A Brief Glossary of Algebraic Structures

Prof. Hubert Kaeslin
Microelectronics Design Center
ETH Zürich

Background material for
Digital Integrated Circuit Design,
from VLSI Architectures to CMOS Fabrication
ISBN 978-0-521-88267-5, www.cambridge.org/kaeslin

last update: December 20, 2011

Book chapter 4, appendix I, pp130...133

Why this glossary?

Many mathematical texts on abstract algebra explain algebraic structures recursively, e.g.

> *A ring [with unity] is a set R with two binary operations, usually called addition (+) and multiplication (·), such that R is an Abelian group under addition, a monoid under multiplication, and such that multiplication is both left- and right-distributive over addition.*

For newcomers to the field such "explanations" just replace one unknown term by several others. So let us break away from that tradition here and present the facts and connections in the most straightforward manner.

Introduction

Almost all calculations from everyday life are carried out in the

- field of reals $(\mathbb{R}, +, \cdot)$ (Körper der reelen Zahlen)

Introduction

Almost all calculations from everyday life are carried out in the
◦ field of reals $(\mathbb{R}, +, \cdot)$ (Körper der reelen Zahlen)
Most engineering students are also familiar with
◦ matrix calculus $(M_{n \times n}, +, \cdot)$ (Matrizenrechnung)
◦ switching algebra $(\{0,1\}, \vee, \wedge)$ (Schaltalgebra)

Introduction

Almost all calculations from everyday life are carried out in the
◦ field of reals $(\mathbb{R}, +, \cdot)$ (Körper der reelen Zahlen)
Most engineering students are also familiar with
◦ matrix calculus $(M_{nxn}, +, \cdot)$ (Matrizenrechnung)
◦ switching algebra $(\{0,1\}, \vee, \wedge)$ (Schaltalgebra)

Many more "algebras" exist.

An algebraic structure is defined by

- a set of elements S
- one or more operations (denoted $\boxplus$, $\boxdot$, ...)

Introduction

Almost all calculations from everyday life are carried out in the
∘ field of reals $(\mathbb{R}, +, \cdot)$ (Körper der reelen Zahlen)
Most engineering students are also familiar with
∘ matrix calculus $(M_{nxn}, +, \cdot)$ (Matrizenrechnung)
∘ switching algebra $(\{0,1\}, \vee, \wedge)$ (Schaltalgebra)

Many more “algebras” exist.

An algebraic structure is defined by

- a set of elements S
- one or more operations (denoted $\boxplus$, $\boxdot$, ...)

- The nature of the operations involved determines which axioms are satisfied and which are not.
- Each algebraic structure so defined is given a name as a function of the axioms found to hold.

Axioms I

Consider a set of elements S and a first binary operation $\boxplus$ (zweistellig)

1. Closure wrt $\boxplus$:
   if a and b are in S then $a \boxplus b$ is also in S.
2. Associative law wrt $\boxplus$:
   $(a \boxplus b) \boxplus c = a \boxplus (b \boxplus c)$.
3. Identity element wrt $\boxplus$ ("zero"): (Neutralelement der Addition)
   There is a unique element e such that
   $a \boxplus e = e \boxplus a = a$ for any a.
4. Inverse element wrt $\boxplus$:
   For every a in S there is an inverse $-a$ such that
   $a \boxplus -a = -a \boxplus a = e$.
5. Commutative law wrt $\boxplus$:
   $a \boxplus b = b \boxplus a$.

Axioms II

Consider a second binary operation $\boxdot$ that takes precedence over $\boxplus$

6. Closure wrt $\boxdot$:
   if a and b are in S then $a \boxdot b$ is also in S.
7. Associative law wrt $\boxdot$:
   $(a \boxdot b) \boxdot c = a \boxdot (b \boxdot c)$.
8. Identity element wrt $\boxdot$ ("unity"): (Neutralelement der Multiplikation)
   There is a unique element i such that
   $a \boxdot i = i \boxdot a = a$ for any a.
9. Inverse element wrt $\boxdot$:
   For every a in S there is an inverse a^{-1} such that
   $a \boxdot a^{-1} = a^{-1} \boxdot a = i$, the only exception is e for which no inverse exists.
10. Commutative law wrt $\boxdot$:
    $a \boxdot b = b \boxdot a$.

Axioms III

... continued

11. Distributive law of $\boxdot$ over $\boxplus$:
    $a \boxdot (b \boxplus c) = a \boxdot b \boxplus a \boxdot c$ and
    $(a \boxplus b) \boxdot c = a \boxdot c \boxplus b \boxdot c$.
12. Distributive law of $\boxplus$ over $\boxdot$:
    $a \boxplus b \boxdot c = (a \boxplus b) \boxdot (a \boxplus c)$ and
    $a \boxdot b \boxplus c = (a \boxplus c) \boxdot (b \boxplus c)$.
13. Complement:
    For every a in S there is a complement $\overline{a}$ such that
    $a \boxplus \overline{a} = i$ and
    $a \boxdot \overline{a} = e$.

Algebraic structures at a glance

Name of algebraic structure	Operations	Axioms satisfied												
		1	2	3	4	5	6	7	8	9	10	11	12	13
Set (Menge)														
Semigroup (Halbgruppe)	$\boxplus$	1	2											
Monoid	$\boxplus$	1	2	3										
Group (Gruppe)	$\boxplus$	1	2	3	4									
Abelian or commutative group	$\boxplus$	1	2	3	4	5								
Abelian semigroup	$\boxplus$	1	2			5								
Abelian monoid	$\boxplus$	1	2	3		5								
Ring	$\boxplus\boxdot$	1	2	3	4	5	6	7				11		
Ring with unity	$\boxplus\boxdot$	1	2	3	4	5	6	7	8			11		
Division ring aka skew field	$\boxplus\boxdot$	1	2	3	4	5	6	7	8	9		11		
Field (Körper)	$\boxplus\boxdot$	1	2	3	4	5	6	7	8	9	10	11		
Commutative ring	$\boxplus\boxdot$	1	2	3	4	5	6	7			10	11		
Commutative ring with unity	$\boxplus\boxdot$	1	2	3	4	5	6	7	8		10	11		
Semiring (Halbring)	$\boxplus\boxdot$	1	2			5	6	7				11		
Commutative semiring	$\boxplus\boxdot$	1	2			5	6	7			10	11		
Boolean algebra	$\boxplus\boxdot$	1	2	3		5	6	7	8		10	11	12	13

Examples of algebraic structures with one operation

- The set S_{DNA} of all possible DNA sequences of non-zero length with characters from {A,T,C,G} together with the binary operation of string concatenation $\smile$ forms an infinite semigroup $(S_{DNA}, \smile)$.

Examples of algebraic structures with one operation

- The set S_{DNA} of all possible DNA sequences of non-zero length with characters from {A,T,C,G} together with the binary operation of string concatenation $\smile$ forms an infinite semigroup $(S_{DNA}, \smile)$.
- All permutations of a given number of elements form a group when combined with binary composition of such permutations as sole operation.

  As an example, consider all six distinct rearrangements of three elements:

  $$\begin{array}{ccc} 1. & 2. & 3. \\ \downarrow & \downarrow & \downarrow \\ 1. & 2. & 3. \end{array} \quad \begin{array}{ccc} 1. & 2. & 3. \\ \downarrow & \downarrow & \downarrow \\ 2. & 3. & 1. \end{array} \quad \begin{array}{ccc} 1. & 2. & 3. \\ \downarrow & \downarrow & \downarrow \\ 3. & 1. & 2. \end{array} \quad \begin{array}{ccc} 1. & 2. & 3. \\ \downarrow & \downarrow & \downarrow \\ 3. & 2. & 1. \end{array} \quad \begin{array}{ccc} 1. & 2. & 3. \\ \downarrow & \downarrow & \downarrow \\ 1. & 3. & 2. \end{array} \quad \begin{array}{ccc} 1. & 2. & 3. \\ \downarrow & \downarrow & \downarrow \\ 2. & 1. & 3. \end{array}$$

  With S_3 denoting this set of permutations and $\circ$ binary composition, $(S_3, \circ)$ is a finite group.

Examples of algebraic structures with one operation

- The set S_{DNA} of all possible DNA sequences of non-zero length with characters from {A,T,C,G} together with the binary operation of string concatenation $\smile$ forms an infinite semigroup $(S_{DNA}, \smile)$.
- All permutations of a given number of elements form a group when combined with binary composition of such permutations as sole operation.

  As an example, consider all six distinct rearrangements of three elements:

1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1.	2.	3.	2.	3.	1.	3.	1.	2.	3.	2.	1.	1.	3.	2.	2.	1.	3.

  With S_3 denoting this set of permutations and $\circ$ binary composition, $(S_3, \circ)$ is a finite group.
- The set of all positive integers $\mathbb{N}^+ = \{1, 2, 3, ...\}$ together with addition constitutes an infinite Abelian semigroup $(\mathbb{N}^+, +)$.

Examples of algebraic structures with one operation

- The set S_{DNA} of all possible DNA sequences of non-zero length with characters from {A,T,C,G} together with the binary operation of string concatenation $\smile$ forms an infinite semigroup $(S_{DNA}, \smile)$.
- All permutations of a given number of elements form a group when combined with binary composition of such permutations as sole operation.

  As an example, consider all six distinct rearrangements of three elements:

1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1.	2.	3.	2.	3.	1.	3.	1.	2.	3.	2.	1.	1.	3.	2.	2.	1.	3.

  With S_3 denoting this set of permutations and $\circ$ binary composition, $(S_3, \circ)$ is a finite group.
- The set of all positive integers $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ together with addition constitutes an infinite Abelian semigroup $(\mathbb{N}^+, +)$.
- When supplemented with 0, the above structure turns into an Abelian monoid $(\mathbb{N}, +)$.

Examples of algebraic structures with one operation

- The set S_{DNA} of all possible DNA sequences of non-zero length with characters from $\{$A,T,C,G$\}$ together with the binary operation of string concatenation $\smile$ forms an infinite semigroup $(S_{DNA}, \smile)$.
- All permutations of a given number of elements form a group when combined with binary composition of such permutations as sole operation.

  As an example, consider all six distinct rearrangements of three elements:

1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1.	2.	3.	2.	3.	1.	3.	1.	2.	3.	2.	1.	1.	3.	2.	2.	1.	3.

  With S_3 denoting this set of permutations and $\circ$ binary composition, $(S_3, \circ)$ is a finite group.
- The set of all positive integers $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ together with addition constitutes an infinite Abelian semigroup $(\mathbb{N}^+, +)$.
- When supplemented with 0, the above structure turns into an Abelian monoid $(\mathbb{N}, +)$.
- $(\mathbb{Z}, +)$ is an infinite Abelian group.

Examples of algebraic structures with two operations I

- A commutative ring with unity $(\mathbb{Z}, +, \cdot)$ results when multiplication is added as a second operation to the Abelian group $(\mathbb{Z}, +)$.

Examples of algebraic structures with two operations I

- A commutative ring with unity $(\mathbb{Z}, +, \cdot)$ results when multiplication is added as a second operation to the Abelian group $(\mathbb{Z}, +)$.
- The set of all reals $\mathbb{R}$ together with addition as a first and multiplication as a second operation forms the field $(\mathbb{R}, +, \cdot)$.

Examples of algebraic structures with two operations I

- A commutative ring with unity $(\mathbb{Z}, +, \cdot)$ results when multiplication is added as a second operation to the Abelian group $(\mathbb{Z}, +)$.
- The set of all reals $\mathbb{R}$ together with addition as a first and multiplication as a second operation forms the field $(\mathbb{R}, +, \cdot)$.

  $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are other infinite fields.

Examples of algebraic structures with two operations I

- A commutative ring with unity $(\mathbb{Z}, +, \cdot)$ results when multiplication is added as a second operation to the Abelian group $(\mathbb{Z}, +)$.
- The set of all reals $\mathbb{R}$ together with addition as a first and multiplication as a second operation forms the field $(\mathbb{R}, +, \cdot)$.

  $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are other infinite fields.

  The set of all quotients of two polynomials $P(x)$ and $Q(x)$ with real-valued coefficients together with addition and multiplication makes up for yet another infinite field $(\frac{P(x)}{Q(x)}, +, \cdot)$.

Examples of algebraic structures with two operations I

- A commutative ring with unity $(\mathbb{Z}, +, \cdot)$ results when multiplication is added as a second operation to the Abelian group $(\mathbb{Z}, +)$.
- The set of all reals $\mathbb{R}$ together with addition as a first and multiplication as a second operation forms the field $(\mathbb{R}, +, \cdot)$.

  $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are other infinite fields.

  The set of all quotients of two polynomials $P(x)$ and $Q(x)$ with real-valued coefficients together with addition and multiplication makes up for yet another infinite field $(\frac{P(x)}{Q(x)}, +, \cdot)$.
- All square matrices $M_{n \times n}$ with coefficients taken from a field together with matrix addition and matrix multiplication form an infinite ring with unity.

Examples of algebraic structures with two operations II

- Any subset of integers $S = \{0, 1, ..., p-1\}$ forms a field together with addition modulo p and multiplication modulo p iff p is a prime number. Any such finite field is called a Galois field GF(p).

  GF(5) ($\{0,1,2,3,4\}$, $+ \bmod 5$, $\cdot \bmod 5$) is the Galois field for $p = 5$. Addition and multiplication tables are as follows

$\boxplus = + \bmod 5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\boxdot = \cdot \bmod 5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

  The best-known finite field is the GF(2) ($\{0,1\}$, $\oplus$, $\wedge$).

Examples of algebraic structures with two operations II

- Any subset of integers $S = \{0, 1, ..., p-1\}$ forms a field together with addition modulo p and multiplication modulo p iff p is a prime number. Any such finite field is called a Galois field GF(p).

  GF(5) ($\{0,1,2,3,4\}$, $+ \bmod 5$, $\cdot \bmod 5$) is the Galois field for $p = 5$. Addition and multiplication tables are as follows

$\boxplus = + \bmod 5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\boxdot = \cdot \bmod 5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

  The best-known finite field is the GF(2) ($\{0,1\}$, $\oplus$, $\wedge$).

- As opposed to this, ($\{0,1,...,m-1\}$, $+ \bmod m$, $\cdot \bmod m$) where m is not prime merely forms a finite commutative ring with unity as 0 is not the only element that lacks a multiplicative inverse. In the occurrence of ($\{0,1,2,3,4,5,6,7,8\}$, $+ \bmod 9$, $\cdot \bmod 9$), this also applies to 3 and 6.

Examples of algebraic structures with two operations III

- Cardinalities of finite fields are not confined to prime numbers. A so-called extension field $GF(p^n)$ can be defined for any power p^n provided $2 \leq n \in \mathbb{N}^+$.

  All polynomials $P(x)$ of degree $0, 1, ..., n-1$ with coefficients from $GF(p)$ constitute the set of elements. The first operation is addition modulo $M(x)$ and the second one multiplication modulo $M(x)$ where $M(x)$ is an irreducible[1] polynomial of degree n with coefficients from $GF(p)$.

  $GF(3^2)$, for instance, consists of the nine elements
  $0, \quad 1, \quad 2, \quad x, \quad x+1, \quad x+2, \quad 2x, \quad 2x+1, \quad 2x+2,$
  the operations are $+ \bmod (x^2+1)$ and $\cdot \bmod (x^2+1)$
  with $M(x) = x^2 + 1$ being an irreducible polynomial[2].

[2] Cannot be expressed as a product of non-trivial factors of lower degree.

Examples of algebraic structures with two operations IV

- The factors of 30 together with operations least common multiple (lcm) and greatest common divisor (gcd) constitute a Boolean algebra of eight elements ($\{1,2,3,5,6,10,15,30\}$, lcm, gcd). Taking the complement $\overline{a}$ is tantamount to computing $\frac{30}{a}$.

Examples of algebraic structures with two operations IV

- The factors of 30 together with operations least common multiple (lcm) and greatest common divisor (gcd) constitute a Boolean algebra of eight elements ({1,2,3,5,6,10,15,30}, lcm, gcd). Taking the complement $\overline{a}$ is tantamount to computing $\frac{30}{a}$.

  Let $\Omega = \{a,b,c\}$. The set of all sets that can be composed from those elements $\{\, \emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\,\}$ is called power set $\mathfrak{P}(\Omega)$. $(\mathfrak{P}(\Omega), \cup, \cap)$ forms another Boolean algebra where the empty set $\emptyset$ and the universal set Ω act as identity elements e and i respectively. Each element $x \in \mathfrak{P}(\Omega)$ has a complement $\overline{x} = \Omega - x$.

Examples of algebraic structures with two operations IV

- The factors of 30 together with operations least common multiple (lcm) and greatest common divisor (gcd) constitute a Boolean algebra of eight elements ({1,2,3,5,6,10,15,30}, lcm, gcd). Taking the complement $\overline{a}$ is tantamount to computing $\frac{30}{a}$.

  Let $\Omega = \{a,b,c\}$. The set of all sets that can be composed from those elements $\{\, \emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\,\}$ is called power set $\mathfrak{P}(\Omega)$. $(\mathfrak{P}(\Omega), \cup, \cap)$ forms another Boolean algebra where the empty set $\emptyset$ and the universal set Ω act as identity elements e and i respectively. Each element $x \in \mathfrak{P}(\Omega)$ has a complement $\overline{x} = \Omega - x$.

  An infinite Boolean algebra results when $|\Omega| = \infty$,
  e.g. if Ω includes all DNA sequences of arbitrary length.

Examples of algebraic structures with two operations IV

- The factors of 30 together with operations least common multiple (lcm) and greatest common divisor (gcd) constitute a Boolean algebra of eight elements ({1,2,3,5,6,10,15,30}, lcm, gcd). Taking the complement $\overline{a}$ is tantamount to computing $\frac{30}{a}$.

  Let $\Omega = \{a,b,c\}$. The set of all sets that can be composed from those elements $\{\,\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\,\}$ is called power set $\mathfrak{P}(\Omega)$. $(\mathfrak{P}(\Omega), \cup, \cap)$ forms another Boolean algebra where the empty set $\emptyset$ and the universal set Ω act as identity elements e and i respectively. Each element $x \in \mathfrak{P}(\Omega)$ has a complement $\overline{x} = \Omega - x$.

  An infinite Boolean algebra results when $|\Omega| = \infty$, e.g. if Ω includes all DNA sequences of arbitrary length.
- The well-known switching algebra $(\{0,1\}, \vee, \wedge)$ is a Boolean algebra with just two elements. The complement of an element is its logic inverse.

Examples of algebraic structures with two operations V

- The class of semirings is very broad and encompasses:

Constituent	S	$\boxplus$	$\boxdot$
the commutative semiring of natural numbers	$\mathbb{N}$	$+$	$\cdot$
the commutative ring with unity of integers	$\mathbb{Z}$	$+$	$\cdot$
the "ordinary" fields	$\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$	$+$	$\cdot$
all Galois fields, e.g.	$\{0,1\}$	$\oplus$	$\wedge$
all other fields, e.g.	$\frac{P(x)}{Q(x)}$	$+$	$\cdot$
the switching algebra	$\{0,1\}$	$\vee$	$\wedge$
other finite Boolean algebras, e.g.	$\{1,2,3,4,6,12\}$	lcm	gcd
all other Boolean algebras, e.g.	$\mathfrak{P}(\Omega)$	$\cup$	$\cap$
the path algebras, e.g.	$\{0,1\}$	max	min
	$\mathbb{R} \cup \{\infty\}$	min	$+$
	$\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$	max	$\cdot$

Note

Many computational problems can be formulated in a semiring.

Engineering applications

Some of the not-so-common algebraic structures prove extremely helpful for studying real-world phenomena.

- AC circuits (field of complex numbers).
- Digital circuits (switching algebra).
- Error correction coding (Galois fields).
- Cryptography (all sorts of algebraic structures).
- Certain optimization problems (path algebras).
- ...