsilon(z)$ is a subset of Dom(f) and $|f[w]| \leq |f[z]|$ for every element w of $B_\epsilon(z)$. Let us show that f is constant on $B_\epsilon(z)$. *Proof.* Assume the contrary. Then $f[\![B_\epsilon(z)]\!]$ is open. We can take δ such that $B_\delta(f[z])$ is a subset of $f[\![B_\epsilon(z)]\!]$. Therefore there exists an element w of $B_\epsilon(z)$ such that $|f[z]| < |f[w]|$. Contradiction. end. Hence f is constant. □

Definition 5. A *scalar function* on V is a function f such that
$\mathrm{Dom}(f) = |V|$ and
(for every element x of $|V|$ $f[x]$ is a scalar) and
(for every element x, y of $|V|$ $f[x +_V y] = f[x] + f[y]$) and
(for every element x of $|V|$ and every scalar a $f[a *_V x] = a * f[x]$).

2 Dual Spaces

Signature 9. $SF(V)$ is the set of scalar functions on V.

Definition 6. The *dual space* of V is a vector space W such that ($|W| = SF(V)$) and (for all scalar functions f, g on V and every element x of $|V|$ $(f +_W g)[x] = f[x] + g[x]$) and (for every scalar function f on V, every scalar a and every element x of $|V|$ $(a *_W f)[x] = a * f[x]$). Let V^* stand for the dual space of V.

Axiom 2 (Separation)**.** Let x, y be elements of $|V|$. Assume $x \neq y$. There exists a scalar function g on V such that $g[x] \neq g[y]$.

Definition 7. The *bidual space* of V is the dual space of the dual space of V. Let V^{**} stand for the bidual space of V.

3 The Embedding

Theorem 1. *There exists an injective function that is linear from V to V^{**}.*

Proof. Define
$$\Phi = \lambda v \in |V|.\lambda g \in |V^*|.g[v].$$
Let us show that Φ is linear from V to V^{**}.
(Claim 1) Φ is from $|V|$ to $|V^{**}|$.
Proof. $\mathrm{Dom}(\Phi) = |V|$. Let x be an element of $|V|$.
(Claim 1.1) $\Phi[x]$ is a scalar function on V^*.
Proof. $\mathrm{Dom}(\Phi[x]) = |V^*|$ and for every element y of $|V^*|$ $\Phi[x][y]$ is a scalar. For all elements h, g of $|V^*|$
$$\Phi[x][h +_{V^*} g] = (h +_{V^*} g)[x] = h[x] + g[x] = \Phi[x][h] + \Phi[x][g].$$
For every element g of $|V^*|$ and every scalar a
$$\Phi[x][a *_{V^*} g] = (a *_{V^*} g)[x] = a * g[x] = a * \Phi[x][g].$$
end (Claim 1.1).
end (Claim 1).
(Claim 2) For all elements x, y of $|V|$
$$\Phi[x +_V y] = \Phi[x] +_{V^{**}} \Phi[y].$$

Signature 4. The *cardinality* of M is a cardinal. Let $\operatorname{card}(M)$ stand for the cardinality of M.

Axiom 4. $\operatorname{card}(M) \leq \operatorname{card}(N)$ iff there exists a function f such that $\operatorname{Dom}(f) = N$ and $f[\![N]\!] = M$.

Axiom 5 (Transitivity)**.** Let v be an element of κ. Assume u is an element of v. u is an element of κ.

Axiom 6. $\operatorname{card}(M \times M) = \operatorname{card}(M)$.

Axiom 7. $\operatorname{card}(\kappa) = \kappa$.

Axiom 8. Let N be a subset of M. $\operatorname{card}(N) \leq \operatorname{card}(M)$.

Definition 5. κ is *regular* iff $\operatorname{card}(M) = \kappa$ for every cofinal subset M of κ.

Signature 5. κ^+ is a cardinal.

Axiom 9. $\alpha < \beta$ or $\beta < \alpha$ or $\beta = \alpha$.

Axiom 10. $\kappa < \kappa^+$.

Axiom 11. $\operatorname{card}(i) \leq \kappa$ for every element i of κ^+.

Axiom 12. For no cardinals κ, μ we have $\kappa < \mu$ and $\mu < \kappa$.

Axiom 13. There is no cardinal μ such that $\kappa < \mu < \kappa^+$.

3 Regularity

Theorem 1. κ^+ *is regular.*

Proof. Assume the contrary. Take a cofinal subset x of κ^+ such that $\operatorname{card}(x) \neq \kappa^+$. Then $\operatorname{card}(x) \leq \kappa$. Take a function f that is surjective from κ onto x. Define

$$g[i] = \text{Choose a function } h \text{ that is surjective from } \kappa \text{ onto } i \text{ in } h$$

for $i \in \kappa^+$. Define

$$h[(\xi,\zeta)] = g[f[\xi]][\zeta]$$

for $(\xi,\zeta) \in \kappa \times \kappa$. Let us show that h is surjective from $\kappa \times \kappa$ onto κ^+.
$\operatorname{Dom}(h) = \kappa \times \kappa$. Every element of κ^+ is an element of $h[\![\kappa \times \kappa]\!]$.
Proof. Let α be an element of κ^+. Take an element ξ of κ such that $\alpha < f[\xi]$. Take an element ζ of κ such that $g[f[\xi]][\zeta] = \alpha$. Then $\alpha = h[(\xi,\zeta)]$. Therefore the thesis. Indeed (ξ,ζ) is an element of $\kappa \times \kappa$. end.
Every element of $h[\![\kappa \times \kappa]\!]$ is an element of κ^+.
Proof. Let α be an element of $h[\![\kappa \times \kappa]\!]$. We can take elements ξ, ζ of κ such that $\alpha = h[(\xi,\zeta)]$. Therefore the thesis (by Transitivity). end. end.
Therefore $\kappa^+ \leq \kappa$. Contradiction. □

The next two theorems correspond to Theorems 1.20(a) and (b) of Rudin. We start with the original introductory text of Rudin and then display the two texts in parallel to illustrate the closeness of the formalization to the original.

The next theorem could be extracted from this construction [of the real numbers] with very little extra effort. However, we prefer to derive it from Theorem 1.19 since this provides a good illustration of what one can do with the least-upper-bound property.

Theorem 5 (120a) *If $x \in \mathbb{R}$ and $y \in \mathbb{R}$ and $x > 0$ then there is a positive integer n such that*

$$n \cdot x > y.$$

Proof Define $X = \{n \cdot x \mid n \text{ is a positive integer}\}$. Assume the contrary. Then y is an upper bound of X. Take a least upper bound α of X. $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of X. Take an element z of X such that not $z \leq \alpha - x$. Take a positive integer m such that $z = m \cdot x$. Then $\alpha - x < m \cdot x$ (by 15b).

$\alpha = (\alpha - x) + x < (m \cdot x) + x = (m + 1) \cdot x$.

$(m + 1) \cdot x$ is an element of X. Contradiction. Indeed α is an upper bound of X. □

Theorem 6 *(a) If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x > 0$, then there is a positive integer n such that*

$$nx > y.$$

Proof Let A be the set of all nx, where n runs through the positive integers. If (a) were false, then y would be an upper bound of A. But then A has a *least* upper bound in $\mathbb{R}$. Put $\alpha = \sup A$. Since $x > 0$, $\alpha - x < \alpha$, and $\alpha - x$ is not an upper bound of A. Hence $\alpha - x < mx$ for some positive integer m. But then $\alpha < (m + 1)x \in A$, which is impossible, since α is an upper bound of A. □

Theorem 7 (120b) *If $x \in \mathbb{R}$ and $y \in \mathbb{R}$ and $x < y$ then there exists a rational number p such that $x < p < y$.*

Proof Assume $x < y$. We have $y - x > 0$. Take a positive integer n such that $n \cdot (y - x) > 1$ (by 120a). Take an integer m such that $m - 1 \leq n \cdot x < m$. Then

$$n \cdot x < m = (m - 1) + 1$$

$$\leq (n \cdot x) + 1 < (n \cdot x) + (n \cdot (y - x))$$

$$= n \cdot (x + (y - x)) = n \cdot y.$$

$m \leq (n \cdot x) + 1 < n \cdot y$. $\frac{m}{n} < \frac{n \cdot y}{n}$. Indeed $m < n \cdot y$ and $1/n > 0$. Then

$$x = \frac{n \cdot x}{n} < \frac{m}{n} < \frac{n \cdot y}{n} = y.$$

Let $p = \frac{m}{n}$. Then $p \in \mathbb{Q}$ and $x < p < y$. □

Theorem 8 *If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x < y$, then there exists a $p \in \mathbb{Q}$ such that $x < p < y$.*

Proof Since $x < y$, we have $y - x > 0$, and (a) furnishes a positive integer n such that

$$m(y - x) > 1.$$

Apply (a) again, to obtain positive integers m_1 and m_2 such that $m_1 > nx$, $m_2 > -nx$. Then

$$-m_2 < nx < m_1.$$

Hence there is an integer m (with $-m_2 \leq m \leq m_1$) such that

$$m - 1 \leq nx < m.$$

If we combine these inequalities, we obtain

$$nx < m \leq 1 + nx < ny.$$

Since $n > 0$, it follows that

$$x < \frac{m}{n} < y.$$

This proves (b), with $p = m/n$. □

3 Remarks

3.1 Structures

Rudin introduces ordered sets and fields axiomatically and then postulates the ordered field of reals. Indeed the reals are constructed from the rationals numbers in an Appendix to chapter 1.

Since ForTheL does not provide general structures and mechanisms to express that a structure satisfies some abstract axioms, I have instead postulated the structure $\mathbb{R}$ of the real numbers right away. The axioms of ordered sets and fields are then only stated for this particular structure.

Instead of building up number systems "from below" we define the sets of rational, integer and positive integer numbers as subsets of $\mathbb{R}$. This has the advantage that we can use the real addition and multiplication also for those

KELLEY

GENERAL TOPOLOGY

VAN
NOSTRAND

JOHN L. KELLEY

GENERAL TOPOLOGY

UNIVERSITY SERIES IN HIGHER MATHEMATICS

Appendix

ELEMENTARY SET THEORY

This appendix is devoted to elementary set theory. The ordinal and cardinal numbers are constructed and the most commonly used theorems are proved. The non-negative integers are defined and Peano's postulates are proved as theorems.

A working knowledge of elementary logic is assumed, but acquaintance with formal logic is not essential. However, an understanding of the nature of a mathematical system (in the technical sense) helps to clarify and motivate some of the discussion. Tarski's excellent exposition [1] describes such systems very lucidly and is particularly recommended for general background.

This presentation of set theory is arranged so that it may be translated without difficulty into a completely formal language.* In order to facilitate either formal or informal treatment the introductory material is split into two sections, the second of which is essentially a precise restatement of part of the first. It may be omitted without loss of continuity.

The system of axioms adopted is a variant of systems of Skolem and of A. P. Morse and owes much to the Hilbert-Bernays-von Neumann system as formulated by Gödel. The formulation used here is designed to give quickly and naturally a foundation for mathematics which is free from the more obvious paradoxes.

* That is, it is possible to write the theorems in terms of logical constants, logical variables, and the constants of the system, and the proofs may be derived from the axioms by means of rules of inference. Of course, a foundation in formal logic is necessary for this sort of development. I have used (essentially) Quine's meta-axioms for logic [1] in making this kind of presentation for a course.

ORDERED PAIRS: RELATIONS

This section is devoted to the properties of ordered pairs and relations. The crucial property for ordered pairs is theorem 55: if x and y are sets, then $(x,y) = (u,v)$ iff $x = u$ and $y = v$.

48 DEFINITION $(x,y) = \{\{x\}\{xy\}\}$.

The class (x,y) is an *ordered pair*.

49 THEOREM *(x,y) is a set if and only if x is a set and y is a set; if (x,y) is not a set, then $(x,y) = \mathcal{U}$.*

50 THEOREM *If x and y are sets, then $\bigcup(x,y) = \{xy\}$, $\bigcap(x,y) = \{x\}$, $\bigcup\bigcap(x,y) = x$, $\bigcap\bigcap(x,y) = x$, $\bigcup\bigcup(x,y) = x \cup y$ and $\bigcap\bigcup(x,y) = x \cap y$.*

If either x or y is not a set, then $\bigcup\bigcap(x,y) = 0$, $\bigcap\bigcap(x,y) = \mathcal{U}$, $\bigcup\bigcup(x,y) = \mathcal{U}$, and $\bigcap\bigcup(x,y) = 0$.

51 DEFINITION 1^{st} coord $z = \bigcap\bigcap z$.

52 DEFINITION 2^{nd} coord $z = (\bigcap\bigcup z) \cup ((\bigcup\bigcup z) \sim \bigcup\bigcap z)$.

These definitions will be used, with one exception, only in the case where z is an ordered pair. The *first coordinate* of z is 1^{st} coord z and the *second coordinate* of z is 2^{nd} coord z.

53 THEOREM 2^{nd} coord $\mathcal{U} = \mathcal{U}$.

54 THEOREM *If x and y are sets* 1^{st} coord $(x,y) = x$ *and* 2^{nd} coord $(x,y) = y$. *If either of x and y is not a set, then* 1^{st} coord $(x,y) = \mathcal{U}$ *and* 2^{nd} coord $(x,y) = \mathcal{U}$.

PROOF If x and y are sets, then the equality for 1^{st} *coord* is immediate from 50 and 51. The equality for 2^{nd} *coord* reduces to showing that $y = (x \cap y) \cup ((x \cup y) \sim x)$, by 50 and 52. It is straightforward to see that $(x \cup y) \sim x = y \sim x$ and by the distributive law $(y \cap x) \cup (y \cap \sim x)$ is $y \cap (x \cup \sim x) = y \cap \mathcal{U} = y$. If either x or y is not a set, then, using 50 it is easy to compute 1^{st} *coord* (x,y) and 2^{nd} *coord* (x,y). ∎

55 THEOREM *If x and y are sets and $(x,y) = (u,v)$, then $x = u$ and $y = v$.*

ELEMENTARY SET THEORY

An SAD3 Formalisation of the Appendix of "General Topology" by John L. Kelley

October 26, 2018

0.1 The Classification Axiom Scheme

Let $a, b, c, d, e, r, s, t, x, y, z$ stand for *classes*.
Let $a \in x$ stand for a is an *element* of x.

Axiom (I). *For each x for each y $x = y$ iff for each z $z \in x$ iff $z \in y$.*

[set/-s]

Definition (1). *A* set *is a class x such that for some y $x \in y$.*

0.2 Elementary Algebra of Classes

Definition (2). $x \cup y = \{set\ u \mid u \in x \ or\ u \in y\}$.

Definition (3). $x \cap y = \{set\ u \mid u \in x \ and\ u \in y\}$.

Let the *union* of x and y stand for $x \cup y$. Let the *intersection* of x and y stand for $x \cap y$.

Theorem (4a). *$z \in x \cup y$ iff $z \in x$ or $z \in y$.*

Theorem (4b). *$z \in x \cap y$ iff $z \in x$ and $z \in y$.*

Theorem (5a). $x \cup x = x$.

Theorem (5b). $x \cap x = x$.

Theorem (6a). $x \cup y = y \cup x$.

Theorem (6b). $x \cap y = y \cap x$.

Theorem (7a). $(x \cup y) \cup z = x \cup (y \cup z)$.

Theorem (7b)**.** $(x \cap y) \cap z = x \cap (y \cap z)$.

Theorem (8a)**.** $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$.

Theorem (8b)**.** $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$.

Let $a \notin b$ stand for a is not an element of b.

Definition (10)**.** $\sim x = \{set\ u \mid u \notin x\}$. *Let the* complement *of* x *stand for* $\sim x$.

Theorem (11)**.** $\sim (\sim x) = x$.

Theorem (12a)**.** $\sim (x \cup y) = (\sim x) \cap (\sim y)$.

Theorem (12b)**.** $\sim (x \cap y) = (\sim x) \cup (\sim y)$.

Definition (13)**.** $x \sim y = x \cap (\sim y)$.

Theorem (14)**.** $x \cap (y \sim z) = (x \cap y) \sim z$.

Definition (15)**.** $0 = \{set\ u \mid u \neq u\}$. *Let the* void class *stand for* 0. *Let* zero *stand for* 0.

Theorem (16)**.** $x \notin 0$.

Theorem (17a)**.** $0 \cup x = x$.

Theorem (17b)**.** $0 \cap x = 0$.

Definition (18)**.** $\mathcal{U} = \{set\ u \mid u = u\}$. *Let the* universe *stand for* $\mathcal{U}$.

Theorem (19)**.** $x \in \mathcal{U}$ *iff* x *is a set.*

Theorem (20a)**.** $x \cup \mathcal{U} = \mathcal{U}$.

Theorem (20b)**.** $x \cap \mathcal{U} = x$.

Theorem (21a)**.** $\sim 0 = \mathcal{U}$.

Theorem (21b)**.** $\sim \mathcal{U} = 0$.

Definition (22)**.** $\bigcap x = \{setu \mid$ *for each* y *if* $y \in x$ *then* $u \in y\}$. *Let the* intersection *of* x *stand for* $\bigcap x$.

Definition (23)**.** $\bigcup x = \{setu \mid$ *for some* $y(y \in x$ *and* $u \in y)\}$. *Let the* union *of* x *stand for* $\bigcup x$.

Theorem (24a)**.** $\bigcap 0 = \mathcal{U}$.

Theorem (24b)**.** $\bigcup 0 = 0$.

Definition (25)**.** *A* subclass *of* y *is a class* x *such that each element of* x *is an element of* y. *Let* $x \subset y$ *stand for* x *is a subclass of* y. *Let* x *is* contained *in* y *stand for* $x \subset y$.

Proposition. $0 \subset 0$ *and* $0 \notin 0$.

Theorem (26a). $0 \subset x$.

Theorem (26b). $x \subset \mathcal{U}$.

Theorem (27). $x = y$ *iff* $x \subset y$ *and* $y \subset x$.

Theorem (28). *If* $x \subset y$ *and* $y \subset z$ *then* $x \subset z$.

Theorem (29). $x \subset y$ *iff* $x \cup y = y$.

Theorem (30). $x \subset y$ *iff* $x \cap y = x$.

Theorem (31a). *If* $x \subset y$ *then* $\bigcup x \subset \bigcup y$.

Theorem (31a). *If* $x \subset y$ *then* $\bigcap y \subset \bigcap x$.

Theorem (32a). *If* $x \in y$ *then* $x \subset \bigcup y$.

Theorem (32b). *If* $x \in y$ *then* $\bigcap y \subset x$.

0.3 Existence of Sets

Axiom (III). *If x is a set then there is a set y such that for each z if $z \subset x$ then $z \in y$.*

Theorem (33). *If x is a set and $z \subset x$ then z is a set.*

Theorem (34a). $0 = \bigcap \mathcal{U}$.

Theorem (34b). $\mathcal{U} = \bigcup \mathcal{U}$.

Theorem (35). *If* $x \neq 0$ *then* $\bigcap x$ *is a set.*

Definition (36). $2^x = \{\textit{set } y \mid y \subset x\}$.

Theorem (37). $\mathcal{U} = 2^{\mathcal{U}}$.

Theorem (38a). *If x is a set then 2^x is a set.*

Proof. Let x be a set. Take a set y such that for each z if $z \subset x$ then $z \in y$ (by III). Then $2^x \subset y$. $\square$

Theorem (38b). *If x is a set then $y \subset x$ iff $y \in 2^x$.*

Definition. $\mathrm{R} = \{\textit{set } x \mid x \notin x\}$.

Lemma. R *is not a set.*

Theorem (39). $\mathcal{U}$ *is not a set.*

Definition (40). $\{x\} = \{set\ z \mid\ \ if\ x \in \mathcal{U}\ then\ z = x\}$. *Let the* singleton *of x stand for $\{x\}$.*

Theorem (41). *If x is a set then for each y $y \in \{x\}$ iff $y = x$.*

Theorem (42). *If x is a set then $\{x\}$ is a set.*

Proof. Let x be a set. Then $\{x\} \subset 2^x$. 2^x is a class. □

Theorem (43). *$\{x\} = \mathcal{U}$ iff x is not a set.*

Theorem (44a). *If x is a set then $\bigcap\{x\} = x$.*

Theorem (44b). *If x is a set then $\bigcup\{x\} = x$.*

Theorem (44c). *If x is not a set then $\bigcap\{x\} = 0$.*

Theorem (44d). *If x is not a set then $\bigcup\{x\} = \mathcal{U}$.*

Axiom (IV). *If x is a set and y is a set then $x \cup y$ is a set.*

Definition (45). $\{x, y\} = \{x\} \cup \{y\}$. *Let the* unordered pair *of x and y stand for $\{x, y\}$.*

Theorem (46a). *If x is a set and y is a set then $\{x, y\}$ is a set.*

Theorem (46b). *If x is a set and y is a set then $z \in \{x, y\}$ iff $z = x$ or $z = y$.*

Theorem (46c). *$\{x, y\} = \mathcal{U}$ iff x is not a set or y is not a set.*

Theorem (47a). *If x, y are sets then $\bigcap\{x, y\} = x \cap y$.*

Theorem (47b). *If x, y are sets then $\bigcup\{x, y\} = x \cup y$.*

Proof. Let x, y be sets. $\bigcup\{x, y\} \subset x \cup y$. $x \cup y \subset \bigcup\{x, y\}$. □

Theorem (47c). *If x is not a set or y is not a set then $\bigcap\{x, y\} = 0$.*

Theorem (47d). *If x is not a set or y is not a set then $\bigcup\{x, y\} = \mathcal{U}$.*

0.4 Ordered Pairs: Relations

Definition (48). $(x, y) = \{\{x\}, \{x, y\}\}$. *Let the* ordered pair *of x and y stand for (x, y).*

Theorem (49a). *(x, y) is a set iff x is a set and y is a set.*

Theorem (49b). *If (x, y) is not a set then $(x, y) = \mathcal{U}$.*

Theorem (50). *If x and y are sets then $\bigcup(x, y) = \{x, y\}$ and $\bigcap(x, y) = \{x\}$ and $\bigcup\bigcap(x, y) = x$ and $\bigcap\bigcap(x, y) = x$ and $\bigcup\bigcup(x, y) = x \cup y$ and $\bigcap\bigcup(x, y) = x \cap y$.*

Theorem. *If x is not a set or y is not a set then $\bigcup\bigcap(x,y) = 0$ and $\bigcap\bigcap(x,y) = \mathcal{U}$ and $\bigcup\bigcup(x,y) = \mathcal{U}$ and $\bigcap\bigcup(x,y) = 0$.*

Definition (51)**.** $1^{st}z = \bigcap\bigcap z$. *Let the* first coordinate *of z stand for $1^{st}z$.*

Definition (52)**.** $2^{nd}z = (\bigcap\bigcup z) \cup ((\bigcup\bigcup z) \sim \bigcup\bigcap z)$. *Let the* second coordinate *of z stand for $2^{nd}z$.*

Theorem (53)**.** $2^{nd}\mathcal{U} = \mathcal{U}$.

Theorem (54a)**.** *If x and y are sets then $1^{st}(x,y) = x$.*

Theorem (54b)**.** *If x and y are sets then $2^{nd}(x,y) = y$.*

Proof. Let x and y be sets. $2^{nd}(x,y) = (\bigcap\bigcup(x,y)) \cup ((\bigcup\bigcup(x,y)) \sim \bigcup\bigcap(x,y)) = (x \cap y) \cup ((x \cup y) \sim x) = y$. □

Theorem (54c)**.** *If x is not a set or y is not a set then $1^{st}(x,y) = \mathcal{U}$ and $2^{nd}(x,y) = \mathcal{U}$.*

Theorem (55)**.** *If x and y are sets and $(x,y) = (r,s)$ then $x = r$ and $y = s$.*

56 Definition *r is a relation if and only if for each member z of r there is x and y such that $z = (x,y)$.*

A *relation* is a class whose members are ordered pairs.

57 Definition $r \circ s = \{u$: for some x, some y and some z, $u = (x,z)$, $(x,y) \in s$ and $(y,z) \in r\}$.

The class $r \circ s$ is the *composition* of r and s.

To avoid excessive notation we agree that $\{(x,z): \cdots\}$ is to be identical with $\{u$: *for some x, some z, $u = (x,z)$ and* $\cdots\}$. Thus $r \circ s = \{(x,z)$: *for some y, $(x,y) \in s$ and $(y,z) \in r$*$\}$.

58 Theorem $(r \circ s) \circ t = r \circ (s \circ t)$.

59 Theorem $r \circ (s \cup t) = (r \circ s) \cup (r \circ t)$ *and* $r \circ (s \cap t) \subset (r \circ s) \cap (r \circ t)$.

60 Definition $r^{-1} = \{(x,y): (y,x) \in r\}$.

If r is a relation r^{-1} is the *relation inverse to r.*

61 Theorem $(r^{-1})^{-1} = r$.

62 Theorem $(r \circ s)^{-1} = s^{-1} \circ r^{-1}$.

FUNCTIONS

Intuitively, a function is to be identical with the class of ordered pairs which is its graph. All functions are single-valued, and consequently two distinct ordered pairs belonging to a function must have different first coordinates.

63 Definition *f is a function if and only if f is a relation and for each x, each y, each z, if $(x,y) \in f$ and $(x,z) \in f$, then $y = z$.*

64 Theorem *If f is a function and g is a function so is $f \circ g$.*

65 Definition domain $f = \{x$: for some y, $(x,y) \in f\}$.

66 Definition range $f = \{y$: for some x, $(x,y) \in f\}$.

67 Theorem domain $\mathcal{U} = \mathcal{U}$ *and* range $\mathcal{U} = \mathcal{U}$.

Proof If $x \in \mathcal{U}$, then $(x,0)$ and $(0,x)$ belong to $\mathcal{U}$ and hence x belongs to *domain* $\mathcal{U}$ and *range* $\mathcal{U}$. ∎

ELEMENTARY SET THEORY

An SAD3 Formalisation of the Appendix of "General Topology" by John L. Kelley Relations and Preliminaries

October 26, 2018

0.1 Preliminaries

[prove off]
Let x, y, z stand for *classes*.
[object/-s]

Signature (Ontology). *An object is a notion. Let a, b, c, d, e stand for objects.*

Let $a \in x$ stand for a is an *element* of x.

Axiom. *Every element of x is an object.*

Axiom (I). *For each x for each y $x = y$ iff for each z $z \in x$ iff $z \in y$.*

[set/-s]

Definition (1). *A* set *is a class that is an object.*

Definition (2). $x \cup y = \{object\ u \mid u \in x\ or\ u \in y\}$.

Definition (3). $x \cap y = \{object\ u \mid u \in x\ and\ u \in y\}$.

Definition (25). *A* subclass *of y is a class x such that each element of x is an element of y. Let $x \subset y$ stand for x is a subclass of y. Let x is* contained *in y stand for $x \subset y$.*

Theorem (27). *$x = y$ iff $x \subset y$ and $y \subset x$.*

Theorem (28). *If $x \subset y$ and $y \subset z$ then $x \subset z$.*

Signature (48). *(a, b) is an object.*

Definition (48a). *An* ordered pair *is an object c such that there exist objects a and b such that $c = (a, b)$.*

Axiom (55). *If $(a, b) = (c, d)$ then $a = c$ and $b = d$.*

0.2 Relations

[relation/-s]

Definition (56)**.** *A* relation *is a class r such that every element of r is an ordered pair.*

Let r, s, t stand for relations.

Definition (57)**.** $r \circ s = \{(x, z) \mid x, z$ *are objects and there exists b such that* $(x, b) \in s$ *and* $(b, z) \in r\}$.

Theorem (58)**.** $(r \circ s) \circ t = r \circ (s \circ t)$.

Proof. $(r \circ s) \circ t \subset r \circ (s \circ t)$ and $r \circ (s \circ t) \subset (r \circ s) \circ t$. □

[/prove]

Theorem (59a)**.** $r \circ (s \cup t) = (r \circ s) \cup (r \circ t)$.

Proof. $r \circ (s \cup t) \subset (r \circ s) \cup (r \circ t)$. $(r \circ s) \cup (r \circ t) \subset r \circ (s \cup t)$. □

Theorem (59b)**.** $r \circ (s \cap t) \subset (r \circ s) \cap (r \circ t)$.

Definition (60)**.** $r^{-1} = \{(b, a) \mid a, b$ *are objects and* $(a, b) \in r\}$. *Let the* relation inverse *to r stand for r^{-1}.*

Lemma. r^{-1} *is a relation.*

Theorem (61)**.** $(r^{-1})^{-1} = r$.

Proof. $r \subset (r^{-1})^{-1}$. $(r^{-1})^{-1} \subset r$. □

Lemma (62a)**.** *Assume $r \subset s$. Then $r^{-1} \subset s^{-1}$.*

Lemma (62b)**.** $(r \circ s)^{-1} \subset (s^{-1}) \circ (r^{-1})$.

Lemma. $(s^{-1}) \circ (r^{-1}) \subset (r \circ s)^{-1}$.

Proof. $((s^{-1}) \circ (r^{-1}))^{-1} \subset ((r^{-1})^{-1}) \circ ((s^{-1})^{-1})$ (by 62b) . $((s^{-1}) \circ (r^{-1}))^{-1} \subset r \circ s$ (by 61) . $(((s^{-1}) \circ (r^{-1}))^{-1})^{-1} \subset (r \circ s)^{-1}$ (by 62a). $(s^{-1}) \circ (r^{-1}) \subset (r \circ s)^{-1}$ (by 61). □

Theorem (62)**.** $(r \circ s)^{-1} = (s^{-1}) \circ (r^{-1})$.

Proof. $(r \circ s)^{-1} \subset (s^{-1}) \circ (r^{-1})$. $(s^{-1}) \circ (r^{-1}) \subset (r \circ s)^{-1}$. □

74 THEOREM *If x and y are sets so is $x \times y$.*

PROOF Let f be the function such that *domain* $f = x$ and $f(u) = \{u\} \times y$ for u in x. (There is a unique function of this sort; namely, $f = \{(u,z)\colon u \in x \text{ and } z = \{u\} \times y\}$.) Because of the axiom of substitution, *range* f is a set. By a direct computation range $f = \{z\colon \text{for some } u,\, u \in x \text{ and } z = \{u\} \times y\}$. Consequently $\bigcup$ *range* f, which by the axiom of amalgamation is a set, is $x \times y$. ▮

75 THEOREM *If f is a function and* domain f *is a set, then f is a set.*

PROOF For $f \subset (\text{domain } f) \times (\text{range } f)$. ▮

76 DEFINITION $y^x = \{f\colon f \text{ is a function, domain } f = x \text{ and range } f \subset y\}$.

77 THEOREM *If x and y are sets so is y^x.*

PROOF If $f \in y^x$, then $f \subset x \times y$, which is a set, and hence $f \in 2^{x \times y}$ (theorem 38) and $2^{x \times y}$ is a set. Since $y^x \subset 2^{x \times y}$ it follows from the axiom of subsets that y^x is a set. ▮

For convenience, three more definitions are made.

78 DEFINITION *f is on x if and only if f is a function and $x =$* domain f.

79 DEFINITION *f is to y if and only if f is a function and* range $f \subset y$.

80 DEFINITION *f is onto y if and only if f is a function and* range $f = y$.

WELL ORDERING

Many of the results of this section are not needed in the development of the integers, ordinals, and cardinals which follows. They are included here because they are interesting in themselves and because the methods are simplified forms of the constructions used later.

Since the basic constructive results have now been proved we are able to assume a somewhat less pedestrian pace.

ELEMENTARY SET THEORY

An SAD3 Formalisation of the Appendix of "General Topology" by John L. Kelley Functions and Preliminaries

October 26, 2018

0.1 Preliminaries

[prove off]
Let x, y, z stand for *classes.*
[object/-s]

Signature (Ontology)**.** *An object is a notion. Let a, b, c, d, e, u, v stand for objects.*

Let $a \in x$ stand for a is an *element* of x.

Axiom. *Every element of x is an object.*

Axiom (I)**.** *For each x for each y $x = y$ iff for each z $z \in x$ iff $z \in y$.*

[set/-s]

Definition (1)**.** *A* set *is a class that is an object.*

Definition (2)**.** $x \cup y = \{object\ u \mid u \in x \ or\ u \in y\}$.

Definition (23)**.** $\bigcup x = \{objectu \mid \ for\ some\ y(y \in x \ and\ u \in y)\}$. *Let the* union *of x stand for $\bigcup x$.*

Definition (25)**.** *A* subclass *of y is a class x such that each element of x is an element of y. Let $x \subset y$ stand for x is a subclass of y. Let x is* contained *in y stand for $x \subset y$.*

Theorem (27)**.** *$x = y$ iff $x \subset y$ and $y \subset x$.*

Theorem (28)**.** *If $x \subset y$ and $y \subset z$ then $x \subset z$.*

Axiom (III)**.** *If x is a set then there is a set y such that for each z if $z \subset x$ then $z \in y$.*

Theorem (33)**.** *If x is a set and $z \subset x$ then z is a set.*

Definition (36)**.** $2^x = \{set\ y \mid y \subset x\}$.

Theorem (38a)**.** *If x is a set then 2^x is a set.*

Proof. Let x be a set. Take a set y such that for each z if $z \subset x$ then $z \in y$ (by III). Then $2^x \subset y$. □

Definition (40)**.** $\{a\} = \{a\}$.

Signature (48)**.** *(a, b) is an object.*

Definition (48a)**.** *An* ordered pair *is an object c such that there exist objects a and b such that $c = (a, b)$.*

Axiom (55)**.** *If $(a, b) = (c, d)$ then $a = c$ and $b = d$.*

[relation/-s]

Definition (56)**.** *A* relation *is a class r such that every element of r is an ordered pair.*

Let r, s, t stand for relations.

Definition (57)**.** $r \circ s = \{(x, z) \mid x, z$ *are objects and there exists b such that* $(x, b) \in s$ *and* $(b, z) \in r\}$.

0.2 Functions (Maps)

Since "function" is predefined in SAD3, we use the word "map" instead.

[/prove] [map/-s]

Definition (63)**.** *A* map *is a relation f such that for each a, b, c if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$. Let f, g stand for maps.*

Theorem (64)**.** *If f, g are maps then $f \circ g$ is a map.*

Definition (65)**.** $\mathrm{domain} f = \{object\ u \mid$ *there exists an object v such that* $(u, v) \in f\}$.

Definition (66)**.** $\mathrm{range} f = \{object\ v \mid$ *there exists an object u such that* $(u, v) \in f\}$.

Signature (68)**.** *Let $u \in \mathrm{domain} f$. The value of f at u is an object v such that $(u, v) \in f$. Let $f(u)$ stand for the value of f at u.*

Theorem (70)**.** *Let f be a map. Then $f = \{(u, f(u)) \mid u \in \mathrm{domain} f\}$.*

Theorem (71)**.** *Assume* $\mathrm{domain} f = \mathrm{domain} g$ *and for every element u of* $\mathrm{domain} f$ $f(u) = g(u)$. *Then $f = g$.*

Axiom (V)**.** *If f is a map and* $\mathrm{domain} f$ *is a set then* $\mathrm{range} f$ *is a set.*

Axiom (VI)**.** *If x is a set then $\bigcup x$ is a set.*

Definition (72)**.** $x \times y = \{(u, v) \mid u \in x$ *and* $v \in y\}$.

Theorem (73)**.** *Let u be an object. Let y be a set. Then $\{u\} \times y$ is a set.*

Proof. Define $f = \{(w, v) \mid w \in y$ and $v = (u, w)\}$. f is a map. domain$f = y$. range$f = \{u\} \times y$. □

Theorem (74)**.** *Let x, y be sets. Then $x \times y$ is a set.*

Proof. Define $f = \{(u, w) \mid u \in x$ and $w = \{u\} \times y\}$. f is a map. domain$f = x$. range$f$ is a set. range$f = \{$set $z \mid$ there exists $u \in x$ such that $z = \{u\} \times y\}$. $\bigcup$(range$f$) is a set. $\bigcup$(range$f$) $\subset x \times y$. Let us show that $x \times y \subset \bigcup$(range$f$). Let $w \in x \times y$. Take an $u \in x$ and $v \in y$ such that $w = (u, v)$. $w \in \{u\} \times y \in$ range$f$. $w \in \bigcup$range$f$. end. □

Theorem (75)**.** *Let f be a map. Let* domain$f$ *be a set. Then f is a set.*

Proof. $f \subset$ domain$f \times$ range$f$. □

Definition (76)**.** $y^x = \{$*map* $f \mid$ domain$f = x$ *and* range$f \subset y\}$.

Theorem (77)**.** *Let x, y be sets. Then y^x is a set.*

Proof. $y^x \subset 2^{x \times y}$. □

Definition (78)**.** f *is* on x *iff* $x =$ domain$f$.

Definition (79)**.** f *is* to y *iff* range$f \subset y$.

Definition (80)**.** f *is* onto y *iff* range$f = y$.