An algorithm for elimination for sets of polynomial equations

John Nixon [http://www.bluesky-home.co.uk]

September 2005

1 Notes on prerequisites for single variable polynomials

1.1 Factors,roots,monicity

Every polynomial A with the coefficient of the highest power of the variable equal to 1 (a monic polynomial) is the product of factors $z - z_i$ for each root z_i. If the factor appears k times z_i it is said to have multiplicity k. $A(z_i) = 0$. When any polynomial A is divided by the coefficient of its term with highest power, the result is a monic polynomial mon(A), the monic form of A, with the same set of roots and multiplicities as A.

1.2 Greatest Common Divisor(GCD)

The GCD of a pair of polynomials A and B is the product of the common factors of A and B. If a factor appears k_1 times in A and k_2 times in B, in the GCD(A, B) it appears $min(k_1, k_2)$ times (i.e. the smaller of k_1 and k_2). GCD(A, B) divides exactly into both A and B, but no polynomial of degree greater than the degree of GCD(A, B) that contains GCD(A, B) as a factor, itself divides both A and B exactly. This is the meaning of Greatest Common Divisor (GCD). GCD can also be applied to sets of polynomials because it is obviously associative: GCD(GCD$(A, B), C)$ = GCD$(A,$ GCD$(B, C))$. This polynomial is defined as GCD(A, B, C) etc. Similarly GCD$(A, B, C, ...)$ is defined. This is all analogous to the properties of GCD for positive integers. This actually defines the GCD to within a constant factor. To make the GCD unique I will choose it to be monic.

1.3 "Square-free" reduction

If a root of polynomial A has multiplicity $k > 1$, this root is also a root of the first derivative of A (i.e. A') with multiplicity $k - 1$, hence the root is also a root of GCD(A, A') with multiplicity $k-1$. Hence $A/$GCD(A, A') has the same

root with multiplicity 1. Thus $A/\mathrm{GCD}(A, A')$ (i.e. the square-free reduction of A) has the same set of distinct roots as A, but each has a multiplicity of 1.

1.4 Polynomial division

If A_n and B_m are polynomials of degree given by their subscripts, and A_n (the dividand) is divided by B_m (the divisor) where $m \leq n$ the result is a quotient polynomial Q_{n-m} of degree $n - m$ and a remainder polynomial R of degree $< m$. i.e. $A_n = B_m Q_{n-m} + R$. This calculation can be done by polynomial long division. In this calculation, the leading term of A_n is divided by the leading term of B_m to give the quotient Q. Then $A^* = A_n - B_m Q$ is computed that now takes the place of A_n. This calculation is repeated until the degree of $A^* < m$. The sum of all the Qs is Q_{n-m} and R is the final value of A^*.

1.5 The Euclidean algorithm for 2 polynomials – computation of their GCD

Convert both polynomials A and B to monic form. Divide one polynomial by the other, with the divisor polynomial having degree $\leq$ the degree of the dividand. Convert the remainder to monic form. Repeat the division with the new dividand equal to the old divisor, and the new divisor equal to the old remainder until the remainder has degree zero. If the final remainder is 0, the previous remainder is $\mathrm{GCD}(A, B)$, otherwise $\mathrm{GCD}(A, B)$ is 1.

The set of distinct roots of $\mathrm{GCD}(A, B)$ is equal to the set of distinct common roots of the A and B. Hence if the final remainder is not 0, then there is no common root for the original polynomials. In order to get the polynomial with lowest degree whose set of roots is exactly the set of distinct common roots of A and B, the square-free reduction of $\mathrm{GCD}(A, B)$ must be taken.

1.6 The Euclidean algorithm for $p \geq 2$ polynomials (extends the algorithm above for $p = 2$)

Take a pair of polynomials, convert them to monic form, divide one by the other with the degree of the divisor $\leq$ the degree of the dividand. Replace the dividand by the monic form of its remainder. Repeat this until all of them but one have degree zero (i.e. constant). It does not matter how the pairs of polynomials are chosen at each step. There are common roots of the original polynomials if and only if all the degree zero polynomials obtained are all zero. In this case the GCD is the last non-constant polynomial R. Equivalently, this can be done one polynomial at a time as associativity of GCD suggests. [F is a factor of A and B if and only if F is a factor of B and R (where $A = QB + R$) so when the calculation terminates, F is a factor of all the original polynomials if and only if F is a factor of R , so R is the GCD of the original polynomials.]

If there are common roots to all the polynomials, these common distinct roots (and only these) will be the zeros of the square-free reduction of the GCD.

2 Extension to polynomials in several variables

A generalisation of the Euclidean algorithm is sought which does systematic elimination of variables (i.e. simplify as much as possible) for sets of p polynomial equations with k variables, including the above GCD calculation for single variable polynomials as a special case. First the case of two polynomials will be considered. Later the argument will be extended to the case of any number of polynomials. The variables will be denoted by $z_1, ...z_k$ and z_1 is a common variable to be eliminated, and w denotes the set of remaining variables.

2.1 The case $p = 2$

The basic method is to apply the Euclidean algorithm as before in the "general case", treating the w variables as unknown constants. Clearly special cases occur when any of the remainders (including the original polynomials) is independent of z_1 and equal to zero for some sets of values of w (*). For such sets of w's, a non-trivial GCD has been found which is the previous remainder, and this equated to zero determines the common roots. It can be seen that whenever this happens, the equations for w and the GCD equated to zero is one system of equations for further analysis (i.e. "a solution"). If the above equation for w is not satisfied, the calculation for the GCD continues as in the general case until (*) happens again or the end of the general GCD calculation is reached (a remainder with degree 0 with respect to z_1 occurs). Again here if (*) is not satisfied, there are no further systems of equations for further analysis.

To identify (*) when it occurs, note that every remainder is a polynomial in z_1 and the coefficients must be rational functions of w. The condition (*) is the condition that the system of equations given by each of these coefficients equated to zero has some solutions for w. After clearing the fractions, this is a problem of the same type that we are considering, but with one fewer variables because z_1 is absent, so this leads to a recursive algorithm.

At the end of the calculation the result is a set of pairs of polynomials, one member of each pair not involving z_1.

2.2 The case $p > 2$

For each of these pairs of polynomials, the third of the original polynomials is introduced and the algorithm is applied again to the two polynomials involving z_1. The result is a set of triplets of polynomials, two of each triplet not involving z_1 and the other involving z_1. After all the polynomials have been introduced in the same way the result is a set of p-tuples of polynomials, all but one of each p-tuple not involving z_1, but some of the other variables may be eliminated "accidentally".

Finally, the whole procedure should be applied eliminating z_2, $z_3 \ldots$ in the same way that z_1 was eliminated. For elimination of z_j, the $z_1 ...z_{j-1}$ dependent polynomials in each p-tuple are ignored. The final result should be a set of p-tuples of polynomials with the j-th polynomial in each p-tuple having z_1 ... z_{j-1}

eliminated.

Because the degrees of the polynomials with respect to the variable being eliminated are checked at each step, there is no chance of accidental independence one of the equations on this variable when it is supposed to be present. So, for each set of values of the variables z_j , z_{j+1},... satisfying the subset of a final p-tuple of polynomial equations that consists of the ith for all $i \geq j$ for any fixed j, the $j-1$th member of the p-tuple has at least one solution for z_{j-1}. Hence every such p-tuple of polynomial equations has a non-empty solution set, justifying the term "solution". One such p-tuple is the form that the equations are naively expected to take using an elimination strategy. In general several such "solutions" exist.

The variables and equations can be taken in different orders giving equivalent results. Must these be identical if the same set of variables is eliminated?

To obtain explicit solutions in the case where the number of variables (k) equals the number of unknowns (p) using this method, after substitution at each step, p separate single variable polynomial equations have to be solved in sequence.

3 Algebraic relations

Definition 1 *The relation between the complex variables z_1,z_2,...z_l is defined to be algebraic if and only if it can be expressed,for some $k \geq 0$, as a set of $k+1$ equations, each of the form $A_k(z_1, z_2, ...z_{l+k}) = 0$ where the A's are polynomials with respect to each of their arguments.*

To convert this to explicit form requires elimination of the variables $z_{l+1}...z_{l+k}$. The above elimination algorithm will reduce it to the union of the solution sets of equations of the form

$$Q_i(z_1, z_2, ...z_l) = 0$$

(which could be written as a single such equation $\prod_i Q_i = 0$) where Q_i are also a polynomials in each of their arguments. The degrees of freedom in the relation is $l-1$ From Definition 1, it is easy to show that the following operations applied to algebraic relations give other algebraic relations (closure):

- Union
- Inversion (i.e. permutations of the variables if there are > 2 of them.)
- Composition (for $\geq$2 variables this is defined by the elimination of a specific variable from a pair of algebraic relations usually with each relation introducing unique variables – a special case of intersection)
- Addition *
- Multiplication *

- Intersection

  The intersection of a pair of solution sets corresponding to sets of p-tuples of polynomials of the type obtained from the elimination algorithm is the solution set of another such set of p-tuples of polynomials but with usually one fewer degrees of freedom (the number of variables - number of equations).

* For the two-variable case, if the relations $R_1(w_1, z)$ and $R_2(w_2, z)$ are regarded as multi-valued functions $w_1(z)$ and $w_2(z)$ respectively, the relation corresponding to all possible values of $w_1(z) + w_2(z)$ for each z is defined as $R_1 + R_2$. Likewise for multiplication. In general to define $+$ and $\times$, the dependent variable must be specified.