

Types of Algebraic Structures in Proof Assistant Systems

Akshobhya Katte Madhusudana
Under the supervision of Dr. Jacques Carette

McMaster University

June 8th, 2023

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra
- 7 Conclusion

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra
- 7 Conclusion

- 1 A theory in universal algebra is defined as a tuple (S, F, E) such that, S is a set of single sort s , F is a finite set of function symbols with their arities, and E is a set of equations that are satisfied in S .
- 2 A signature of a theory (S, F, E) is a pair (S, F) such that S is set of sorts and F is set of operation names. An operation can be defined as a triple $(f, [s_1, \dots, s_n], s)$ consisting of name, its arity, and the target sort.
- 3 An algebra A is defined as $A = (S_A, F_A)$ a mathematical structure consisting of a domain and functions on the domain. Algebra provides an interpretation for the carrier set S and function symbols F of a theory.

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra
- 7 Conclusion

Algebraic structures in proof systems

- 1 Survey on standard libraries of four proof assistant systems Agda, Lean, Idris, and Coq.
- 2 Create a web crawler to capture definitions of algebraic structures.
- 3 Create a clickable table that takes to definition in source library.

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup**
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra
- 7 Conclusion

Theory of Quasigroup

Quasigroup division operation

$$y = x \cdot (x \backslash y)$$

$$y = x \backslash (x \cdot y)$$

$$y = (y / x) \cdot x$$

$$y = (y \cdot x) / x$$

Loop is a quasigroup with identity:

$$x \cdot e = e \cdot x = x$$

```
record IsQuasigroup (· \\ // : Op₂ A) : Set
  ⇐ (a ⊔ ℓ) where
    field
      isMagma      : IsMagma ·
      \\-cong      : Congruent₂ \\
      //-cong      : Congruent₂ //
      leftDivides  : LeftDivides · \\
      rightDivides : RightDivides · //
  open IsMagma isMagma public
```


Types of Quasigroup

A loop is called a *right bol loop* if it satisfies the identity

$$((z \cdot x) \cdot y) \cdot x = z \cdot ((x \cdot y) \cdot x)$$

A loop is called a *left bol loop* if it satisfies the identity

$$x \cdot (y \cdot (x \cdot z)) = (x \cdot (y \cdot x)) \cdot z$$

A loop is called a *middle bol loop* if it satisfies the identity

$$(z \cdot x) \cdot (y \cdot z) = z \cdot ((x \cdot y) \cdot z)$$

A left-right bol loop is called a *moufang loop* if it satisfies identity

$$(z \cdot x) \cdot (y \cdot z) = z \cdot ((x \cdot y) \cdot z)$$

Quasigroup homomorphism

A Quasigroup homomorphism $f : (Q_1, \cdot, \backslash, //) \rightarrow (Q_2, \circ, \backslash, /)$

- f preserves the binary operation: $f(x \cdot y) = f(x) \circ f(y)$
- f preserves the left division operation : $f(x \backslash y) = f(x) \backslash f(y)$
- f preserves the right division operation: $f(x // y) = f(x) / f(y)$

```
record IsQuasigroupHomomorphism ( _ : A → B ) : Set (a ⊔ ℓ1 ⊔ ℓ2) where
  field
    isRelHomomorphism : IsRelHomomorphism _≈1_ _≈2_ _
    ·-homo              : Homomorphic2 _·1_ _·2_
    \-homo              : Homomorphic2 _\ 1_ _\ 2_
    //-homo              : Homomorphic2 _//1_ _//2_

open IsRelHomomorphism isRelHomomorphism public
renaming (cong to -cong)
```

Properties of Quasigroup

Properties of Quasigroup

- 1 Q is cancellative.
- 2 If $x \cdot y = z$ then $y = x \backslash z$
- 3 If $x \cdot y = z$ then $x = z / y$

Properties of Loop

- 1 $x / x = e$
- 2 $x \backslash x = e$
- 3 $e \backslash x = x$
- 4 $x / e = x$

```
cancel1 : LeftCancellative _ =>
cancel1 x y z eq = begin
  y                ≈⟨ sym( leftDividesr x y) ⟩
  x \ (x · y) ≈⟨ \-cong1 eq ⟩
  x \ (x · z) ≈⟨ leftDividesr x z ⟩
  z                ■
```

Properties of types of loop

Properties of middle bol loop

- ① $x \cdot ((y \cdot x) \setminus x) = y \setminus x$
- ② $x \cdot ((x \cdot z) \setminus x) = x / z$
- ③ $x \cdot (z \setminus x) = (x / z) \cdot x$
- ④ $(x / (y \cdot z)) \cdot x = (x / z) \cdot (y \setminus x)$
- ⑤ $(x / (y \cdot x)) \cdot x = y \setminus x$
- ⑥ $(x / (x \cdot z)) \cdot x = x / z$

Properties of Moufang loop:

- ① Moufang loop is alternative.
- ② Moufang loop is flexible.
- ③ $z \cdot (x \cdot (z \cdot y)) = ((z \cdot x) \cdot z) \cdot y$
- ④ $x \cdot (z \cdot (y \cdot z)) = ((x \cdot z) \cdot y) \cdot z$
- ⑤ $z \cdot ((x \cdot y) \cdot z) = (z \cdot (x \cdot y)) \cdot z$

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring**
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra
- 7 Conclusion

Semigroup

A Semigroup is a magma with associativity:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

```
record IsSemigroup (· : Op2 A) : Set (a ⊔ ℓ) where
  field
    isMagma : IsMagma ·
    assoc    : Associative ·

open IsMagma isMagma public
```

A commutative semigroup is a semigroup with commutativity:

$$x \cdot y = y \cdot x$$

Ring $(R, +, *, ^{-1}, 0, 1)$

- $(R, +, ^{-1}, 0)$ is an Abelian Group:
 - Associativity: $\forall x, y, z \in R, x + (y + z) = (x + y) + z$
 - commutativity : $\forall x, y \in R, (x + y) = (y + x)$
 - Identity: $\forall x \in R, (x + 0) = x = (0 + x)$
 - Inverse: $\forall x \in R, (x + x^{-1}) = 0 = (x^{-1} + x)$
- $(R, *, 1)$ is a monoid
 - Associativity: $\forall x, y, z \in R, x * (y * z) = (x * y) * z$
 - Identity: $\forall x, y \in R, (x * 1) = x = (1 * x)$
- Multiplication distributes over addition:
 $\forall x, y, z \in R, (x * (y + z)) = (x * y) + (x * z)$ and
 $(x + y) * z = (x * z) + (y * z)$
- Annihilating zero: $\forall x \in R, (x * 0) = 0 = (0 * x)$

Properties of types of loop

Properties of Semigroup:

- 1 Semigroup is alternative.
- 2 Semigroup is flexible.
- 3 $(x \cdot y) \cdot (x \cdot x) = x \cdot (y \cdot (x \cdot x))$.

Properties of commutative Semigroup:

- 1 Semimedial
- 2 Middle Semimedial

Properties of ring without one structure:

- 1 $-(x * y) = -x * y$
- 2 $-(x * y) = x * -y$

Properties of Ring:

- 1 $-1 * x = -x$
- 2 if $x + x = 0$ then $x = 0$
- 3 $x * (y - z) = x * y - x * z$
- 4 $(y - z) * x = (y * x) - (z * x)$

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra**
- 6 Problem in programming algebra
- 7 Conclusion

Idempotent semiring

An idempotent semiring $(S, +, *, 0, 1)$:

- $(S, +, 0)$ is a commutative monoid:
 - Associativity: $\forall x, y, z \in S, x + (y + z) = (x + y) + z$
 - Identity: $\forall x \in S, (x + 0) = x = (0 + x)$
 - Commutativity: $\forall x, y \in S, (x + y) = (y + x)$
- $(S, *, 1)$ is a monoid:
 - Associativity: $\forall x, y, z \in S, x * (y * z) = (x * y) * z$
 - Identity: $\forall x \in S, (x * 1) = x = (1 * x)$
- Idempotent: $\forall x \in S, (x + x) = x$
- Multiplication distributes over addition:
 $\forall x, y, z \in S, (x * (y + z)) = (x * y) + (x * z)$ and
 $(x + y) * z = (x * z) + (y * z)$
- Annihilating zero: $\forall x \in S, (x * 0) = 0 = (0 * x)$

Kleene Algebra

A Kleene algebra is an idempotent semiring with unary $*$ operator that satisfies:

$$1 + (x \cdot (x^*)) \leq x^*$$

$$1 + (x^*) \cdot x \leq x^*$$

$$\text{If } b + a \cdot x \leq x \text{ then, } (a^*) \cdot b \leq x$$

$$\text{If } b + x \cdot a \leq x \text{ then, } b \cdot (a^*) \leq x$$

```
record IsKleeneAlgebra (+ * : Op2 A) (★ : Op1 A) (0# 1# : A) : Set (a ⊔  
→ ℓ) where  
  field  
    isIdempotentSemiring : IsIdempotentSemiring + * 0# 1#  
    starExpansive         : StarExpansive 1# + * ★  
    starDestructive       : StarDestructive + * ★  
  
open IsIdempotentSemiring isIdempotentSemiring public
```

Properties of Kleene Algebra

- ① $1 + x^* = x^*$
- ② $x * x^* + x^* = x^*$
- ③ $x^* + x^* * x = x^*$
- ④ $0 + x + x^* = x^*$
- ⑤ $1 + x + x^* = x^*$
- ⑥ $x + x^* = x^*$
- ⑦ $x^* * x^* + x^* = x^*$
- ⑧ $1 + x^* * x^* + x^* = x^*$
- ⑨ If $a * x = x * b$ then, $a^* * x + x * b^* = x * b^*$
- ⑩ If $x = y$ then, $1 + x * y^* + y^* = y^*$
- ⑪ $(x * y)^* * x + x * (y * x)^* = x * (y * x)^*$

Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra**
- 7 Conclusion

Ambiguity and Equivalent

- ① Ambiguity in naming e.g. Ring and Rng, Nearing (*-semigroup/*-monoid).
- ② Equivalent but structurally different e.g. Quasigroups

A quasigroup with Latin square property is a type (2) algebra.

$$a \cdot x = b$$

$$y \cdot a = b$$

A quasigroup with division operation is a type (2,2,2) algebra

$$y = x \cdot (x \setminus y)$$

$$y = x \setminus (x \cdot y)$$

$$y = (y / x) \cdot x$$

$$y = (y \cdot x) / x$$

Redundant field

Duplicate field in structural inheritance: e.g. semiring
($+$ -commutativeMonoid and $*$ -monoid)

```
record IsSemiringWithoutOne (+ * : Op2 A) (0# : A) : Set (a  $\sqcup$   $\ell$ ) where
field
  +-isCommutativeMonoid : IsCommutativeMonoid + 0#
  *-cong                 : Congruent2 *
  *-assoc                 : Associative *
  distrib                 : * DistributesOver +
  zero                   : Zero 0# *

open IsCommutativeMonoid +-isCommutativeMonoid public
```

Equivalent and Identical

- 1 Equivalent structures e.g. Bounded semilattice and Idempotent commutative monoid
- 2 Identical structures e.g. Nearing ($+$ -group, $*$ -monoid)

```
record IsNearing (+ * : Op2 A) (0# 1# : A) (_-1 : Op1 A) : Set (a ⊔ ℓ)
↪ where
  field
    isQuasiring : IsQuasiring + * 0# 1#
    +-inverse    : Inverse 0# _-1 +
    -1-cong      : Congruent1 _-1

open IsQuasiring isQuasiring public

+-isGroup : IsGroup + 0# _-1
+-isGroup = record
{ isMonoid = +-isMonoid
; inverse = +-inverse
; -1-cong = -1-cong
}
```


Table of Contents

- 1 Universal Algebra
- 2 Algebraic structures in proof systems
- 3 Theory of Quasigroup
- 4 Theory of Semigroup and Ring
- 5 Theory of Kleene Algebra
- 6 Problem in programming algebra
- 7 Conclusion**

Conclusion

To sum up, we...

- 1 Set the scope by doing a survey
- 2 Study select subset of types of algebraic structures in Agda
- 3 Analyze five problems that we encountered.