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 $+$: $\quad a \times (b + c) = (a \times b) + (a \times c)$

If $\times$ is commutative too $\rightsquigarrow$ commutative semiring

Examples I

- Arithmetic Semirings: $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{N}, +, \cdot \rangle$, $\ldots$
- Boolean Semiring: $\langle \{0, 1\}, \vee, \wedge \rangle$
- 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: $\langle \mathbb{N}, lcm, gcd \rangle$
- Formal Languages: $\langle \mathcal{P}(\Sigma^*), \cup, \circ \rangle \rightsquigarrow$ 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:

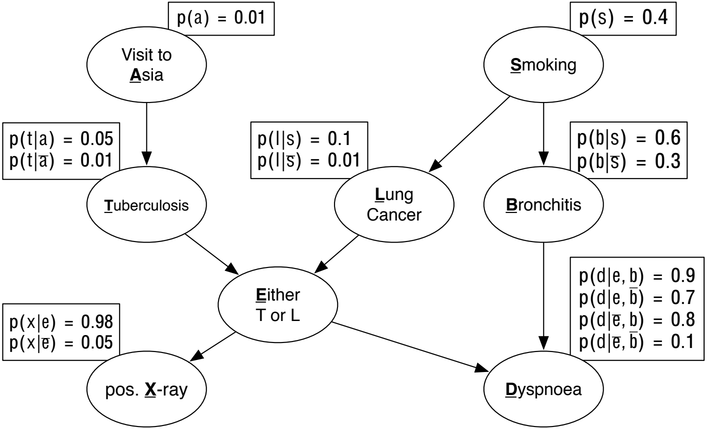
- they reduce problem complexity
- they enable generic problem solving

2 reasons why mathematicians are interested in semirings:

- ordered semirings are fundamentally different from fields
- new research fields thanks to applications in CS

Reducing Problem Complexity

Bayesian Networks



Medical Diagnostics

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

$$p(A, B, D, E, L, S, T, X) \;=\; p(A) \times p(T|A) \times \cdots \times p(D|E, B)$$

Medical Diagnostics

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

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

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

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

Complexity Concerns

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

- 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

Generic Reasoning

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 $\langle \mathbb{R}, +, \cdot \rangle$

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

$$p(A) \max p(D|B,E) \max p(X|E) \Big(\max p(T|A) \Big(\max p(E|L,T) \Big(\max p(L|S) p(B|S) p(S) \Big) \Big) \Big)$$

- This identifies the value of the most probable configuration

Beyond Bayesian Networks

The same computational problem over different semirings:

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

Different semirings $\rightsquigarrow$ different semantics of

- the same problem
- the same algorithm
- the same complexity
- the same implementation

A fundamentally different Branch of Mathematics

Semirings and Order I

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: $a \preceq b$ 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:

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

- Reflexivity: $a \preceq a$
- Transitivity: $a \preceq b$ 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 II

- In general, $\preceq$ is not antisymmetric, i.e.

$$a \preceq b \text{ and } b \preceq a \quad \not\Rightarrow \quad a = b$$

- 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 $(A, +)$

Semirings and Order II

- In general, $\preceq$ is not antisymmetric, i.e.

$$a \preceq b \text{ and } b \preceq a \quad \not\Rightarrow \quad a = b$$

- 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 $(A, +)$

Dioids

- 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: $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{N}, +, \cdot \rangle$, ...
- Boolean Semiring: $\langle \{0, 1\}, \vee, \wedge \rangle$
- 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: $\langle \mathbb{N}, lcm, gcd \rangle$
- Formal Languages: $\langle \mathcal{P}(\Sigma^*), \cup, \circ \rangle \rightsquigarrow$ not commutative

Examples of Dioids

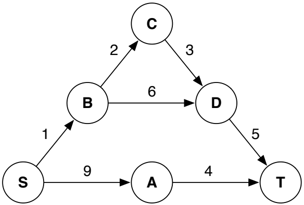
Theorem

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

- Arithmetic Semirings: $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{N}, +, \cdot \rangle$, ...
- Boolean Semiring: $\langle \{0, 1\}, \vee, \wedge \rangle$
- 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: $\langle \mathbb{N}, lcm, gcd \rangle$
- Formal Languages: $\langle \mathcal{P}(\Sigma^*), \cup, \circ \rangle \rightsquigarrow$ not commutative

Application of Dioid Theory

Shortest Distance from S to T



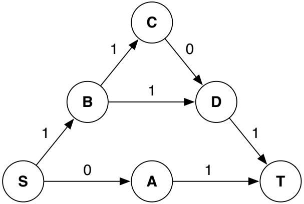
Compute

$$\begin{aligned} 9+4 &= 13 \\ 1+6+5 &= 12 \\ 1+2+3+5 &= 11 \end{aligned}$$

and then

$$\min\{13, 12, 11\} = 11$$

Connectivity of S and T



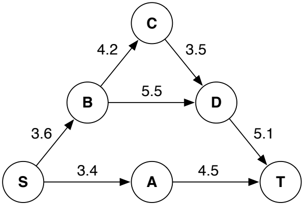
Compute

$$\begin{aligned} \min\{0,1\} &= 0 \\ \min\{1,1,1\} &= 1 \\ \min\{1,1,0,1\} &= 0 \end{aligned}$$

and then

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

Largest Capacity from S to T



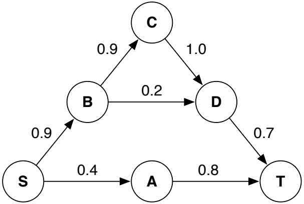
Compute

$$\begin{aligned} \min\{3.4, 4.5\} &= 3.4 \\ \min\{3.6, 5.5, 5.1\} &= 3.6 \\ \min\{3.6, 4.2, 3.5, 5.1\} &= 3.5 \end{aligned}$$

and then

$$\max\{3.4, 3.6, 3.5\} = 3.6$$

Maximum Reliability from S to T



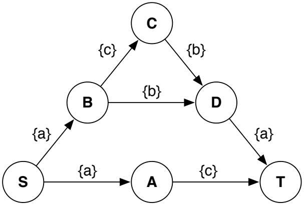
Compute

$$
\begin{aligned}
0.4 \cdot 0.8 &= 0.32 \\
0.9 \cdot 0.2 \cdot 0.7 &= 0.126 \\
0.9 \cdot 0.9 \cdot 1.0 \cdot 0.7 &= 0.567
\end{aligned}
$$

and then

$$\max\{0.32, 0.126, 0.567\} = 0.567$$

Language leading from S to T in the Automaton



Compute

$$\begin{aligned} \{a\} \circ \{c\} &= \{ac\} \\ \{a\} \circ \{b\} \circ \{a\} &= \{aba\} \\ \{a\} \circ \{c\} \circ \{b\} \circ \{a\} &= \{acba\} \end{aligned}$$

and then

$$\bigcup \{\{ac\}, \{aba\}, \{acba\}\} = \{ac, aba, acba\}$$

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

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

  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

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

  This is an infinite series of semiring matrices

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

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 $\mathbf{D}$ *exists, then it corresponds to the least solution to the fixpoint equation* $\mathbf{X} = \mathbf{MX} + \mathbf{I}$

- 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

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 $\mathbf{D}$ exists, then it corresponds to the least solution to the fixpoint equation $\mathbf{X} = \mathbf{MX} + \mathbf{I}$

- 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