

# An unexpected application of minimization theory to module decompositions

G erard Duchamp, Hatem Hadj Kacem,  Eric Laugerotte  
{gerard.duchamp, hatem.hadj-kacem, eric.laugerotte}@univ-rouen.fr  
*LIFAR, Facult e des Sciences et des Techniques,  
76821 Mont-Saint-Aignan Cedex, France.*

The first step in the minimization process of an automaton  $(\lambda, \mu, \gamma)$  taking its multiplicities in a (commutative or not) field, due to Sch utzenberger, is the construction of a prefix set  $P$  such that the orbit  $\lambda\mu(P)$  of the initial vector be a basis of  $\lambda\mu(k\langle\Sigma\rangle)$  (this amounts to construct a covering tree)[1, 3]. Surprisingly, this permits to study  $\mathcal{H}om_{\mathcal{A}}(M)$  where  $\mathcal{A}$  is a finitely generated algebra and  $M$  has a single generator[2]. In particular one can obtain a certificate  $cert(M)$  checking whether the module is or not indecomposable. Exploiting the degrees of freedom in the intermediate computations, one can study in complete detail the moduli of decompositions of  $M$ . Applications can be designed in every characteristic ( $c$ ). Here are given two of them:

- decomposition of boolean functions ( $c = 2$ ). This provides a criterion of complexity usable in cryptography.
- decomposition of combinatorial modules ( $c = 0$ ).

This new method is intended to take place in MuPAD-Combinat.

## Example:

We consider the boolean function  $f : \{0, 1\}^3 \rightarrow \{0, 1\}$  defined by  $f(x_1, x_2, x_3) = x_1x_2 + x_1 + x_3$ , the action being given by the algebra of the symmetric group permuting the variables ( $\mathcal{A} = \mathbb{Z}/2\mathbb{Z}[S_3]$ ). We apply our algorithm on this function and obtain figure 1 which represent a complete maximal decomposition of the module. When we apply the algorithm, we deduce that the module  $M$  can be decomposed into  $M_1 \oplus M_2$  with  $M_1 = \mathbb{Z}/2\mathbb{Z}[S_3](x_1x_2 + x_1x_3 + x_2x_3)$  and  $M_2 = \mathbb{Z}/2\mathbb{Z}[S_3](x_1 + x_3 + x_1x_2 + x_2x_3)$  (see figure 2).

## References

- [1] J. BERSTEL, C. REUTENAUER, "Rational series and their languages". EATCS Monographs on Theoretical Computer Science. Springer 1988.
- [2] G. DUCHAMP, F. HIVERT, J.-Y. THIBON, "Noncommutative symmetric functions VI: Free quasi-symmetric functions and related algebras." International Journal of Algebra and computation **12** No. 5, 671-717, 2002.
- [3] M. FLOURET, E. LAUGEROTTE, "Noncommutative minimization algorithms". Information Processing Letters **64**, 123-126, 1997.

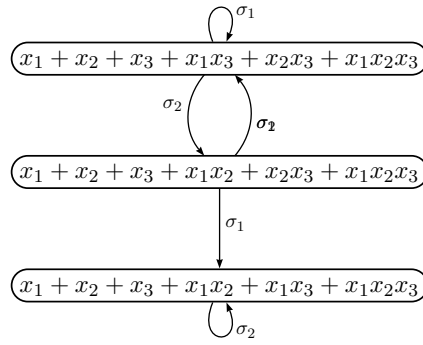


Figure 1: Action of  $\sigma_i$  on  $g = \mathbb{Z}/2\mathbb{Z}[S_3](x_1 + x_2 + x_3 + x_1x_3 + x_2x_3 + x_1x_2x_3)$

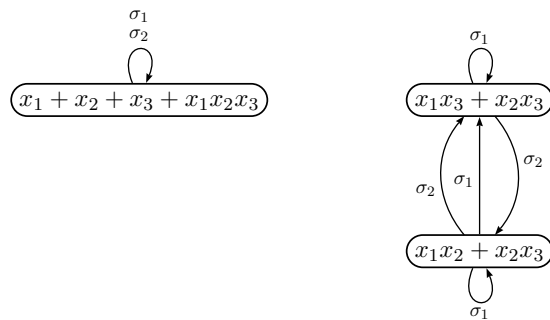


Figure 2: Complete maximal decomposition of  $M = g \cdot \mathcal{F}$