Semirings for Breakfast

Marc Pouly

marc.pouly@unifr.ch
Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg

July 2010
Semirings

Algebraic structure with two operations $+$ and $\times$ over a set $A$.
- $+$ and $\times$ are associative
- $+$ is commutative
- $\times$ distributes over $+$: $a \times (b + c) = (a \times b) + (a \times c)$

If $\times$ is commutative too $\Rightarrow$ commutative semiring
Examples I

- Arithmetic Semirings: \( \langle \mathbb{R}, +, \cdot \rangle, \langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{N}, +, \cdot \rangle, \ldots \)
- Boolean Semiring: \( \langle \{0, 1\}, \lor, \land \rangle \)
- Tropical Semiring: \( \langle \mathbb{N}, \min, + \rangle \)
- Arctic Semiring: \( \langle \mathbb{N}, \max, + \rangle \)
- Possibilistic Semiring: \( \langle [0, 1], \max, \cdot \rangle \)
- Powerset lattice: \( \langle \mathcal{P}(S), \cup, \cap \rangle \)
- Bottleneck Semiring: \( \langle \mathbb{R}, \max, \min \rangle \)
- Truncation Semiring: \( \langle \{0, \ldots, k\}, \max, \min\{a + b, k\} \rangle \)
- Lukasiewicz Semiring: \( \langle [0, 1], \min, \max\{a + b - 1, 0\} \rangle \)
- Division Semiring: \( \langle \mathbb{N}, \text{lcm}, \text{gcd} \rangle \)
- Formal Languages: \( \langle \mathcal{P}(\Sigma^*), \cup, \circ \rangle \not\rightarrow \text{not commutative} \)
Examples II

- Vectors over semirings form a semiring
- Matrices over semirings form a semiring
- Polynomials over semirings form a semiring
- ...

...
Today’s Breakfast Lessons

2 reasons why computer scientists are interested in semirings:
- they reduce problem complexity
- they enable generic problem solving

2 reasons why mathematicians are interested in semirings:
- ordered semirings are fundamentally different from fields
- new research fields thanks to applications in CS
Today’s Breakfast Lessons

2 reasons why computer scientists are interested in semirings:
- they reduce problem complexity
- they enable generic problem solving

2 reasons why mathematicians are interested in semirings:
- ordered semirings are fundamentally different from fields
- new research fields thanks to applications in CS
Lesson 1:
Reducing Problem Complexity
Bayesian Networks

- **Visit to Asia**
  - $p(a) = 0.01$
  - $p(t|a) = 0.05$
  - $p(t|\bar{a}) = 0.01$

- **Tuberculosis**
  - $p(x|e) = 0.98$
  - $p(x|\bar{e}) = 0.05$

- **Smoking**
  - $p(s) = 0.4$
  - $p(b|s) = 0.6$
  - $p(b|\bar{s}) = 0.3$

- **Lung Cancer**
  - $p(l|s) = 0.1$
  - $p(l|\bar{s}) = 0.01$

- **Bronchitis**
  - $p(b|s) = 0.6$
  - $p(b|\bar{s}) = 0.3$

- **Either T or L**
  - $p(d|e, b) = 0.9$
  - $p(d|e, \bar{b}) = 0.7$
  - $p(d|\bar{e}, b) = 0.8$
  - $p(d|\bar{e}, \bar{b}) = 0.1$

- **Dyspnoea**

- **X-ray**
  - $p(x|e) = 0.98$
  - $p(x|\bar{e}) = 0.05$
A patient turns to a doctor and complains about shortness of breath (Dyspnoea). Also, she confirms a recent trip to Asia. What is the probability that she suffers from Bronchitis?

\[ p(B|A, D) = \frac{p(A, B, D)}{p(A, D)} \]

This requires to compute

\[ p(A, B, D) = \sum_{E, L, S, T, X} p(A, B, D, E, L, S, T, X) \]

with

\[ p(A, B, D, E, L, S, T, X) = p(A) \times p(T|A) \times \cdots \times p(D|E, B) \]
A patient turns to a doctor and complains about shortness of breath (Dyspnoea). Also, she confirms a recent trip to Asia. What is the probability that she suffers from Bronchitis?

\[
p(B|A, D) = \frac{p(A, B, D)}{p(A, D)}
\]

This requires to compute

\[
p(A, B, D) = \sum_{E, L, S, T, X} p(A, B, D, E, L, S, T, X)
\]

with

\[
p(A, B, D, E, L, S, T, X) = p(A) \times p(T|A) \times \cdots \times p(D|E, B)
\]
Complexity Concerns

- \( p(A, B, D, E, L, S, T, X) \) is a table with \( 2^8 \) values
- A joint prob. distribution over \( n \) variables has \( 2^n \) entries
- *Quick Medical Reference* has more than 5000 variables

Solution: Apply the distributive law:

\[
p(A, B, D) = \sum_{E,L,S,T,X} p(A, B, D, E, L, S, T, X)
\]

is equal to

\[
p(A) \sum_{E} p(D|B,E) \sum_{X} p(X|E) \left( \sum_{T} p(T|A) \left( \sum_{L} p(E|L,T) \left( \sum_{S} p(L|S)p(B|S)p(S) \right) \right) \right)
\]
Complexity Concerns

- $p(A, B, D, E, L, S, T, X)$ is a table with $2^8$ values
- A joint prob. distribution over $n$ variables has $2^n$ entries
- *Quick Medical Reference* has more than 5000 variables
- Solution: Apply the distributive law:

$$p(A, B, D) = \sum_{E, L, S, T, X} p(A, B, D, E, L, S, T, X)$$

is equal to

$$p(A) \sum_E p(D | B, E) \sum_X p(X | E) \left( \sum_T p(T | A) \left( \sum_L p(E | L, T) \left( \sum_S p(L | S) p(B | S) p(S) \right) \right) \right)$$
Complexity Concerns

\[ p(A) \sum_E p(D|B, E) \sum_X p(X|E) \left( \sum_T p(T|A) \left( \sum_L p(E|L, T) \left( \sum_S p(L|S)p(B|S)p(S) \right) \right) \right) \]

- The largest intermediate table involves 4 variables

Semirings allow to reduce complexity.

- Intuitively, compare the number of operations

\[ a \times (b + c) = (a \times b) + (a \times c) \]

- The fusion algorithm produces such factorizations
Lesson 2:

Generic Reasoning
The fusion algorithm is only based on the properties of a commutative semiring.

We can exchange the semiring in the problem description.

Example: take \(\langle [0, 1], \max, \cdot \rangle\) instead of \(\langle \mathbb{R}, +, \cdot \rangle\)

\[
\max_{E,L,S,T,X} p(A, B, D, E, L, S, T, X) = \\
p(A) \max_{D|B, E} \max_{X|E} \left( \max_{T|A} \left( \max_{E|L, T} \left( \max_{L|S} p(B|S)p(S) \right) \right) \right)\]

This identifies the value of the most probable configuration.
Beyond Bayesian Networks

The same computational problem over different semirings:

- \( \langle \{0, 1\}, \lor, \land \rangle \leadsto \) crisp constraint reasoning
- \( \langle \mathbb{N}, \min, + \rangle \leadsto \) weighted constraint reasoning
- \( \langle [0, 1], \max, \cdot \rangle \leadsto \) possibilistic constraint reasoning
- \( \langle \mathcal{P}(S), \cup, \cap \rangle \leadsto \) assumption-based reasoning

Different semirings \( \leadsto \) different semantics of

- the same problem
- the same algorithm
- the same complexity
- the same implementation
A fundamentally different Branch of Mathematics
We introduce the following relation on a semiring:

\[ a \preceq b \quad \text{if, and only if} \quad \exists c \in A \text{ such that } a + c = b \]

- Reflexivity: \( a \preceq a \)
- Transitivity: \( a \preceq b \text{ and } b \preceq c \Rightarrow a \preceq c \)
- Conclusion: \( \preceq \) is a preorder called canonical preorder

All semirings provide a canonical preorder
Semirings and Order I

We introduce the following relation on a semiring:

\[ a \preceq b \text{ if, and only if } \exists c \in A \text{ such that } a + c = b \]

- Reflexivity: \( a \preceq a \)
- Transitivity: \( a \preceq b \) and \( b \preceq c \) \( \Rightarrow \) \( a \preceq c \)
- Conclusion: \( \preceq \) is a preorder called canonical preorder

All semirings provide a canonical preorder
In general, $\preceq$ is not antisymmetric, i.e.
\[ a \preceq b \text{ and } b \preceq a \nRightarrow a = b \]

Example: in $\langle \mathbb{Z}, +, \cdot \rangle$ we have $-1 \preceq 2$ and $2 \preceq -1$

Does not only hold for $\langle \mathbb{Z}, +, \cdot \rangle$ but for all structures with inverse additive elements

Antisymmetry of $\preceq$ contradicts the group structure of $(A, +)$
In general, \( \preceq \) is not antisymmetric, i.e.
\[
a \preceq b \text{ and } b \preceq a \not\Rightarrow a = b
\]

Example: in \( \langle \mathbb{Z}, +, \cdot \rangle \) we have \( -1 \preceq 2 \) and \( 2 \preceq -1 \)

Does not only hold for \( \langle \mathbb{Z}, +, \cdot \rangle \) but for all structures with inverse additive elements

Antisymmetry of \( \preceq \) contradicts the group structure of \( (A, +) \)
This splits algebra into:
- semirings with additive inverse elements (e.g. fields)
- semirings with a canonical partial order called dioids

Dioid theory is fundamentally different from maths over fields

Are dioids of (practical) importance?
Examples of Dioids

Theorem

Semirings with idempotent \( + \) (i.e. \( a + a = a \)) are always dioids.

- Arithmetic Semirings: \( \langle \mathbb{R}, +, \cdot \rangle, \langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{N}, +, \cdot \rangle, \ldots \)
- Boolean Semiring: \( \langle \{0, 1\}, \lor, \land \rangle \)
- Tropical Semiring: \( \langle \mathbb{N}, \min, + \rangle \)
- Arctic Semiring: \( \langle \mathbb{N}, \max, + \rangle \)
- Possibilistic Semiring: \( \langle [0, 1], \max, \cdot \rangle \)
- Powerset lattice: \( \langle \mathcal{P}(\mathcal{S}), \cup, \cap \rangle \)
- Bottleneck Semiring: \( \langle \mathbb{R}, \max, \min \rangle \)
- Truncation Semiring: \( \langle \{0, \ldots, k\}, \max, \min\{a + b, k\} \rangle \)
- Lukasiewicz Semiring: \( \langle [0, 1], \min, \max\{a + b - 1, 0\} \rangle \)
- Division Semiring: \( \langle \mathbb{N}, \text{lcm}, \gcd \rangle \)
- Formal Languages: \( \langle \mathcal{P}(\Sigma^*), \cup, \circ \rangle \rightsquigarrow \text{not commutative} \)
Examples of Dioids

**Theorem**

*Semirings with idempotent* $+$ (i.e. $a + a = a$) *are always dioids.*

- Arithmetic Semirings: $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{N}, +, \cdot \rangle$, \ldots
- Boolean Semiring: $\langle \{0, 1\}, \lor, \land \rangle$
- Tropical Semiring: $\langle \mathbb{N}, \min, + \rangle$
- Arctic Semiring: $\langle \mathbb{N}, \max, + \rangle$
- Possibilistic Semiring: $\langle [0, 1], \max, \cdot \rangle$
- Powerset lattice: $\langle \mathcal{P}(\mathcal{S}), \cup, \cap \rangle$
- Bottleneck Semiring: $\langle \mathbb{R}, \max, \min \rangle$
- Truncation Semiring: $\langle \{0, \ldots, k\}, \max, \min\{a + b, k\} \rangle$
- Lukasiewicz Semiring: $\langle [0, 1], \min, \max\{a + b - 1, 0\} \rangle$
- Division Semiring: $\langle \mathbb{N}, \text{lcm}, \text{gcd} \rangle$
- Formal Languages: $\langle \mathcal{P}(\Sigma^*), \cup, \circ \rangle \leadsto$ not commutative
Application of Dioid Theory
Shortest Distance from $S$ to $T$

Compute

\[
9 + 4 = 13
\]
\[
1 + 6 + 5 = 12
\]
\[
1 + 2 + 3 + 5 = 11
\]

and then

\[
\min\{13, 12, 11\} = 11
\]
Connectivity of $S$ and $T$

Compute

$$
\min\{0, 1\} = 0 \\
\min\{1, 1, 1\} = 1 \\
\min\{1, 1, 0, 1\} = 0
$$

and then

$$
\max\{0, 1, 0\} = 1
$$
Largest Capacity from $S$ to $T$

Compute

$$\min\{3.4, 4.5\} = 3.4$$
$$\min\{3.6, 5.5, 5.1\} = 3.6$$
$$\min\{3.6, 4.2, 3.5, 5.1\} = 3.5$$

and then

$$\max\{3.4, 3.6, 3.5\} = 3.6$$
Maximum Reliability from $S$ to $T$

Compute

\[
0.4 \cdot 0.8 = 0.32 \\
0.9 \cdot 0.2 \cdot 0.7 = 0.126 \\
0.9 \cdot 0.9 \cdot 1.0 \cdot 0.7 = 0.567
\]

and then

\[
\max\{0.32, 0.126, 0.567\} = 0.567
\]
Language leading from $S$ to $T$ in the Automaton

Compute

$$\{a\} \circ \{c\} = \{ac\}$$
$$\{a\} \circ \{b\} \circ \{a\} = \{aba\}$$
$$\{a\} \circ \{c\} \circ \{b\} \circ \{a\} = \{acba\}$$

and then

$$\bigcup \{\{ac\}, \{aba\}, \{acba\}\} = \{ac, aba, acba\}$$
The Algebraic Path Problem

- These are path problems over different semirings

- If $\mathbf{M}$ denotes the matrix of edge weights in the graph, all-pairs path problems are solved by computing

$$\mathbf{D} = \bigoplus_{r \geq 0} \mathbf{M}^r = \mathbf{I} + \mathbf{M} + \mathbf{M}^2 + \mathbf{M}^3 + \ldots$$

This is an infinite series of semiring matrices.

- A solution is obtained if the series converges. This requires the notion of a topology.
The Algebraic Path Problem

- These are path problems over different semirings.

- If \( M \) denotes the matrix of edge weights in the graph, all-pairs path problems are solved by computing

\[
D = \bigoplus_{r \geq 0} M^r = I + M + M^2 + M^3 + \ldots
\]

This is an infinite series of semiring matrices.

- A solution is obtained if the series converges. This requires the notion of a topology.
The partial order in dioids allows to introduce a particular topology and to study the convergence of the series.

**Theorem**

*If the limit $D$ exists, then it corresponds to the least solution to the fixpoint equation $X = MX + I$.*

Hence, arbitrary path problems are computed by a single algorithm that solves a dioid fixpoint equation system.

This was the hour of birth of semiring topology.
The partial order in dioids allows to introduce a particular topology and to study the convergence of the series.

**Theorem**

*If the limit $D$ exists, then it corresponds to the least solution to the fixpoint equation $X = MX + I$.*

Hence, arbitrary path problems are computed by a single algorithm that solves a dioid fixpoint equation system.

This was the hour of birth of semiring topology.
Recap of today’s Breakfast Lessons

2 reasons why computer scientists are interested in semirings:
  • they reduce problem complexity
  • they enable generic problem solving

2 reasons why mathematicians are interested in semirings:
  • ordered semirings are fundamentally different from fields
  • new research fields thanks to applications in CS