THE USE OF "LET" STATEMENTS IN PRODUCING SHORT COMPREHENSIBLE OUTPUTS

R. Shtokhamer
Department of Physics
Technion-Israel Institute of Technology
Haifa, Israel

Abstract

It is shown that an algebraic implementation of "LET" statements may be useful in producing comprehensible outputs. The suggested algorithm is based on solving large set of linear equations over a field.

Substitution rules of the type "LET P=Q" have wide use in all algebraic systems. The use of it may vary from simple text editing to more complicated algebraic substitutions used, for example, in Fourier analysis. Here we shall address ourselves to another possible use, namely, in producing short comprehensible algebraic outputs.

Consider for example the following expression: $E = (x+y)^{100} - x^{100}$, which consists in an expanded form of 100 terms. Introducing "LET x+y = z" we would like to obtain as output: $E = z^{100} - x^{100}$, $z = x+y$. Clearly any pattern matching techniques will miss that aim, moreover they allow only primitive structures to appear on the left hand side of a "LET" statement. An interesting generalization of substitution rules (overcoming the above restriction) was suggested by H. Kanoui and M. Bergman [1]; however their algorithm is still unable to produce the above simple output.

In this paper we limit outselves to polynomial expressions. A polynomial in t variables $x_1 \ldots x_t$ over a field F may be expressed as a sum of terms: $\Sigma C_{i_1 \ldots i_t} x_1^{i_1} \ldots x_t^{i_t}$, $C_{i_1 \ldots i_t} \varepsilon F$. Let T(P) be the number of nonzero terms in a polynomial P. As indicated by the above example, given a polynomial P, we are interested in producing a polynomial Q, equivalent to P under imposed "LET" statements, for which T(Q) is minimal.

LET statements and ideals

In this section we shall discuss a pure algebraic implementation of "LET" statements. Given a set of LET statements: LET $P_1 = Q_1$, $P_2 = Q_2 \ldots P_\ell = Q_\ell$; we introduce the ideal I spanned by the set $\{P_1-Q_1, P_2-Q_2 \ldots P_\ell-Q_\ell\}$. Two polynomials A,B are said to be equivalent if A-B belongs to I. In such a manner we have introduced equivalence classes. It has already been shown that there exists a canonical representative for each equivalence class [2], [3], [4]. Let $\{P_1,,,,,P_\ell\}$ be a given basis (Gröbner basis for example [2]) for an ideal I.

Let P be a polynomial, and I_p be the equivalence class of P. Hence if $Z \varepsilon I_p \Rightarrow Z = P + \sum_{i=1}^{\ell} B_i P_i$, where B_i are polynomials, our aim is to find $Z \varepsilon I_p$ such that: $\forall \tilde{Z} \varepsilon I_p$, $T(Z) < T(\tilde{Z})$. (We do not require Z to be canonical.)

Description of the algorithm

For simplicity let us first discuss the case of a principal ideal I spanned by $\{P_1\}$ and polynomials in one variable x.

Let Degree $(P_1) = n-1$, Degree $(P) = N-1$, $T(P) = k$. First one needs to obtain a bound on the degree D of the "minimal" polynomial Z. In this case one can easily show: $D<N+(k-1)\cdot n$. Consider now the relation $Z = P+B\cdot P_1$. Let $1,x\ldots x^{D-1}$ be a base of a D dimensional vector space. Viewing Z and P as D dimensional vectors the above relation translates into $\underline{Z} = \underline{P}+\underline{\underline{P}}_1\cdot\underline{B}$ where $\underline{B}$ is a (D-n) dimensional vector and $\underline{\underline{P}}_1$ is a $D\times(D-n)$ matrix. In this equation $\underline{P}$ and $\underline{\underline{P}}_1$ are known. We have essentially a parametric representation of a hyperspace and we need to find in it a vector having a minimal number of components (in a fixed basis). First, all the D-n columns in $\underline{\underline{P}}_1$ are linearly independent. Moreover without losing any generality we may assume $P_1(0) \neq 0$, in which case any D-n rows of $\underline{\underline{P}}_1$ are linearly independent as well. Hence there exists a unique vector $\underline{B}$ (obtained by solving D-n linear equations over F) for which given D-n components of $\underline{Z}$ are zero. It is obvious that the "minimal" vector $\underline{Z}$ has to have at least D-n zero components, hence by searching among $\binom{D}{n}$ possible solutions we must encounter the minimal one! The complexity of the algorithm is of the order $\binom{D}{n}(D-n)n^2 \simeq \left(\frac{De}{n}\right)^n Dn^2$. The $\binom{D}{n}$ factor comes from the search. However, in practice, once more than (D-n) zeros in the vector $\underline{Z}$ have been found, many linear equations will not be repeated. Moreover, one puts a more restricted bound on the degree D, $(D \simeq N)$ whereas n will in general be a small number. Still the complexity of the algorithm is such that at this stage it should not be applied for $N > 20$. The generalization to many variables is straightforward (consider the space spanned by $\{x_1^{i_1}x_2^{i_2}\ldots x_t^{i_t}\}i_1\ldots i_t$). For non-principal ideals one obtains equations of the form $Z = \underline{P} + \sum_1^k \underline{\underline{P}}_i\,\underline{B}_i$. One has to choose a basis for all the columns appearing in the matrices $\underline{\underline{P}}_1,\ldots,\underline{\underline{P}}_k$ and repeat the above construction. In conclusion we have demonstrated the ability of an algebraic approach to "Let" statements to solve an "output" problem. At this stage however it is rather limited to polynomial domains in a few variables and of not large degree.

Example

We consider here two examples in the domain of polynomials in two variables x,z . A typical polynomial may be written as $P = \Sigma C_{ij}x^iz^j$. In a vector notation such a polynomial transforms to the vector $(C_{00}, C_{10}, C_{01}, \ldots)$, where the x^iz^j term corresponds to the $(i+j+1)\,(i+j)/2 + j + 1$ column. The two expressions we consider are:

$$Ex1 = x^4 + 4x^3 + 6x^2 + 4x - 4$$

$$Ex2 = 4x^3 + 6x^2 + 4x + 1$$

We shall seek an output of smallest complexity in the form $\sum C_{ij}x^iz^j$ with $i+j < 5$, having the side relation "LET x+1 = z" . In the previous notations, the polynomials Z, P become 21 dimensional vectors, the polynomial P_1 becomes 21×15 matrix and the polynomial B becomes a 15 dimensional vector.

In the linear equation $\underline{Z} = \underline{P} + \underline{\underline{P}}_1\cdot\underline{B}$, we may find solutions having at least 15 zero entries in $\underline{Z}$ if the corresponding rows in $\underline{\underline{P}}_1$ are linearly independent. Having done it,we find the following alternative forms for Ex1 and Ex2 respectively.

Ex1: $z^5 - xz^4 - 5,\ xz^4 + z^3 - 5,\ z^4 - 5$

Ex2: $z^5 - xz^4 - x^4,\ x + 3x^2z + z^3,\ z^4 - x^4$

Hence the desired output reads:

$$\begin{aligned} \text{Ex1} &= z^4 - 1 \\ \text{Ex2} &= z^4 - x^4 \\ z &= x + 1. \end{aligned}$$

An open problem

Let the complexity of an output be the sum of the complexities of the outputed expression and of the side relations.

Given a polynomial expression, introduce side relations (keeping the indeterminates in the polynomial algebraically independent) which will produce an output of minimal complexity!

References:

1. H. Kanoui and M. Bergman, "Generalized Substitution", preprint. To appear in Proceedings 4th International Colloquium on Algebraic Methods (Saint Maximin 1977).
2. B. Buchberger, ACM SIGSAM Bulletin,30 Aug.1976.
3. M. Lauer, "Canonical Representatives for Residue Classes of a Polynomial Ideal", Proceedings 1976 ACM Symposium on Symbolic and Algebraic Computation (R.D. Jenks, editor), (August 1976), pp. 339-345.
4. R. Shtokhamer, "A Canonical form of polynomials in the presence of side relations", Physics Dept., Technion, Haifa, Israel, Technion-PH-76-25, 1976.