Gröbner presentations of a monoid algebras and applications

M. Borges-Quintana M. Borges-Trenard
University of Oriente, Cuba

E. Martínez-Moro
University of Valladolid, Spain

March 26, 2008

Let $X = \{x_1, \ldots, x_n\}$ be a finite alphabet and $\langle X \rangle$ the free monoid (with multiplicative structute and 1) generated by X. Let $\mathcal{I}$ be an ideal of $k\langle X \rangle$. We will say, as usual, that a k-algebra (k a field) $\mathcal{A}$ generated by $A = \{a_1, \ldots, a_n\} \subset \mathcal{A}$ is canonically isomorphic to $k\langle X \rangle / \mathcal{I}$ if $\ker(E) = \mathcal{I}$, where E is the natural projection of $k\langle X \rangle$ into $\mathcal{A}$. We will say that a set $G \subset k\langle X \rangle$ is a Gröbner presentation of $k\langle X \rangle / \mathcal{I}$ (therefore of the algebra $\mathcal{A}$) if there exist an ordering $\prec$ in the terms of $\langle X \rangle$ such that G is a reduced Gröbner basis of $\mathcal{I}$ w.r.t. the ordering $\prec$. Note that, if there exists a finite reduced Gröbner basis (it is not always true, there are some ideals with no finite reduced Gröbner basis for any oredering, moreover, the problem of knowing it is not decidible) several computational task can be made for answering about "properties" of the algebra using the presentation. Note also that this is always the case when we are dealing with zero-dimensional ideals. In this talk we will review several aplications of this setting:

- Computing the normal closure of a group.
- Computing the canonical form of a finite abelian group.
- Computing the Grobner presentation of a binary linear code.

References

[1] Borges-Quintana, M. ; Borges-Trenard, M. A. ; Martínez-Moro, E. On a Gröbner bases structure associated to linear codes. J. Discrete Math. Sci. Cryptogr. 10 (2007), no. 2, 151–191.

[2] Borges-Quintana, M. ; Borges-Trenard, M. A. ; Martínez-Moro, E. A general framework for applying FGLM techniques to linear codes. Applied algebra, algebraic algorithms and error-correcting codes, 76–86, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006.

[3] Borges-Trenard, Miguel A. ; Borges-Quintana, Mijail ; Castellanos-Garzón, José A. ; Martínez-Moro, Edgar . The symmetric group given by a Gröbner basis. J. Pure Appl. Algebra 207 (2006), no. 1, 149–154.

[4] Borges-Quintana, M. ; Borges-Trenard, M. A. ; Martínez-Moro, E. On the use of Gröbner bases for computing the structure of finite abelian groups. Computer algebra in scientific computing, 52–64, Lecture Notes in Comput. Sci., 3718, Springer, Berlin, 2005.