GRÖBNER BASES -- A POWERFUL TOOL FOR SOLVING DSP TASKS

Woodburn C.J.

Pittsburg State University
Department of Mathematics
1701 S. Broadway, Pittsburg, KS 66762, USA
E-mail: cwoodbur@pittstate.edu, Tel. (620) 235-4409

Abstract: Many problems in digital signal processing can be reduced to mathematical questions involving multivariate polynomials. Techniques involving Gröbner bases can then be efficiently applied. We present a brief overview of Gröbner basis theory, followed by a look at some applications in DSP.

1. Introduction

The concept of a Gröbner basis was first introduced by Bruno Buchberger in his Ph.D. thesis in 1966. Since that time the theory has been expanded and applied to a variety of fields including mathematics, computer science and engineering. Gröbner basis theory is a powerful mathematical tool since it provides a method for efficiently performing computations involving multivariate polynomials. Buchberger's algorithm for constructing a Gröbner basis of a multivariate polynomial ideal generalizes both the Euclidean algorithm for univariate polynomials and Gaussian elimination for systems of linear polynomials. So it is natural to try and apply Gröbner basis techniques to generalizations of problems which can be answered by using either the Euclidean algorithm or Gaussian elimination. For example, the need to solve and/or investigate solutions of a system of multivariate polynomials arises quite often in any technical area including DSP. Linear systems can be solved using Gaussian elimination, while Gröbner bases provide a tool for attacking multivariate polynomial systems [3]. As another example, the Euclidean algorithm is often used in the analysis of 1-D multirate systems, while Gröbner basis techniques are useful in the analysis of M-D multirate systems [PKV]. Much work has already been done to apply Gröbner basis techniques to a variety of problems in systems theory. (See [1] for a list of 18 problems and 15 papers.)

2. Fundamental Ideas of Gröbner Bases Theory

We begin with some notation and terminology. A multivariate polynomial ring with coefficients from a field such as the real numbers will be denoted by $R = k[x_1, \ldots, x_n]$, where k represents the field. An **ideal** I of R is a nonempty subset such that the following two conditions hold:

1. if f and g are in I then $f + g$ is in I, and
2. if f is in I and h is any polynomial in R then fh is in I.

A set $\{f_1, \ldots, f_n\}$ is called a **basis** for I if $I = < f_1, \ldots, f_n> = \{g_1 f_1 + \cdots + g_n f_n : g_1, \ldots, g_n$ are in $R\}$. According to the Hilbert Basis Theorem, every ideal of R is finitely generated. In the univariate case, we can say even more: every ideal of $k[x]$ is generated by just one element, and we can use the Euclidean algorithm to find such a generator. So, in $k[x]$, a polynomial f is in an ideal $I = <g>$ if and only if a remainder of 0 is obtained when f is divided by g.

Ordering the monomials of a polynomial by degree is implicit in the division algorithm in $k[x]$. But, the situation is more complicated in the multivariate case. For example, does one write $2x^2+3y^2-xy$ or $3y^2-xy+2x^2$ or $2x^2-xy+3y^2$ or perhaps some other ordering? A **monomial ordering** is defined to be a total ordering on the set of monomials of R which is preserved under multiplication by a monomial (compatibility) and is a well-ordering. The last condition is useful to guarantee that algorithms such as the division algorithm will terminate, and this condition may be replaced with the equivalent condition that 1 is the smallest monomial. In the univariate case, there is only one monomial ordering, namely increasing order by degree. Some examples of monomial orders include lexicographic (dictionary) ordering, graded lexicographic ordering, and graded reverse lexicographic ordering. There are also weight orderings based on using a vector to weight the variables and product orderings in which different orderings are used for different variables in the monomials.

Having a monomial ordering allows one to generalize the division algorithm over $k[x]$ to the multivariate case. So, any multivariate polynomial f can be divided by a set of polynomials $\{f_1, f_2, \ldots, f_n\}$ to obtain $f = q_1 f_1 + q_2 f_2 + \cdots + q_n f_n + r$, for some polynomials $q_1, q_2, \ldots, q_n, r$. In general, however, if one switches the order of the f_i during the division algorithm, the remainder is not unique. For example,

$xy^2 - x = y(xy+1) + 0(y^2-1) + (-x-y) = x(y^2-1) + 0(xy+1) + 0.$

(Notice that the latter expression shows $xy^2 - x$ is in $< xy+1, y^2-1 >$, but the former does not.) However, the remainder is uniquely determined whenever one divides a polynomial by a Gröbner basis. Therefore, Gröbner bases provide an easy algorithmic method for answering the ideal membership question: If G is a Gröbner basis of an ideal I, then a polynomial f is in I if and only if the remainder upon division of f by G is 0. Many applications of Gröbner bases are based on the ideal membership question.

Important to DSP applications of Gröbner bases are the fact that every ideal of *R* has a Gröbner basis with respect to each monomial ordering and the existence of Buchberger's algorithm, which provides an implementable way to compute Gröbner bases. Most general-purpose computer algebra systems, such as Derive, Maple, and Mathematica, contain implementations of Buchberger's algorithm. In addition, there are several systems, such as CoCoA, Macaulay, and Singular, which specialize in efficient methods for computing Gröbner bases along with related algorithms and applications.

3. Some Applications of Gröbner Bases

A. Solving a system of multivariate polynomial or Laurent polynomial equations

Problems often arise in any technical field which involve solving a system of equations. If the equations are linear, Gaussian elimination can be used. If the equations are multivariate polynomials, Gröbner bases can be used to determine if the system has a solution, whether or not there are finitely many solutions, and if so, to find the solutions [3]. If the equations involve Laurent polynomials (negative exponents on the variables), the problem can be reduced to the multivariate polynomial (nonnegative exponents) case and Gröbner basis techniques applied [5].

B. Elimination Theory

The above example is actually an application of elimination theory. By computing a Gröbner basis with respect to an elimination monomial ordering, such as a lexicographic order, the problem of solving a system of polynomial equations, $f_1 = f_2 = \cdots = f_s = 0$, is reduced to finding the roots of a univariate polynomial. So, in any situation in which one would like to eliminate variables, Gröbner basis techniques are a possible tool. One such situation arises in the area of computer vision. In [10] it is shown that elimination theory using Gröbner basis techniques is useful in the recovery and manipulation of general 3D information from 2D projections. "The elimination approach can be applied also to shading and coloring domains as well." [10]

C. Matrix Completion

The matrix completion problem is to complete a unimodular rectangular polynomial matrix to an invertible matrix. One place where this problem arises is in the area of MD digital filters, an important area due to the growing demand for processing and compression of still 2D images and video 3D signals in telecommunications and multimedia technology. The design of a perfect reconstruction finite impulse response (FIR) filter bank deals with the problem of completing a unimodular matrix. The polyphase matrix, each of whose rows can be derived directly from the transfer function of each subband filter, is actually a multivariate polynomial matrix in the delay variables. The overall filter bank satisfies the perfect reconstruction constraint if its polyphase matrix is unimodular. The unimodular completion algorithm, which relies on Gröbner basis techniques, enables one to obtain the whole class of perfect reconstruction filter banks when the first row (or the first subband filter) of the polyphase matrix is specified. If desired, further optimization can be implemented to single out the `best' filter bank (with respect to some desired design constraints) [8].

D. Matrix Factorization

Factorization of multivariate polynomial matrices is linked to problems arising in MD digital filter bank design and implementation and in state-space realizations of 2D systems. For example, decomposing a causal biorthogonal MD 2-band filter bank into elementary ladder steps is essentially equivalent to factoring a multivariate polynomial matrix into a product of elementary matrices [5]. According to [4], "elementary multivariable polynomial matrices are expected to be an useful tool for obtaining equivalent state-space realizations of possible minimal dimension for a given 2D system." An algorithm for factoring 3x3 or larger multivariate polynomial matrices with determinant one exists and uses Gröbner basis techniques [7]. There is also an algorithm available for deciding when a 2x2 multivariate polynomial matrix with determinant one can be factored into elementary matrices and for obtaining the factorization when it exists [5].

4. Summary

Problems involving multivariate polynomials arise in many different settings in DSP. Gröbner basis techniques provide a powerful (yet accessible) tool for investigating and solving such problems, since Buchberger's algorithm for computing a Gröbner basis for a polynomial ideal generalizes both the Euclidean algorithm and Gaussian elimination. Much work has already been done to apply Gröbner basis techniques to various problems, but there is more that can be done.

References

[1] B. Buchberger. Gröbner bases and system theory. Special Issue on Applications of Gröbner Bases in Multidimensional Systems and Signal Processing". Kluwer Academic Publishers, 2001.

[2] D. Cox. Introduction to Gröbner bases. Proceedings of Symposia in Applied Mathematics, Vol. 53, 1998.

[3] D. Cox, J. Little, D. O'Shea. Ideals, Varieties and Algorithms. Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[4] K. Galkowski. Elementary operation approach to state-space realizations of 2-D systems. IEEE Trans. on Circuits and Systems - I: Fundamental Theory and Applications, 44(2): 120-129, February 1997.

[5] H. Park. A realization algorithm for $SL_2(k[x_1,...,x_n])$ over the Euclidean domain. SIAM Jour. on Matrix Analysis and Applications, 21:178--184, 1999.

[6] H. Park, T. Kalker, and M. Vetterli. Gröbner bases techniques in multidimensional multirate systems. Jour. of multidimensional systems and signal processing, 8:11-30, 1997.

[7] H. Park and C. Woodburn. An algorithmic proof of Suslin's stability theorem for polynomial rings. Journ. of Algebra, 178:277-298, 1995.

[8] M.Tchobanou and C. Woodburn. The Quillen-Suslin theorem and the design and implementation of multi-dimensional filter banks. In Proc. 3rd Intl. Conf. on Digital Signal Processing and Its Applications DSPA-2000, Moscow, Russia, 2000, p. 314.

[9] M. Tchobanou and C. Woodburn. Design of M-D filter banks by factorization of M-D polynomial matrices. In Proc. 3rd Intl. Conf. on Information, Communications, and Signal Processing ICICS-2001, Singapore, 2001.

[10] M. Werman and A. Shashua. The study of 3D-from-2D using elimination. In Proc. of the Intl. Conf. on Computer Vision (ICCV), June 1995, Boston MA, 1995.