Contents

Formaliz. Math. 27 (4)

AIM Loops and the AIM Conjecture	
By Chad E. Brown and Karol Pąk	321
Formal Development of Rough Inclusion Functions	
By Adam Grabowski	



AIM Loops and the AIM $Conjecture^1$

Chad E. Brown Český Institut Informatiky Robotiky a Kybernetiky Zikova 4, 166 36 Praha 6, Czech Republic

> Karol Pąk[®] Institute of Informatics University of Białystok Poland

Summary. In this article, we prove, using the Mizar [2] formalism, a number of properties that correspond to the AIM Conjecture. In the first section, we define division operations on loops, inner mappings T, L and R, commutators and associators and basic attributes of interest. We also consider subloops and homomorphisms. Particular subloops are the nucleus and center of a loop and kernels of homomorphisms. Then in Section 2, we define a set Mlt Q of multiplicative mappings of Q and cosets (mostly following Albert 1943 for cosets [1]). Next, in Section 3 we define the notion of a normal subloop and construct quotients by normal subloops. In the last section we define the set InnAut of inner mappings of Q, define the notion of an AIM loop and relate this to the conditions on T, L, and R defined by satisfies TT, etc. We prove in Theorem (67) that the nucleus of an AIM loop is normal and finally in Theorem (68) that the AIM Conjecture follows from knowing every AIM loop satisfies aa1, aa2, aa3, Ka, aK1, aK2 and aK3.

The formalization follows M.K. Kinyon, R. Veroff, P. Vojtechovsky [4] (in [3]) as well as Veroff's Prover9 files.

MSC: 20N05 68T99 03B35

Keywords: loops; Abelian inner mapping; groups

MML identifier: AIMLOOP, version: 8.1.09 5.59.1363

¹This work has been supported by the European Research Council (ERC) Consolidator grant nr. 649043 *AI4REASON* and the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

1. LOOPS – INTRODUCTION

From now on Q, Q_1 , Q_2 denote multiplicative loops and x, y, z, w, u, v denote elements of Q. Let X be a 1-sorted structure.

A permutation of X is a permutation of the carrier of X. Let Y be a 1-sorted structure. The functor Y^X yielding a set is defined by the term

(Def. 1) (the carrier of Y)^{α}, where α is the carrier of X.

Let X, Y be 1-sorted structures. Let us observe that Y^X is functional.

Let Q be an invertible, left mult-cancelable, non empty multiplicative loop structure and x, y be elements of Q. The functor $x \setminus y$ yielding an element of Qis defined by

(Def. 2) $x \cdot it = y$.

Let Q be an invertible, right mult-cancelable, non empty multiplicative loop structure. The functor x/y yielding an element of Q is defined by

(Def. 3) $it \cdot y = x$.

Let us consider Q, x, and y. Note that $x \setminus (x \cdot y)$ reduces to y and $x \cdot (x \setminus y)$ reduces to y and $x \cdot y/y$ reduces to x and $(x/y) \cdot y$ reduces to x.

Let Q be an invertible, left mult-cancelable, non empty multiplicative loop structure and u, x be elements of Q. The functor T(u, x) yielding an element of Q is defined by the term

(Def. 4)
$$x \setminus (u \cdot x)$$
.

Let u, x, y be elements of Q. The functor L(u, x, y) yielding an element of Q is defined by the term

(Def. 5) $y \cdot x \setminus (y \cdot (x \cdot u)).$

Let Q be an invertible, right mult-cancelable, non empty multiplicative loop structure. The functor $\mathbf{R}(u, x, y)$ yielding an element of Q is defined by the term (Def. 6) $u \cdot x \cdot y/(x \cdot y)$.

Let us consider Q. We say that Q satisfies TT if and only if

- (Def. 7) for every elements u, x, y of Q, T(T(u, x), y) = T(T(u, y), x). We say that Q satisfies TL if and only if
- (Def. 8) for every elements u, x, y, z of Q, T(L(u, x, y), z) = L(T(u, z), x, y). We say that Q satisfies TR if and only if
- (Def. 9) for every elements u, x, y, z of Q, T(R(u, x, y), z) = R(T(u, z), x, y). We say that Q satisfies LR if and only if
- (Def. 10) for every elements u, x, y, z, w of Q, L(R(u, x, y), z, w) = R(L(u, z, w), x, y). We say that Q satisfies LL if and only if
- (Def. 11) for every elements u, x, y, z, w of Q, L(L(u, x, y), z, w) = L(L(u, z, w), x, y).

We say that Q satisfies RR if and only if

- (Def. 12) for every elements u, x, y, z, w of Q, $\mathbb{R}(\mathbb{R}(u, x, y), z, w) = \mathbb{R}(\mathbb{R}(u, z, w), x, y)$. Let us consider x and y. The functor $\mathbb{K}(x, y)$ yielding an element of Q is defined by the term
- (Def. 13) $y \cdot x \setminus (x \cdot y)$.

Let us consider z. The functor a(x, y, z) yielding an element of Q is defined by the term

(Def. 14) $x \cdot (y \cdot z) \setminus (x \cdot y \cdot z)$.

Let Q be a multiplicative loop. We say that Q satisfies an if and only if

(Def. 15) for every elements x, y, z, u, w of Q, $a(a(x, y, z), u, w) = 1_Q$.

We say that Q satisfies an 2 if and only if

- (Def. 16) for every elements x, y, z, u, w of Q, $a(x, a(y, z, u), w) = 1_Q$. We say that Q satisfies aa3 if and only if
- (Def. 17) for every elements x, y, z, u, w of Q, $a(x, y, a(z, u, w)) = 1_Q$. We say that Q satisfies Ka if and only if
- (Def. 18) for every elements x, y, z, u of Q, $K(a(x, y, z), u) = 1_Q$. We say that Q satisfies aK1 if and only if
- (Def. 19) for every elements x, y, z, u of Q, $a(K(x, y), z, u) = 1_Q$. We say that Q satisfies aK2 if and only if
- (Def. 20) for every elements x, y, z, u of Q, $a(x, K(y, z), u) = 1_Q$. We say that Q satisfies aK3 if and only if
- (Def. 21) for every elements x, y, z, u of Q, $\mathbf{a}(x, y, \mathbf{K}(z, u)) = \mathbf{1}_Q$.

Let us observe that there exists a multiplicative loop which is strict and satisfies TT, TL, TR, LR, LL, RR, aa1, aa2, aa3, Ka, aK1, aK2, and aK3.

Now we state the propositions:

- (1) If $x \cdot y = u$ and $x \cdot z = u$, then y = z.
- (2) If $y \cdot x = u$ and $z \cdot x = u$, then y = z.
- (3) If $x \cdot y = x \cdot z$, then y = z.
- (4) If $y \cdot x = z \cdot x$, then y = z.

Let us consider Q and x. Let us observe that $1_Q \setminus x$ reduces to x and $x/(1_Q)$ reduces to x. Let us consider y. Observe that $y/(x \setminus y)$ reduces to x and $(y/x) \setminus y$ reduces to x. Now we state the propositions:

- (5) $x \setminus x = 1_Q$.
- (6) $x/x = 1_Q$.
- (7) If $x \setminus y = 1_Q$, then x = y.
- (8) If $x/y = 1_Q$, then x = y.

- (9) If $a(x, y, z) = 1_Q$, then $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- (10) If $K(x, y) = 1_Q$, then $x \cdot y = y \cdot x$.
- (11) If $a(x, y, z) = 1_Q$, then L(z, y, x) = z. The theorem is a consequence of (9).

Let us consider Q. The functors: $\operatorname{Nucl}_{l}(Q)$, $\operatorname{Nucl}_{m}(Q)$, $\operatorname{Nucl}_{r}(Q)$, and $\operatorname{Comm}(Q)$ yielding subsets of Q are defined by conditions

- (Def. 22) $x \in \text{Nucl}(Q)$ iff for every y and z, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- (Def. 23) $y \in \operatorname{Nucl}_{\mathbf{m}}(Q)$ iff for every x and z, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- (Def. 24) $z \in \text{Nucl}_{r}(Q)$ iff for every x and y, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- (Def. 25) $x \in \text{Comm}(Q)$ iff for every $y, x \cdot y = y \cdot x$,

respectively. The functor $\operatorname{Nucl}(Q)$ yielding a subset of Q is defined by the term (Def. 26) $(\operatorname{Nucl}_1(Q) \cap \operatorname{Nucl}_m(Q)) \cap \operatorname{Nucl}_r(Q)$.

Now we state the proposition:

(12) $x \in \text{Nucl}(Q)$ if and only if $x \in \text{Nucl}(Q)$ and $x \in \text{Nucl}(Q)$ and $x \in \text{Nucl}(Q)$.

Let us consider Q. The functor Cent(Q) yielding a subset of Q is defined by the term

(Def. 27) $\operatorname{Comm}(Q) \cap \operatorname{Nucl}(Q)$.

Let Q_1, Q_2 be multiplicative loops and f be a function from Q_1 into Q_2 . We say that f is unity-preserving if and only if

(Def. 28) $f(1_{Q_1}) = 1_{Q_2}$.

We say that f is quasi-homomorphic if and only if

(Def. 29) for every elements x, y of $Q_1, f(x \cdot y) = f(x) \cdot f(y)$.

We say that f is homomorphic if and only if

(Def. 30) f is unity-preserving and quasi-homomorphic.

Observe that every function from Q_1 into Q_2 which is unity-preserving and quasi-homomorphic is also homomorphic and every function from Q_1 into Q_2 which is homomorphic is also unity-preserving and quasi-homomorphic and $\Omega_{Q_1} \mapsto 1_{Q_2}$ is homomorphic as a function from Q_1 into Q_2 and there exists a function from Q_1 into Q_2 which is homomorphic.

Let us consider Q and Q_2 . Let f be a homomorphic function from Q into Q_2 . The functor Ker f yielding a subset of Q is defined by

(Def. 31) $x \in it \text{ iff } f(x) = 1_{Q_2}$.

Let us consider a homomorphic function f from Q_1 into Q_2 and elements x, y of Q_1 . Now we state the propositions:

- (13) $f(x \setminus y) = f(x) \setminus f(y).$
- (14) f(x/y) = f(x)/f(y).

- (15) Let us consider a homomorphic function f from Q_1 into Q_2 . Suppose for every element y of Q_2 , there exists an element x of Q_1 such that f(x) = y and for every elements x, y, z of $Q_1, a(x, y, z) \in \text{Ker } f$. Then Q_2 is associative. The theorem is a consequence of (13) and (9).
- (16) Let us consider multiplicative loop Q_1 satisfying aa1, aa2, aa3, aK1, aK2, and aK3, a multiplicative loop Q_2 , and a homomorphic function f from Q_1 into Q_2 . Suppose for every element y of Q_2 , there exists an element x of Q_1 such that f(x) = y and $\operatorname{Nucl}(Q_1) \subseteq \operatorname{Ker} f$. Then Q_2 is a commutative multiplicative group. The theorem is a consequence of (9), (12), (13), (10), and (15).
- (17) Let us consider multiplicative loop Q_1 satisfying aa1, aa2, aa3, and Ka, a multiplicative loop Q_2 , and a homomorphic function f from Q_1 into Q_2 . Suppose for every element y of Q_2 , there exists an element x of Q_1 such that f(x) = y and $\operatorname{Cent}(Q_1) \subseteq \operatorname{Ker} f$. Then Q_2 is a multiplicative group. The theorem is a consequence of (10), (9), (12), and (15).

Let Q be a non empty multiplicative loop structure. A sub-loop structure of Q is a non empty multiplicative loop structure defined by

(Def. 32) the carrier of $it \subseteq$ the carrier of Q and the multiplication of it = (the multiplication of Q) \upharpoonright (the carrier of it) and the one of it = the one of Q.

Let Q be a multiplicative loop. Let us note that there exists a sub-loop structure of Q which is well unital, invertible, cancelable, non empty, and strict.

A sub-loop of Q is a well unital, invertible, cancelable sub-loop structure of Q. Let Q be a non empty multiplicative loop structure, H be a sub-loop structure of Q, and A be a subset of H. The functor [@]A yielding a subset of Qis defined by the term

(Def. 33) A.

Let us consider Q. Let H_1 , H_2 be subsets of Q. The functor LoopClose1 (H_1, H_2) yielding a subset of Q is defined by

(Def. 34) $x \in it$ iff $x \in H_1$ or $x = 1_Q$ or there exists y and there exists z such that $y, z \in H_2$ and $(x = y \cdot z \text{ or } x = y \setminus z \text{ or } x = y/z)$.

Let H be a subset of Q. The functor lp(H) yielding a strict sub-loop of Q is defined by

(Def. 35) $H \subseteq \Omega_{it}$ and for every sub-loop H_2 of Q such that $H \subseteq \Omega_{H_2}$ holds $\Omega_{it} \subseteq \Omega_{H_2}$.

Now we state the propositions:

(18) Let us consider a subset H of Q. Suppose $1_Q \in H$ and for every x and y such that $x, y \in H$ holds $x \cdot y \in H$ and for every x and y such that x,

 $y \in H$ holds $x \setminus y \in H$ and for every x and y such that $x, y \in H$ holds $x/y \in H$. Then $\Omega_{lp(H)} = H$.

PROOF: Reconsider $O = 1_Q$ as an element of H.

Set $m_2 = (\text{the multiplication of } Q) \upharpoonright H$. Set $L_4 = \langle H, m_2, O \rangle$ by [5, (1)]. L_4 is a sub-loop of Q. \Box

- (19) Let us consider a homomorphic function f from Q into Q_2 . Then $\Omega_{\operatorname{lp}(\operatorname{Ker} f)} = \operatorname{Ker} f$. The theorem is a consequence of (13), (14), and (18).
- (20) $1_Q \in \operatorname{Nucl}(Q).$
- (21) $1_Q \in \operatorname{Nucl}_{\mathrm{m}}(Q).$
- (22) $1_Q \in \operatorname{Nucl}_{\mathbf{r}}(Q).$
- (23) $1_Q \in \text{Nucl}(Q)$. The theorem is a consequence of (20), (21), (12), and (22).

Let us consider Q. Note that $\operatorname{Nucl}_{l}(Q)$ is non empty and $\operatorname{Nucl}_{m}(Q)$ is non empty and $\operatorname{Nucl}_{r}(Q)$ is non empty and $\operatorname{Nucl}_{r}(Q)$ is non empty.

- (24) If $x, y \in \text{Nucl}(Q)$, then $x \cdot y \in \text{Nucl}(Q)$. The theorem is a consequence of (12).
- (25) If $x, y \in \text{Nucl}(Q)$, then $x \setminus y \in \text{Nucl}(Q)$. The theorem is a consequence of (12) and (1).
- (26) If $x, y \in \text{Nucl}(Q)$, then $x/y \in \text{Nucl}(Q)$. The theorem is a consequence of (12) and (2).
- (27) $\Omega_{\text{lp(Nucl}(Q))} = \text{Nucl}(Q)$. The theorem is a consequence of (23), (24), (25), (26), and (18).
- (28) $\Omega_{\text{lp(Cent}(Q))} = \text{Cent}(Q)$. The theorem is a consequence of (23), (12), (24), (25), (26), and (18).

2. Multiplicative Mappings and Cosets

Let X be a functional set. We say that X is composition-closed if and only if

(Def. 36) for every elements f, g of X such that $f, g \in X$ holds $f \cdot g \in X$.

We say that X is inverse-closed if and only if

(Def. 37) for every element f of X such that $f \in X$ holds $f^{-1} \in X$.

Let A be a set. One can verify that $\{id_A\}$ is composition-closed and inverseclosed and there exists a functional set which is composition-closed, inverseclosed, and non empty.

Let Q be a multiplicative loop structure. Let us note that there exists a subset of Q^Q which is composition-closed, inverse-closed, and non empty. Let Q be a non empty multiplicative loop structure, H be a subset of Q, and S be a subset of Q^Q . We say that H is left-right-mult-closed w.r.t. S if and only if

(Def. 38) for every element u of Q such that $u \in H$ holds (curry(the multiplication of Q))(u), (curry'(the multiplication of Q)) $(u) \in S$.

The functor MltClos1(H, S) yielding a subset of Q^Q is defined by

(Def. 39) for every object $f, f \in it$ iff there exists an element u of Q such that $u \in H$ and $f = (\operatorname{curry}'(\text{the multiplication of } Q))(u)$ or there exists an element u of Q such that $u \in H$ and $f = (\operatorname{curry}(\text{the multiplication of } Q))(u)$ or there exist permutations g, h of Q such that $g, h \in S$ and $f = g \cdot h$ or there exists a permutation g of Q such that $g \in S$ and $f = g^{-1}$.

Now we state the propositions:

- (29) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q} . Suppose for every subset X of Q^Q , $\varphi(X) = \text{MltClos1}(H, X)$. Then φ is \subseteq -monotone.
- (30) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q} . Suppose for every subset X of Q^Q , $\varphi(X) = \text{MltClos1}(H, X)$. Let us consider a subset Y of Q^Q . Suppose $\varphi(Y) \subseteq Y$. Then
 - (i) for every element u of Q such that $u \in H$ holds (curry(the multiplication of Q)) $(u) \in Y$, and
 - (ii) for every element u of Q such that $u \in H$ holds (curry'(the multiplication of Q)) $(u) \in Y$.
- (31) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q} . Suppose for every subset X of Q^Q , $\varphi(X) = \text{MltClos1}(H, X)$. Let us consider a subset Y of Q^Q . Suppose for every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $Y \subseteq S$. Let us consider an element f of Q^Q . If $f \in Y$, then f is a permutation of Q. PROOF: Set $S_3 =$ the set of all f where f is a permutation of Q. $S_3 \subseteq Q^Q$. $\varphi(S_3) \subseteq S_3$. \Box
- (32) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q} . Suppose for every subset X of Q^Q , $\varphi(X) = \text{MltClos1}(H, X)$. Let us consider a subset Y of Q^Q . Suppose Y is a fixpoint of φ and for every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $Y \subseteq S$. Then Y is composition-closed and inverse-closed. The theorem is a consequence of (31).
- (33) (curry(the multiplication of Q))(u) is a permutation of Q. PROOF: Set f = (curry(the multiplication of <math>Q))(u). Define $\mathcal{G}(element of Q) = u \setminus$ \$1. Consider g being a function from Q into Q such that for

every element x of Q, $g(x) = \mathcal{G}(x)$. For every element x of Q, $(g \cdot f)(x) = (\mathrm{id}_Q)(x)$. For every element x of Q, $(f \cdot g)(x) = (\mathrm{id}_Q)(x)$. \Box

(34) (curry'(the multiplication of Q))(u) is a permutation of the carrier of Q. PROOF: Set f = (curry'(the multiplication of <math>Q))(u). Define $\mathcal{G}(element$ of Q) = $\$_1/u$. Consider g being a function from Q into Q such that for every element x of Q, $g(x) = \mathcal{G}(x)$. For every element x of Q, $(g \cdot f)(x) = (id_Q)(x)$. For every element x of Q, $(f \cdot g)(x) = (id_Q)(x)$. \Box

Let us consider Q. Let H be a subset of Q. The functor Mlt(H) yielding a composition-closed, inverse-closed subset of Q^Q is defined by

(Def. 40) H is left-right-mult-closed w.r.t. it and for every composition-closed, inverse-closed subset X of Q^Q such that H is left-right-mult-closed w.r.t. X holds $it \subseteq X$.

Let us consider a subset H of Q and an element u of Q. Now we state the propositions:

- (35) If $u \in H$, then (curry(the multiplication of Q)) $(u) \in Mlt(H)$.
- (36) If $u \in H$, then $(\operatorname{curry}'(\operatorname{the multiplication of } Q))(u) \in \operatorname{Mlt}(H)$.
- (37) Let us consider a subset H of Q, and a function φ from 2^{Q^Q} into 2^{Q^Q} . Suppose for every subset X of Q^Q , $\varphi(X) = \text{MltClos1}(H, X)$. Then
 - (i) Mlt(H) is a fixpoint of φ , and
 - (ii) for every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $Mlt(H) \subseteq S$.

The theorem is a consequence of (36), (35), (33), (34), and (31).

(38) Let us consider a subset H of Q, and an element f of Q^Q . If $f \in Mlt(H)$, then f is a permutation of Q. PROOF: Define $\mathcal{M}(\text{subset of } Q^Q) = MltClos1(H, \$_1)$. Consider φ being a function from 2^{Q^Q} into 2^{Q^Q} such that for every subset X of Q^Q , $\varphi(X) = \mathcal{M}(X)$. For every subset S of Q^Q such that $\varphi(S) \subseteq S$ holds $Mlt(H) \subseteq S$.

Let us consider Q. Let H be a subset of Q and x be an element of Q. The functor $x \cdot H$ yielding a subset of Q is defined by

(Def. 41) $y \in it$ iff there exists a permutation h of Q such that $h \in Mlt(H)$ and y = h(x).

Let H be a sub-loop of Q. The functor $x \cdot H$ yielding a subset of Q is defined by the term

(Def. 42) $x \cdot ({}^{@}\Omega_{H}).$

Let N be a sub-loop of Q. The functor Cosets(N) yielding a family of subsets of Q is defined by

(Def. 43) for every subset H of Q, $H \in it$ iff there exists x such that $H = x \cdot N$.

Let us note that Cosets(N) is non empty.

3. Normal Subloop

Let Q be a multiplicative loop structure and H_1 , H_2 be subsets of Q. The functors: $H_1 \cdot H_2$ and $H_1 \setminus H_2$ yielding subsets of Q are defined by conditions

- (Def. 44) for every element x of Q, $x \in H_1 \cdot H_2$ iff there exist elements y, z of Q such that $y \in H_1$ and $z \in H_2$ and $x = y \cdot z$,
- (Def. 45) for every element x of Q, $x \in H_1 \setminus H_2$ iff there exist elements y, z of Q such that $y \in H_1$ and $z \in H_2$ and $x = y \setminus z$,

respectively. Let Q be a multiplicative loop and H be a sub-loop of Q. We say that H is normal if and only if

(Def. 46) for every elements x, y of $Q, x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every element z of Q, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$.

Let us consider Q. One can verify that there exists a sub-loop of Q which is normal.

Let N be a normal sub-loop of Q. The functor SubLoopAsCoset(N) yielding an element of Cosets(N) is defined by the term

(Def. 47) $1_Q \cdot N$.

The functor CosetLoopOp(N) yielding a binary operation on Cosets(N) is defined by

(Def. 48) for every elements H_1 , H_2 of Cosets(N), $it(H_1, H_2) = H_1 \cdot H_2$.

The functor Q / N yielding a strict multiplicative loop structure is defined by the term

(Def. 49) $\langle \text{Cosets}(N), \text{CosetLoopOp}(N), \text{SubLoopAsCoset}(N) \rangle$.

One can check that Q / N is non empty and Q / N is well unital, invertible, and cancelable.

The functor QuotientHom(Q, N) yielding a function from Q into Q/N is defined by

(Def. 50) for every x, $it(x) = x \cdot N$.

Let us observe that QuotientHom(Q, N) is homomorphic. Now we state the propositions:

- (39) Let us consider a sub-loop H of Q, x, y, and elements x_1 , y_1 of H. If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.
- (40) Let us consider a sub-loop H of Q, x, and y. Suppose $x, y \in$ the carrier of H. Then $x \cdot y \in$ the carrier of H. The theorem is a consequence of (39).

- (41) Let us consider a sub-loop H of Q, x, y, and elements x_1 , y_1 of H. If $x = x_1$ and $y = y_1$, then $x \setminus y = x_1 \setminus y_1$. The theorem is a consequence of (39).
- (42) Let us consider a sub-loop H of Q, x, and y. Suppose $x, y \in$ the carrier of H. Then $x \setminus y \in$ the carrier of H. The theorem is a consequence of (41).
- (43) Let us consider a sub-loop H of Q, x, y, and elements x_1 , y_1 of H. If $x = x_1$ and $y = y_1$, then $x/y = x_1/y_1$. The theorem is a consequence of (39).
- (44) Let us consider a sub-loop H of Q, x, and y. Suppose x, y ∈ the carrier of H. Then x/y ∈ the carrier of H. The theorem is a consequence of (43). The scheme MltInd deals with a multiplicative loop Q and a subset H of Q and a unary predicate P and states that
- (Sch. 1) For every function f from Q into Q such that $f \in Mlt(\mathcal{H})$ holds $\mathcal{P}[f]$ provided
 - for every element u of \mathcal{Q} such that $u \in \mathcal{H}$ for every function f from \mathcal{Q} into \mathcal{Q} such that for every element x of \mathcal{Q} , $f(x) = x \cdot u$ holds $\mathcal{P}[f]$ and
 - for every element u of \mathcal{Q} such that $u \in \mathcal{H}$ for every function f from \mathcal{Q} into \mathcal{Q} such that for every element x of \mathcal{Q} , $f(x) = u \cdot x$ holds $\mathcal{P}[f]$ and
 - for every permutations g, h of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$ and
 - for every permutation g of \mathcal{Q} such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$.

Now we state the proposition:

(45) Let us consider a sub-loop N of Q, and a function f from Q into Q. Suppose $f \in Mlt({}^{@}\Omega_{N})$. $x \in {}^{@}\Omega_{N}$ if and only if $f(x) \in {}^{@}\Omega_{N}$.

PROOF: Reconsider $H = {}^{@}\Omega_N$ as a subset of Q. Define $\mathcal{P}[$ function from Q into $Q] \equiv$ for every $x, x \in H$ iff $\$_1(x) \in H$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = x \cdot u$ holds $\mathcal{P}[f]$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$. For every permutations g, h of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in Mlt(H)$ holds $\mathcal{P}[f]$. \Box

Let us consider a normal sub-loop N of Q. Now we state the propositions: (46) The carrier of $N = 1_Q \cdot N$.

PROOF: The carrier of $N \subseteq 1_Q \cdot N$. \Box

- (47) Ker QuotientHom $(Q, N) = {}^{@}\Omega_N$. PROOF: Set f =QuotientHom(Q, N). For every $x, x \in$ Ker f iff $x \in {}^{@}\Omega_N$. \Box
- (48) Let us consider a multiplicative loop Q_2 , a homomorphic function ffrom Q into Q_2 , and a function h from Q into Q. If $h \in Mlt(Ker f)$, then $f \cdot h = f$. PROOF: Set H = Ker f. Define $\mathcal{P}[$ function from Q into $Q] \equiv f \cdot \$_1 = f$. For every element u of Q such that $u \in H$ for every function h from Qinto Q such that for every element x of Q, $h(x) = x \cdot u$ holds $\mathcal{P}[h]$. For every element u of Q such that $u \in H$ for every function h from Q into Q such that for every element x of Q, $h(x) = u \cdot x$ holds $\mathcal{P}[h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in Mlt(H)$ holds $\mathcal{P}[f]$. \Box

Let us consider a multiplicative loop Q_2 , a homomorphic function f from Q into Q_2 , x, and y. Now we state the propositions:

- (49) $y \in x \cdot (\text{Ker } f)$ if and only if f(x) = f(y). PROOF: If $y \in x \cdot (\text{Ker } f)$, then f(x) = f(y). There exists a permutation h of Q such that $h \in \text{Mlt}(\text{Ker } f)$ and y = h(x). \Box
- (50) $y \in x \cdot (\operatorname{lp}(\operatorname{Ker} f))$ if and only if f(x) = f(y). The theorem is a consequence of (19) and (49).
- (51) $x \cdot (\operatorname{lp}(\operatorname{Ker} f)) = y \cdot (\operatorname{lp}(\operatorname{Ker} f))$ if and only if f(x) = f(y). The theorem is a consequence of (50).
- (52) Let us consider a multiplicative loop Q_2 , and a homomorphic function f from Q into Q_2 . Then lp(Ker f) is normal. PROOF: Set H = lp(Ker f). For every x and $y, x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$. For every x and $y, x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every z, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$. \Box
- (53) (i) $1_Q \in \Omega_{\operatorname{lp}(\operatorname{Cent}(Q))}$, and
 - (ii) $1_Q \in \operatorname{Cent}(Q)$.

The theorem is a consequence of (28).

- (54) Let us consider a function f from Q into Q. Suppose $f \in Mlt(Cent(Q))$. Then there exists z such that
 - (i) $z \in Cent(Q)$, and
 - (ii) for every $x, f(x) = x \cdot z$.

PROOF: Set H = Cent(Q). Define $\mathcal{P}[\text{function from } Q \text{ into } Q] \equiv \text{there}$ exists z such that $z \in H$ and for every x, $\$_1(x) = x \cdot z$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$. For every permutations g, h of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in \mathrm{Mlt}(H)$ holds $\mathcal{P}[f]$. \Box

- (55) $y \in x \cdot (\operatorname{lp}(\operatorname{Cent}(Q)))$ if and only if there exists z such that $z \in \operatorname{Cent}(Q)$ and $y = x \cdot z$. PROOF: If $y \in x \cdot (\operatorname{lp}(\operatorname{Cent}(Q)))$, then there exists z such that $z \in \operatorname{Cent}(Q)$ and $y = x \cdot z$. Reconsider $h = (\operatorname{curry}'(\text{the multiplication of } Q))(z)$ as a permutation of Q. There exists a permutation h of Q such that $h \in \operatorname{Mlt}(\operatorname{Cent}(Q))$ and h(x) = y. \Box
- (56) $x \cdot (\operatorname{lp}(\operatorname{Cent}(Q))) = y \cdot (\operatorname{lp}(\operatorname{Cent}(Q)))$ if and only if there exists z such that $z \in \operatorname{Cent}(Q)$ and $y = x \cdot z$. PROOF: If $x \cdot (\operatorname{lp}(\operatorname{Cent}(Q))) = y \cdot (\operatorname{lp}(\operatorname{Cent}(Q)))$, then there exists z such that $z \in \operatorname{Cent}(Q)$ and $y = x \cdot z$. If there exists z such that $z \in \operatorname{Cent}(Q)$ and $y = x \cdot z$, then $x \cdot (\operatorname{lp}(\operatorname{Cent}(Q))) = y \cdot (\operatorname{lp}(\operatorname{Cent}(Q)))$. \Box
- (57) lp(Cent(Q)) is normal.

PROOF: Set H = lp(Cent(Q)). For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$. For every x and y, $x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every z, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$. \Box

4. AIM CONJECTURE

Let Q be a multiplicative loop. The functor InnAut(Q) yielding a subset of Q^Q is defined by

(Def. 51) for every object $f, f \in it$ iff there exists a function g from Q into Q such that f = g and $g \in Mlt(\Omega_Q)$ and $g(1_Q) = 1_Q$.

Observe that InnAut(Q) is non empty, composition-closed, and inverse closed.

Now we state the proposition:

(58) Let us consider a function f from Q into Q. Then $f \in \text{InnAut}(Q)$ if and only if $f \in \text{Mlt}(\Omega_Q)$ and $f(1_Q) = 1_Q$.

Let Q be a multiplicative loop. We say that Q is an AIM if and only if

(Def. 52) for every functions f, g from Q into Q such that $f, g \in \text{InnAut}(Q)$ holds $f \cdot g = g \cdot f$.

Let us consider Q and x. The functor T(x) yielding a function from Q into Q is defined by

(Def. 53) for every u, it(u) = T(u, x).

Now we state the proposition:

(59) $T(x) \in \text{InnAut}(Q).$

PROOF: Set f = T(x). Reconsider g = (curry(the multiplication of Q))(x) as a permutation of the carrier of Q.

Reconsider h = (curry'(the multiplication of Q))(x) as a permutation of the carrier of Q. $f = g^{-1} \cdot h$. $g \in \text{Mlt}(\Omega_Q)$. $h \in \text{Mlt}(\Omega_Q)$. \Box

Let us consider Q, x, and y. The functor L(x, y) yielding a function from Q into Q is defined by

(Def. 54) for every u, it(u) = L(u, x, y).

Now we state the proposition:

(60) $L(x,y) \in \text{InnAut}(Q).$

PROOF: Set f = L(x, y). Reconsider $g = (\text{curry}(\text{the multiplication of } Q))(y \cdot x)$ as a permutation of the carrier of Q.

Reconsider h = (curry(the multiplication of Q))(x) as a permutation of the carrier of Q.

Reconsider k = (curry(the multiplication of Q))(y) as a permutation of the carrier of Q. $f = g^{-1} \cdot (k \cdot h)$. $g \in \text{Mlt}(\Omega_Q)$. $h, k \in \text{Mlt}(\Omega_Q)$. \Box

Let us consider Q, x, and y. The functor $\mathbb{R}(x, y)$ yielding a function from Q into Q is defined by

(Def. 55) for every u, $it(u) = \mathbf{R}(u, x, y)$.

Now we state the proposition:

(61) $\mathbf{R}(x, y) \in \mathrm{InnAut}(Q).$

PROOF: Set $f = \mathbb{R}(x, y)$. Reconsider $g = (\text{curry}'(\text{the multiplication of } Q))(x \cdot y)$ as a permutation of the carrier of Q.

Reconsider h = (curry'(the multiplication of Q))(x) as a permutation of the carrier of Q.

Reconsider k = (curry'(the multiplication of Q))(y) as a permutation of the carrier of Q. $f = g^{-1} \cdot (k \cdot h)$. $g \in \text{Mlt}(\Omega_Q)$. $h, k \in \text{Mlt}(\Omega_Q)$. \Box

Observe that Trivial-multLoopStr is an AIM and there exists a multiplicative loop which is non empty, strict, and AIM and every AIM multiplicative loop satisfies TT, TL, TR, LR, LL, and RR.

Now we state the propositions:

(62) Let us consider a function f from Q into Q. Suppose $f \in Mlt(Nucl(Q))$. Then there exists u and there exists v such that $u, v \in Nucl(Q)$ and for every $x, f(x) = u \cdot (x \cdot v)$.

PROOF: Set H = Nucl(Q). Define $\mathcal{P}[\text{function from } Q \text{ into } Q] \equiv \text{there}$ exists u and there exists v such that $u, v \in \text{Nucl}(Q)$ and for every x, $\$_1(x) = u \cdot (x \cdot v)$. For every element u of Q such that $u \in H$ for every function f from Q into Q such that for every element x of Q, $f(x) = x \cdot u$ holds $\mathcal{P}[f]$. For every element u of Q such that $u \in H$ for every function ffrom Q into Q such that for every element x of Q, $f(x) = u \cdot x$ holds $\mathcal{P}[f]$. For every permutations g, h of the carrier of Q such that $\mathcal{P}[g]$ and $\mathcal{P}[h]$ holds $\mathcal{P}[g \cdot h]$. For every permutation g of Q such that $\mathcal{P}[g]$ holds $\mathcal{P}[g^{-1}]$. For every function f from Q into Q such that $f \in \mathrm{Mlt}(H)$ holds $\mathcal{P}[f]$. \Box

- (63) $y \in x \cdot (\operatorname{lp}(\operatorname{Nucl}(Q)))$ if and only if there exists u and there exists v such that $u, v \in \operatorname{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$. PROOF: If $y \in x \cdot (\operatorname{lp}(\operatorname{Nucl}(Q)))$, then there exists u and there exists v such that $u, v \in \operatorname{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$. There exists a permutation h of the carrier of Q such that $h \in \operatorname{Mlt}(\operatorname{Nucl}(Q))$ and h(x) = y. \Box
- (64) $x \cdot (\operatorname{lp}(\operatorname{Nucl}(Q))) = y \cdot (\operatorname{lp}(\operatorname{Nucl}(Q)))$ if and only if there exists u and there exists v such that $u, v \in \operatorname{Nucl}(Q)$ and $y = u \cdot (x \cdot v)$. The theorem is a consequence of (23), (63), (12), (27), (44), (42), and (40).

Let us consider AIM multiplicative loop Q and elements x, u of Q. Now we state the propositions:

(65) If $u \in \operatorname{Nucl}(Q)$, then $\operatorname{T}(u, x) \in \operatorname{Nucl}(Q)$.

PROOF: $u \in \text{Nucl}_{l}(Q)$ and $u \in \text{Nucl}_{m}(Q)$ and $u \in \text{Nucl}_{r}(Q)$. For every elements y, z of $Q, (T(u, x) \cdot y) \cdot z = T(u, x) \cdot (y \cdot z)$. For every elements y, z of $Q, (y \cdot z) \cdot T(u, x) = y \cdot (z \cdot T(u, x))$. For every elements y, z of Q, $(y \cdot T(u, x)) \cdot z = y \cdot (T(u, x) \cdot z)$. \Box

(66) If
$$u \in \operatorname{Nucl}(Q)$$
, then $x \cdot u/x \in \operatorname{Nucl}(Q)$.

PROOF: $u \in \operatorname{Nucl}_{\mathbf{l}}(Q)$ and $u \in \operatorname{Nucl}_{\mathbf{m}}(Q)$ and $u \in \operatorname{Nucl}_{\mathbf{r}}(Q)$. Define $\mathcal{T}(\text{element of } Q) = x \cdot \$_1/x$. Consider t being a function from Q into Q such that for every element v of Q, $t(v) = \mathcal{T}(v)$. $t \in \operatorname{InnAut}(Q)$. For every elements y, z of Q, $(\mathcal{T}(u) \cdot y) \cdot z = \mathcal{T}(u) \cdot (y \cdot z)$. For every elements y, z of Q, $(\mathcal{T}(u) = y \cdot (z \cdot \mathcal{T}(u))$. For every elements y, z of Q, $(y \cdot z) \cdot \mathcal{T}(u) = y \cdot (z \cdot \mathcal{T}(u))$. For every elements y, z of Q, $(y \cdot \mathcal{T}(u)) \cdot z = y \cdot (\mathcal{T}(u) \cdot z)$. \Box

Now we state the proposition:

(67) If Q is an AIM, then lp(Nucl(Q)) is normal.

PROOF: Set H = lp(Nucl(Q)). For every elements x, y of Q, there exists an element v of Q such that $v \in Nucl(Q)$ and $y = x \cdot v$ iff there exist elements u, v of Q such that $u, v \in Nucl(Q)$ and $y = u \cdot (x \cdot v)$. For every elements x, y of $Q, y \in x \cdot H$ iff there exists an element v of Q such that $v \in Nucl(Q)$ and $y = x \cdot v$. For every elements x, y of $Q, x \cdot H = y \cdot H$ iff there exists an element v of Q such that $v \in Nucl(Q)$ and $y = x \cdot v$. For every xand $y, x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$. For every x and $y, x \cdot H \cdot (y \cdot H) = (x \cdot y) \cdot H$ and for every z, if $(x \cdot H) \cdot (y \cdot H) = x \cdot H \cdot (z \cdot H)$, then $y \cdot H = z \cdot H$ and if $(y \cdot H) \cdot (x \cdot H) = z \cdot H \cdot (x \cdot H)$, then $y \cdot H = z \cdot H$. \Box Let Q be AIM multiplicative loop. Let us observe that lp(Nucl(Q)) is normal. Let Q be a multiplicative loop. One can check that lp(Cent(Q)) is normal. Now we state the proposition:

(68) Main Theorem: THE AIM CONJECTURE

The AIM Conjecture follows from knowing every AIM loop satisfies aa1, aa2, aa3, Ka, aK1, aK2 and aK3. This theorem justifies using first-order theorem provers to try to prove the AIM Conjecture:

Suppose for every multiplicative loop Q such that Q satisfies TT, TL, TR, LR, LL, and RR holds Q satisfies aa1, aa2, aa3, Ka, aK1, aK2, and aK3. Let us consider AIM multiplicative loop Q. Then

- (i) $Q/\ln(\operatorname{Nucl}(Q))$ is a commutative multiplicative group, and
- (ii) $Q / \operatorname{lp}(\operatorname{Cent}(Q))$ is a multiplicative group.

The theorem is a consequence of (47), (27), (16), (28), and (17).

References

- A. A. Albert. Quasigroups. I. Transactions of the American Mathematical Society, 54(3): 507–519, 1943.
- [2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.
- Maria Paola Bonacina and Mark E. Stickel, editors. Automated Reasoning and Mathematics

 Essays in Memory of William W. McCune, volume 7788 of Lecture Notes in Computer Science, 2013. Springer.
- [4] Michael K. Kinyon, Robert Veroff, and Petr Vojtěchovský. Loops with abelian inner mapping groups: An application of automated deduction. In Bonacina and Stickel [3], pages 151–164.
- [5] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. Formalized Mathematics, 23(4):333–349, 2015. doi:10.1515/forma-2015-0027.

Accepted August 29, 2019



Formal Development of Rough Inclusion Functions

Adam Grabowski[©] Institute of Informatics University of Białystok Poland

Summary. Rough sets, developed by Pawlak [16], are important tool to describe situation of incomplete or partially unknown information. In this article, continuing the formalization of rough sets [13], we give the formal characterization of three rough inclusion functions (RIFs). We start with the standard one, κ^{\pounds} , connected with Łukasiewicz [15], and extend this research for two additional RIFs: κ_1 , and κ_2 , following a paper by Gomolińska [5], [4]. We also define q-RIFs and weak q-RIFs [3]. The paper establishes a formal counterpart of [8] and makes a preliminary step towards rough mereology [17], [18] in Mizar [14].

MSC: 03E70 68T99 03B35 Keywords: rough set; rough inclusion; approximation space MML identifier: ROUGHIF1, version: 8.1.09 5.59.1363

0. INTRODUCTION

In the paper, continuing our development of rough sets, we define three closely related rough inclusion functions (RIFs).

Until now, most of the Mizar formalization of rough sets [6], [9] was done by means of the notion of a generalized approximation space understood as a pair $\langle U, \rho \rangle$, where ρ is an indiscernibility relation defined on the universe U. This viewpoint, based on tolerances instead of equivalence relations, was studied by Skowron and Stepaniuk [19], then, in a general form, by Zhu [20], among many others, and the Mizar counterpart of it is included in [10] and [11]. In the alternative approach, used by Gomolińska [4], approximation spaces are treated as triples of the form

$$\mathcal{A} = (U, I, \kappa),$$

where U is a non-empty set called the universe, $I: U \mapsto \wp U$ is an uncertainty mapping, and $\kappa: \wp U \times \wp U \mapsto [0, 1]$ is a rough inclusion function. The formalization of uncertainty mappings was discussed in [13], and this article tries to define the missing part of the above definition, with future possibility of merging approaches via theory merging mechanism [7], avoiding duplication as much as we can [12].

We start with some preliminaries, which cover gaps in the existing state of the Mizar Mathematical Library. Section 2 deals with the standard rough inclusion function, which appears in some form in the research by Jan Łukasiewicz [15], obviously without any reference for rough sets. This pretty general Mizar functor κ^{\pounds} is defined as follows:

$$\kappa^{\pounds}(X,Y) = \begin{cases} \frac{|X \cap Y|}{|X|}, & \text{if } X \neq \emptyset \\ 1, & \text{otherwise} \end{cases}$$

For a given universe U, rough inclusion functions (RIFs for short) are the mappings κ from $\wp U \times \wp U$ into unit interval which satisfy two properties:

$$\operatorname{rif}_{1}(\kappa) \Leftrightarrow \forall_{X,Y \subseteq U} \ (\kappa(X,Y) = 1 \Leftrightarrow X \subseteq Y)$$

$$\operatorname{rif}_{2}(\kappa) \Leftrightarrow \forall_{X,Y,Z \subseteq U} \ (Y \subseteq Z \Rightarrow \kappa(X,Y) \leqslant \kappa(X,Z))$$

This is discussed in Sect. 3; corresponding Mizar modes RIF and preRIF are also introduced.

Besides κ^{\pounds} , there are two relatively well-known RIFs:

$$\kappa_1(X,Y) = \begin{cases} \frac{|Y|}{|X \cup Y|}, & \text{if } X \cup Y \neq \emptyset\\ 1, & \text{otherwise} \end{cases}$$
$$\kappa_2(X,Y) = \frac{|(U-X) \cup Y|}{|U|}.$$

Section 4 contains their definitions, both of the form of Mizar functors, and as set-theoretic functions.

It should be mentioned that in this Mizar translation (and also in the source code), predicative form of the properties of RIFs, as, for example, $\operatorname{rif}_1(\kappa)$ is replaced by the phrase " κ satisfies (RIF₁)" (and for others, respectively). In Sect. 5 we formulate some additional characteristic properties of rough inclusions; in Sect. 6 we show that, under the assumption that rif_1 holds, rif_2 can be replaced by rif₂^{*}. We introduce also some weakened versions of rough inclusions: quasi-RIF and weak quasi-RIF.

All three considered RIFs $(\kappa^{\pounds}, \kappa_1, \kappa_2)$ are distinct. Gomolińska takes $U = \{0, 1, 2, \ldots, 9\}, X = \{0, \ldots, 4\}, Y = \{2, \ldots, 6\}$. Then $\kappa^{\pounds}(X, Y) = 3/5, \kappa_1(X, Y) = 5/7$, and $\kappa_2(X, Y) = 4/5$. In Sect. 9, we constructed an example, which in Mizar is the functor ExampleRIFSpace, claiming that $U = \{1, 2, 3, 4, 5\}, X = \{1, 2\}, Y = \{2, 3, 4\}$ with $\kappa^{\pounds}(X, Y) = 1/2, \kappa_1(X, Y) = 3/4$, and $\kappa_2(X, Y) = 4/5$. Obviously, the indiscernibility relation does not matter, and so we took the identity as the simplest. The proofs, based on our specific example, are significantly shorter than those proposed by Gomolińska.

In the final section, we formalized two theorems from another Gomolińska's paper [2], which was already translated into Mizar [13], but without the notion of RIF; now we can fill this gap.

1. Preliminaries

Now we state the propositions:

(1) Let us consider real numbers a, b, c. If b > 0 and $a \le b$ and $c \ge 0$, then $\frac{a}{b} \le \frac{a+c}{b+c}$.

Observe that there exists an approximation space which is strict and finite.

Let R be a finite 1-sorted structure. One can check that every subset of R is finite.

From now on R denotes a 1-sorted structure and X, Y denote subsets of R.

(2) $X \subseteq Y$ if and only if $X^{c} \cup Y = \Omega_{R}$. PROOF: If $X \subseteq Y$, then $X^{c} \cup Y = \Omega_{R}$. \Box

From now on R denotes a finite 1-sorted structure and X, Y denote subsets of R. Now we state the propositions:

- (3) $\overline{\overline{X \cup Y}} = \overline{\overline{Y}}$ if and only if $X \subseteq Y$.
- (4) If $\overline{\overline{X^c \cup Y}} = \overline{\overline{\Omega_R}}$, then $X^c \cup Y = \Omega_R$.

Let R be a non empty 1-sorted structure and X be a subset of R. Note that $\Omega_R \cup X$ reduces to Ω_R and $\Omega_R \cap X$ reduces to X.

2. Standard Rough Inclusion Function

From now on R denotes a finite approximation space and X, Y, Z, W denote subsets of R.

Let R be a finite approximation space and X, Y be subsets of R. The functor $\kappa^{\pounds}(X, Y)$ yielding an element of [0, 1] is defined by the term



Now we state the propositions:

- (5) $\kappa^{\pounds}(\emptyset_R, X) = 1.$
- (6) $\kappa^{\pounds}(X, Y) = 1$ if and only if $X \subseteq Y$.
- (7) If $Y \subseteq Z$, then $\kappa^{\pounds}(X, Y) \leq \kappa^{\pounds}(X, Z)$.
- (8) If $Z \subseteq Y \subseteq X$, then $\kappa^{\pounds}(X, Z) \leq \kappa^{\pounds}(Y, Z)$.
- (9) $\kappa^{\pounds}(X, Y \cup Z) \leq \kappa^{\pounds}(X, Y) + \kappa^{\pounds}(X, Z).$
- (10) If $X \neq \emptyset$ and Y misses Z, then $\kappa^{\pounds}(X, Y \cup Z) = \kappa^{\pounds}(X, Y) + \kappa^{\pounds}(X, Z)$.

3. Rough Inclusion Functions

Let R be a 1-sorted structure.

A pre-rough inclusion function of R is a function from $2^{\text{(the carrier of }R)} \times 2^{\text{(the carrier of }R)}$ into [0, 1].

A preRIF of R is a pre-rough inclusion function of R.

The scheme BinOpEq deals with a non empty 1-sorted structure \mathcal{R} and a binary functor \mathcal{F} yielding an element of [0, 1] and states that

(Sch. 1) For every preRIFs f_1 , f_2 of \mathcal{R} such that for every subsets x, y of \mathcal{R} , $f_1(x,y) = \mathcal{F}(x,y)$ and for every subsets x, y of \mathcal{R} , $f_2(x,y) = \mathcal{F}(x,y)$ holds $f_1 = f_2$.

Let R be a finite approximation space. The functor $\kappa^{\pounds}(R)$ yielding a preRIF of R is defined by

(Def. 2) for every subsets x, y of R, $it(x, y) = \kappa^{\pounds}(x, y)$.

4. Defining Two New RIFs

Let R be a finite approximation space and X, Y be subsets of R. The functor $\kappa_1(X, Y)$ yielding an element of [0, 1] is defined by the term

(Def. 3)
$$\begin{cases} \frac{\overline{Y}}{\overline{X} \cup Y}, & \text{if } X \cup Y \neq \emptyset, \\ 1, & \text{otherwise.} \end{cases}$$

The functor $\kappa_2(X, Y)$ yielding an element of [0, 1] is defined by the term (Def. 4) $\frac{\overline{X^c \cup Y}}{\overline{\Omega_R}}$.

The functor $\kappa_1(R)$ yielding a preRIF of R is defined by

(Def. 5) for every subsets x, y of R, $it(x, y) = \kappa_1(x, y)$.

The functor $\kappa_2(R)$ yielding a preRIF of R is defined by

(Def. 6) for every subsets x, y of R, $it(x, y) = \kappa_2(x, y)$.

Now we state the propositions:

- (11) $\kappa_1(X,Y) = 1$ if and only if $X \subseteq Y$. The theorem is a consequence of (3).
- (12) $\kappa_2(X,Y) = 1$ if and only if $X \subseteq Y$. The theorem is a consequence of (2) and (4).
- (13) If $\kappa_1(X, Y) = 0$, then $Y = \emptyset$.
- (14) If $X \neq \emptyset$, then $\kappa_1(X, Y) = 0$ iff $Y = \emptyset$. The theorem is a consequence of (13).
- (15) $\kappa_2(X, Y) = 0$ if and only if $X = \Omega_R$ and $Y = \emptyset$.
- (16) If $Y \subseteq Z$, then $\kappa_1(X, Y) \leq \kappa_1(X, Z)$. The theorem is a consequence of (1).
- (17) If $Y \subseteq Z$, then $\kappa_2(X, Y) \leq \kappa_2(X, Z)$.
- (18) $\kappa_1(\emptyset_R, X) = 1$. The theorem is a consequence of (11).
- (19) $\kappa_2(\emptyset_R, X) = 1$. The theorem is a consequence of (12).

5. Characteristic Properties of Rough Inclusions

Let R be a non empty relational structure and κ be a preRIF of R. We say that κ satisfies (RIF₁) if and only if

(Def. 7) for every subsets X, Y of R, $\kappa(X, Y) = 1$ iff $X \subseteq Y$. We say that κ satisfies (RIF₂) if and only if

- (Def. 8) for every subsets X, Y, Z of R such that $Y \subseteq Z$ holds $\kappa(X, Y) \leq \kappa(X, Z)$. We say that κ satisfies (RIF₃) if and only if
- (Def. 9) for every subset X of R such that $X \neq \emptyset$ holds $\kappa(X, \emptyset_R) = 0$. We say that κ satisfies (RIF₄) if and only if
- (Def. 10) for every subsets X, Y of R such that $\kappa(X, Y) = 0$ holds X misses Y. We say that κ satisfies (RIF₀) if and only if
- (Def. 11) for every subsets X, Y of R such that $X \subseteq Y$ holds $\kappa(X, Y) = 1$. We say that κ satisfies $(\operatorname{RIF}_0^{-1})$ if and only if
- (Def. 12) for every subsets X, Y of R such that $\kappa(X,Y) = 1$ holds $X \subseteq Y$. We say that κ satisfies (RIF₂^{*}) if and only if
- (Def. 13) for every subsets X, Y, Z of R such that $\kappa(Y, Z) = 1$ holds $\kappa(X, Y) \leq \kappa(X, Z)$.

Observe that every preRIF of R which satisfies (RIF₁) satisfies also (RIF₀) and (RIF₀⁻¹) and every preRIF of R which satisfies (RIF₀) and (RIF₀⁻¹) satisfies also (RIF₁).

Let R be a finite approximation space. One can check that $\kappa^{\pounds}(R)$ satisfies (RIF₁) and $\kappa^{\pounds}(R)$ satisfies (RIF₂) and $\kappa_1(R)$ satisfies (RIF₁) and $\kappa_1(R)$ satisfies (RIF₂) and $\kappa_2(R)$ satisfies (RIF₁) and $\kappa_2(R)$ satisfies (RIF₂).

Let us consider R. Note that there exists a preRIF of R which satisfies (RIF₁) and (RIF₂).

6. On the Connections between Postulates

Now we state the proposition:

(20) Let us consider preRIF κ of R satisfying (RIF₁). Then κ satisfies (RIF₂) if and only if κ satisfies (RIF₂).

Let us consider R. Let us observe that every preRIF of R satisfying (RIF₁) which satisfies (RIF₂) satisfies also (RIF₂) and every preRIF of R satisfying (RIF₁) which satisfies (RIF₂) satisfies also (RIF₂) and $\kappa^{\pounds}(R)$ satisfies (RIF₀) and (RIF₂) and there exists a pre-rough inclusion function of R which satisfies (RIF₀), (RIF₁), (RIF₂), and (RIF₂^{*}).

A rough inclusion function of R is pre-rough inclusion function of R satisfying (RIF₁) and (RIF₂).

A quasi-rough inclusion function of R is preRIF of R satisfying (RIF₀) and (RIF₂^{*}).

A weak quasi-rough inclusion function of R is preRIF of R satisfying (RIF₀) and (RIF₂).

A RIF of R is a rough inclusion function of R.

A q-RIF of R is a quasi-rough inclusion function of R.

A weak q-RIF of R is a weak quasi-rough inclusion function of R.

7. Formalization of Proposition 2 [4]

Now we state the propositions:

(21) If $X \neq \emptyset$ and $Z \cup W = \Omega_R$ and Z misses W, then $\kappa^{\pounds}(X, Z) + \kappa^{\pounds}(X, W) = 1$.

- (22) If $\kappa^{\pounds}(X, Y) = 0$, then X misses Y.
- (23) If $X \neq \emptyset$, then $\kappa^{\pounds}(X, Y) = 0$ iff X misses Y. The theorem is a consequence of (22).
- (24) If $X \neq \emptyset$, then $\kappa^{\pounds}(X, \emptyset_R) = 0$.

Now we state the propositions:

- (25) If $X \neq \emptyset$ and X misses Y, then $\kappa^{\pounds}(X, Z \setminus Y) = \kappa^{\pounds}(X, Z \cup Y) = \kappa^{\pounds}(X, Z)$. The theorem is a consequence of (23), (10), (7), and (9).
- (26) If Z misses W, then $\kappa^{\pounds}(Y \cup Z, W) \leq \kappa^{\pounds}(Y, W) \leq \kappa^{\pounds}(Y \setminus Z, W)$.
- (27) If Z misses Y and $Z \subseteq W$, then $\kappa^{\pounds}(Y \setminus Z, W) \leqslant \kappa^{\pounds}(Y, W) \leqslant \kappa^{\pounds}(Y \cup Z, W)$.

8. Formalization of Proposition 4 [4]

Let us consider R. Let X be a non empty subset of R. Let us note that $\kappa^{\pounds}(X, \emptyset_R)$ is empty.

Now we state the propositions:

- (28) If $\kappa_1(X, Y) = 0$, then X misses Y. The theorem is a consequence of (14).
- (29) If $\kappa_2(X, Y) = 0$, then X misses Y. The theorem is a consequence of (15).
- Let us consider R. Observe that $\kappa^{\pounds}(R)$ satisfies (RIF₄) and $\kappa_1(R)$ satisfies (RIF₄) and $\kappa_2(R)$ satisfies (RIF₄).
- (30) $\kappa^{\pounds}(X,Y) \leq \kappa_1(X,Y) \leq \kappa_2(X,Y)$. The theorem is a consequence of (1), (18), and (19).
- (31) $\kappa_1(X,Y) = \kappa^{\pounds}(X \cup Y,Y)$. The theorem is a consequence of (6) and (11).
- (32) $\kappa_2(X,Y) = \kappa^{\pounds}(\Omega_R, X^c \cup Y) = \kappa^{\pounds}(\Omega_R, X^c) + \kappa^{\pounds}(\Omega_R, X \cap Y).$
- (33) $\kappa^{\pounds}(X,Y) = \kappa^{\pounds}(X,X\cap Y) = \kappa_1(X,X\cap Y) = \kappa_1(X\setminus Y,X\cap Y).$
- (34) If $X \cup Y = \Omega_R$, then $\kappa_1(X, Y) = \kappa_2(X, Y)$. The theorem is a consequence of (2).
- (35) If $X \neq \emptyset$, then $1 \kappa^{\pounds}(X, Y) = \kappa^{\pounds}(X, Y^{c})$. The theorem is a consequence of (10) and (6).

9. Concrete Example

Let X be a set. The functor DiscreteApproxSpace(X) yielding a strict relational structure is defined by the term

(Def. 14) $\langle X, \operatorname{id}_X \rangle$.

Let us note that DiscreteApproxSpace(X) has equivalence relation.

Let X be a non empty set. Observe that DiscreteApproxSpace(X) is non empty.

Let X be a finite set. Let us observe that DiscreteApproxSpace(X) is finite.

The functor ExampleRIFSpace yielding a strict, finite approximation space is defined by the term (Def. 15) $DiscreteApproxSpace(\{1, 2, 3, 4, 5\}).$

Now we state the propositions:

- (36) Let us consider subsets X, Y of ExampleRIFSpace. Suppose $X = \{1, 2\}$ and $Y = \{2, 3, 4\}$. Then $\kappa^{\pounds}(X, Y) \neq \kappa^{\pounds}(Y, X)$.
- (37) Let us consider subsets X, Y, U of ExampleRIFSpace. Suppose $X = \{1, 2\}$ and $Y = \{1, 2, 3\}$ and $U = \{2, 4, 5\}$. Then $\kappa^{\pounds}(X, U) \not\leq \kappa^{\pounds}(Y, U)$.
- (38) Let us consider subsets X, Y of ExampleRIFSpace. Suppose $X = \{1, 2\}$ and $Y = \{2, 3, 4\}$. Then $\kappa^{\pounds}(X, Y)$, $\kappa_1(X, Y)$, $\kappa_2(X, Y)$ are mutually different.

10. Continuing Formalization of Theorem 4.1 [2]

Let us consider a finite approximation space R, an element u of R, and subsets x, y of R. Now we state the propositions:

- (39) If $u \in (f_1(R))(x)$ and $(I_R)(u) = y$, then $\kappa^{\pounds}(y, x) > 0$. The theorem is a consequence of (22).
- (40) If $u \in (\text{Flip } f_1(R))(x)$ and $(I_R)(u) = y$, then $\kappa^{\pounds}(y, x) = 1$. The theorem is a consequence of (6).

References

- Maria Paola Bonacina and Mark E. Stickel, editors. Automated Reasoning and Mathematics – Essays in Memory of William W. McCune, volume 7788 of Lecture Notes in Computer Science, 2013. Springer.
- [2] Anna Gomolińska. A comparative study of some generalized rough approximations. Fundamenta Informaticae, 51:103–119, 2002.
- [3] Anna Gomolińska. Rough approximation based on weak q-RIFs. In James F. Peters, Andrzej Skowron, Marcin Wolski, Mihir K. Chakraborty, and Wei-Zhi Wu, editors, Transactions on Rough Sets X, volume 5656 of Lecture Notes in Computer Science, pages 117–135, Berlin, Heidelberg, 2009. Springer. ISBN 978-3-642-03281-3. doi:10.1007/978-3-642-03281-3_4.
- [4] Anna Gomolińska. On three closely related rough inclusion functions. In Marzena Kryszkiewicz, James F. Peters, Henryk Rybiński, and Andrzej Skowron, editors, *Rough Sets and Intelligent Systems Paradigms*, volume 4585 of *Lecture Notes in Computer Science*, pages 142–151, Berlin, Heidelberg, 2007. Springer. doi:10.1007/978-3-540-73451-2_16.
- [5] Anna Gomolińska. On certain rough inclusion functions. In James F. Peters, Andrzej Skowron, and Henryk Rybiński, editors, *Transactions on Rough Sets IX*, volume 5390 of *Lecture Notes in Computer Science*, pages 35–55. Springer Berlin Heidelberg, 2008. doi:10.1007/978-3-540-89876-4_3.
- [6] Adam Grabowski. On the computer-assisted reasoning about rough sets. In B. Dunin-Kęplicz, A. Jankowski, A. Skowron, and M. Szczuka, editors, *International Workshop on Monitoring, Security, and Rescue Techniques in Multiagent Systems Location*, volume 28 of Advances in Soft Computing, pages 215–226, Berlin, Heidelberg, 2005. Springer-Verlag. doi:10.1007/3-540-32370-8_15.
- [7] Adam Grabowski. Efficient rough set theory merging. Fundamenta Informaticae, 135(4): 371–385, 2014. doi:10.3233/FI-2014-1129.

- [8] Adam Grabowski. Building a framework of rough inclusion functions by means of computerized proof assistant. In Tamás Mihálydeák, Fan Min, Guoyin Wang, Mohua Banerjee, Ivo Düntsch, Zbigniew Suraj, and Davide Ciucci, editors, *Rough Sets*, volume 11499 of *Lecture Notes in Computer Science*, pages 225–238, Cham, 2019. Springer International Publishing. ISBN 978-3-030-22815-6. doi:10.1007/978-3-030-22815-6_18.
- [9] Adam Grabowski. Lattice theory for rough sets a case study with Mizar. Fundamenta Informaticae, 147(2–3):223–240, 2016. doi:10.3233/FI-2016-1406.
- [10] Adam Grabowski. Relational formal characterization of rough sets. Formalized Mathematics, 21(1):55–64, 2013. doi:10.2478/forma-2013-0006.
- [11] Adam Grabowski. Binary relations-based rough sets an automated approach. Formalized Mathematics, 24(2):143–155, 2016. doi:10.1515/forma-2016-0011.
- [12] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics*, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5-10, 2010. Proceedings, volume 6167 of Lecture Notes in Computer Science, pages 300-314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.
- [13] Adam Grabowski and Michał Sielwiesiuk. Formalizing two generalized approximation operators. *Formalized Mathematics*, 26(2):183–191, 2018. doi:10.2478/forma-2018-0016.
- [14] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. Journal of Automated Reasoning, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.
- [15] Jan Łukasiewicz. Die logischen Grundlagen der Wahrscheinlichkeitsrechnung. In L. Borkowski, editor, Jan Lukasiewicz – Selected Works, pages 16–63. North Holland, Polish Scientific Publ., Amsterdam London Warsaw, 1970. First published in Kraków, 1913.
- Zdzisław Pawlak. Rough sets. International Journal of Parallel Programming, 11:341–356, 1982. doi:10.1007/BF01001956.
- [17] Lech Polkowski. Rough mereology. In Approximate Reasoning by Parts, volume 20 of Intelligent Systems Reference Library, pages 229–257, Berlin, Heidelberg, 2011. Springer. ISBN 978-3-642-22279-5. doi:10.1007/978-3-642-22279-5_6.
- [18] Lech Polkowski and Andrzej Skowron. Rough mereology: A new paradigm for approximate reasoning. International Journal of Approximate Reasoning, 15(4):333–365, 1996. doi:10.1016/S0888-613X(96)00072-2.
- [19] Andrzej Skowron and Jarosław Stepaniuk. Tolerance approximation spaces. Fundamenta Informaticae, 27(2/3):245–253, 1996. doi:10.3233/FI-1996-272311.
- [20] William Zhu. Generalized rough sets based on relations. *Information Sciences*, 177: 4997–5011, 2007.

Accepted August 29, 2019