Symbolic Petri Net Analysis Using Polynomials

Jochen Spranger
BTU Cottbus
Computer Science Institute
jsp@informatik.tu-cottbus.de

October 29, 1997

.

Contents

(Symbolic) RG Generation

- **Statespace:** $(p_1, \ldots, p_n) \in \mathbb{F}_2^n$
- **Transitionrel.:** $(p_1, \ldots, p_n, p'_1, \ldots, p'_n) \in \mathbb{F}_2^{2n}$

---

function next($States$, TR);
begin
  N := Expand($States \cap TR|_{[p_1,\ldots,p_n]}$);
  return subst($p'_i \to p_i$, N$|_{[p'_1,\ldots,p'_n]}$);
end.

function SymbRG(M_0, TR);
begin
  new := $\{M_0\}$;
  repeat
    old := new;
    new := old $\cup$ next(old, TR);
  until old == new;
  return old;
end.

Monomials, Polynomials, Varieties, Ideals

- **Monomial:** $x^\alpha := x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$
- **Polynomial:**

$$f := \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in \mathbb{F}_2$$

- **Polynomial Ring:** $\mathbb{F}_2[x_1, \ldots, x_n]$
- **Variety:**

$$V(f_1, \ldots, f_m) := \{(a_1, \ldots, a_n) \in \mathbb{F}_2^n \mid f_i(a_1, \ldots, a_n) = 0\}$$

- **Examples:**

1. $V(0) = \mathbb{F}_2^n$
2. $V(x_1^2 + x_1, x_2^2 + x_2, \ldots, x_n^2 + x_n) = \mathbb{F}_2^n$
3. $V(x_1, x_2 + 1) = \{(0, 1, \ldots) \in \mathbb{F}_2^n\}$
4. $V(x_1 \cdot (x_2 + 1), (x_1 + 1) \cdot x_2) = \emptyset$

- **Ideal:** $f_1, \ldots, f_s \in \mathbb{F}_2[x_1, \ldots, x_n]$

$$\langle f_1, \ldots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i \cdot f_i \mid h_1, \ldots, h_s \in \mathbb{F}_2[x_1, \ldots, x_n] \right\}$$

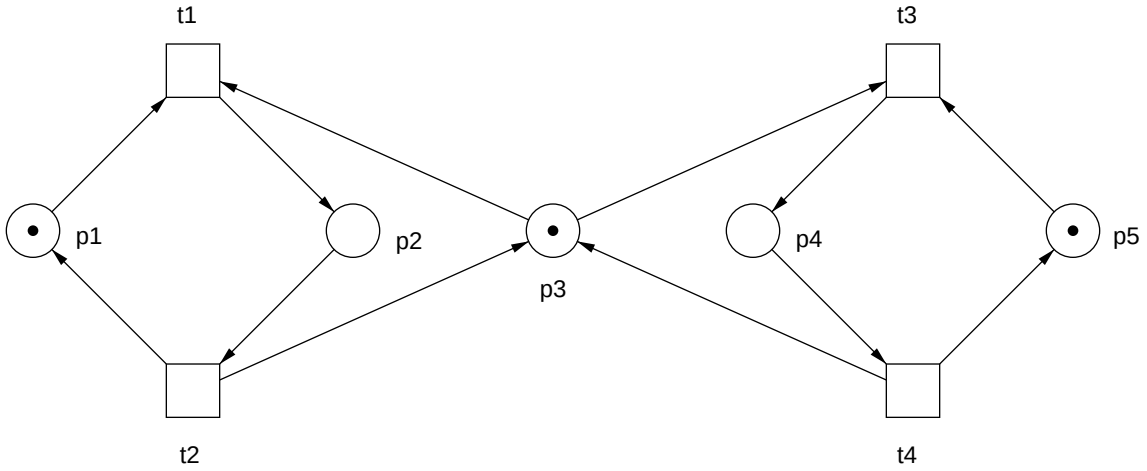
- **Rem:**

1. $\langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_2[x_1, \ldots, x_n]$
2. $f_1, \ldots, f_s$ are a basis of $\langle f_1, \ldots, f_s \rangle$

- **Properties:** $I = \langle f_1, \ldots, f_s \rangle,\ J = \langle g_1, \ldots, g_t \rangle$

1. $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$
   $\Longrightarrow V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$
2. $V(f_1, \ldots, f_s) = V(\langle f_1, \ldots, f_s \rangle)$
3. $V(I) \cap V(J) = V(I + J)$
   $= V(\{f + g \mid f \in I, g \in J\})$
4. $V(I) \cup V(J) = V(I \cdot J)$
   $= V(\langle \{f_i \cdot g_j \mid 1 \leq i \leq s, 1 \leq j \leq t\} \rangle)$

Example



$$t_1 = V(p_1{+}1, p_3{+}1, p'_1, p'_3, p_2, p'_2{+}1, p_4{+}p'_4, p_5{+}p'_5)$$
$$t_2 = V(p_2{+}1, p'_2, p_1, p'_1{+}1, p_3, p'_3{+}1, p_4{+}p'_4, p_5{+}p'_5)$$
$$t_3 = V(p_3{+}1, p_5{+}1, p'_3, p'_5, p_4, p'_4{+}1, p_1{+}p'_1, p_2{+}p'_2)$$
$$t_4 = V(p_4{+}1, p'_4, p_3, p'_3{+}1, p_5, p'_5{+}1, p_1{+}p'_1, p_2{+}p'_2)$$

$$\Longrightarrow TR = t_1 \cup t_2 \cup t_3 \cup t_4$$

$$M_0 = V(p_1 + 1, p_2, p_3 + 1, p_4, p_5 + 1)$$

Reachability:

$V(p_2 + 1, p_4 + 1) \cap RG = \emptyset$
$V(p_1, p_2 + 1, p_3, p_4, p_5 + 1) \cap RG \neq \emptyset$

Deadlock:

$INVTR = V(p_1 * p_3, p_2, p_3 * p_5, p_4)$
$INVTR \cap RG = \emptyset$

Elimination

- **Admissible monomial ordering**

- **Gröbner bases:** Every ideal have an uniquely defined (reduced) basis (with respect to an admissible ordering), such that holds:

  1. $I = J \Longleftrightarrow GB(I) = GB(J)$
  2. $V(I) = V(GB(I))$

- **Elimination:** $I_m := I \cap \mathbb{F}_2[x_1, \ldots, x_m], \quad m < n$

$$V(I_m) = \{(a_1, \ldots, a_m) \in \mathbb{F}_2^n \mid \exists a_{m+1}, \ldots, a_n \in \mathbb{F}_2, (a_1, \ldots, a_n) \in V(I)\}$$

  1. Compute the Gröbner basis of I for an elimination ordering.
  2. Remove all polynomials of the Gröbner basis where the leading term have variables from $\{x_{m+1}, \ldots, x_n\}$.

Equality of Varieties

Theorem. [Hilbert's Nullstellensatz] *Let* $\overline{k}$ *be the algebraically closed field of* k*. If* I_1 *and* I_2 *are ideals of* $k[x_1, \ldots, x_n]$*, then* $\overline{V}(I_1) = \overline{V}(I_2)$ *iff* $rad(I_1) = rad(I_2)$*.*

- **Radical:**

  $$rad(I) = \{f \mid f(a_1, \ldots, a_n) = 0,\ \forall (a_1, \ldots, a_n) \in V(I)\}$$

- **Rem:** radicals are ideals

- **Problem:** $\overline{V}(I_1) = \overline{V}(I_2)$

- **Idea:** $Z := \langle x_1^2 + x_1, x_2^2 + x_2, \ldots, x_n^2 + x_n \rangle$

  It holds:

  1. $\mathbf{V(I)} = V(I) \cap \mathbb{F}_2^n = V(I) \cap V(Z) = \mathbf{V(I + Z)}$
  2. $\overline{V}(Z) = \mathbb{F}_2^n$

$$\Longrightarrow \overline{\mathbf{V}}(\mathbf{I} + \mathbf{Z}) = \overline{V}(I) \cap \overline{V}(Z) = \overline{V}(I) \cap \mathbb{F}_2^n = \mathbf{V(I)}$$

$$\mathbf{V(I_1 + Z) = V(I_2 + Z)} \Longleftrightarrow \mathbf{rad(I_1 + Z) = rad(I_2 + Z)}$$

Conclusion

---

function next(Ideal $States$, Ideal TR);
begin
  return subst($p'_i \to p_i$, Elim(p_i, $TR + States$));
end.

function SymbRG(Ideal M_0, Ideal TR, Ideal Z);
begin
  new := M_0;
  repeat
    old := new;
    new := old $*$ next(old, $TR + Z$);
  until GB(rad(old)) == GB(rad(new));
  return old;
end.

References

[1] E. Pastor, J. Cortella, O. Roig. *Symbolic Petri Net Analysis Using Boolean Manipulation*. UPC/DAC RR-97/8, 1997.

[2] O. Caprotti, A. Ferscha, H. Hong. *Reachability Test in Petri Nets by Gröbner Bases*. RISC-Linz TR. 95-03, 1995.

[3] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer Verlag, 1992.

[4] G. S. Avrunin. *Symbolic Model Checking Using Algebraic Geometry*. Computer Aided Verification, LNCS 1102, 1996.