Using Gröbner Bases for Detecting Polynomial Identities: A Case Study on Fermat's Ideal

BRUNO BUCHBERGER

Research Institute for Symbolic Computation,
Johannes Kepler University, A4040 Linz, Austria

AND

JUAN ELIAS

Department Algebra i Geometria, Universitat de Barcelona,
Gran Via 585, 08007 Barcelona, Spain

Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 41, No. 3, July 1992
Printed in Belgium

Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 41, No. 3, July 1992
Printed in Belgium

Using Gröbner Bases for Detecting Polynomial Identities: A Case Study on Fermat's Ideal

BRUNO BUCHBERGER

Research Institute for Symbolic Computation,
Johannes Kepler University, A4040 Linz, Austria

AND

JUAN ELIAS

Department Algebra i Geometria, Universitat de Barcelona,
Gran Via 585, 08007 Barcelona, Spain

Communicated by Hans Zassenhaus

Received April 2, 1991

We show that the Fermat polynomials $F_n := X^n + Y^n - Z^n$ satisfy the identity $F_{n+3} = -(S_0 F_n + S_1 F_{n+1} + S_2 F_{n+2})$, for all n, where the S_i are the elementary symmetric polynomials in three variables. A similar relation holds for the "generalized" Fermat polynomials $F_{m,n} := X_1^n + \cdots + X_{m-1}^n - X_m^n$. The proof of these identities is elementary as soon as the identities are conjectured. The main emphasis of the paper is on explaining a new method, based on the first author's Gröbner bases technique, by which such identities can be *generated*. © 1992 Academic Press, Inc.

1. INTRODUCTION

Let $F_n = X^n + Y^n - Z^n$ for all $n \geqslant 1$. In [C] a relation of the form

$$F_{n+3} = R_0 \cdot F_n + R_1 \cdot F_{n+1} + R_2 \cdot F_{n+2} \tag{1}$$

(for all $n \geqslant 1$, with rational functions R_0, R_1, R_2) was established by a complicated calculation involving certain determinants.

In this paper we show that, in fact, the much simpler relation,

$$F_{n+3} = -(S_0 \cdot F_n + S_1 \cdot F_{n+1} + S_2 \cdot F_{n+2}), \tag{2}$$

0022-314X/92 $5.00

holds, where

$$S_0 = -XYZ,$$
$$S_1 = XY + XZ + YZ,$$
$$S_2 = -(X + Y + Z),$$

are just the elementary symmetric polynomials.

With the convention $S_3 = 1$, this relation can be rewritten in the form

$$S_0 \cdot F_n + S_1 \cdot F_{n+1} + S_2 \cdot F_{n+2} + S_3 \cdot F_{n+3} = 0. \tag{3}$$

This result has some interesting consequences:

- It shows that the "Fermat ideal," i.e., the ideal generated by all F_n ($n \geqslant 3$) can be already generated by F_3, F_4, F_5. This follows from the above relation by inductively concluding that $F_6 \in (F_3, F_4, F_5)$, $F_7 \in (F_4, F_5, F_6)$, and hence $F_7 \in (F_3, F_4, F_5)$, and so on.
- It is furthermore interesting that the multipliers S_i needed in the representation of F_{n+3} in terms of F_n, F_{n+1}, F_{n+2} are polynomials with *integer* coefficients. Also, one can see that these multipliers do not depend on n.
- The fact that the multipliers S_i are so simple, namely the elementary symmetric polynomials over X, Y, Z, may allow us to draw conclusions for the solution of Fermat's problem, see [C].

Once the relation (2) is conjectured, the proof is very easy. Just expand the right-hand side of the equation (for indeterminate n) and verify that the result is equal to F_{n+3}.

The main emphasis, therefore, of this paper is not the actual relation but a general method, based on the Gröbner bases method introduced in [B-1], by which such polynomial identities can be detected. The present paper is an extension of [E-1, B-3].

We proceed in two steps reflecting the two approaches taken in [E-1, B-3] yielding increasing detail. The first approach (Section 2) uses the Gröbner bases technique as a "black box" as implemented in most of the current computer algebra software systems, for example, the Macaulay system. This approach yields the result that a relation of the form (1) with *polynomials* R_i must *exist*. It does not actually produce the polynomials R_i.

The second approach (Section 3) needs a "white box" Gröbner bases implementation, as provided, for example, by [B-3], that allows us to trace the actual steps of Gröbner bases calculations.

For an easy-to-read introduction into the Gröbner bases method, see [B-2].

This paper should also be seen as a case study that may motivate readers to apply the same technique for the invention of other polynomial identities.

2. Using Gröbner Bases for Hilbert Function Computation: Existence of a Polynomial Relation Between the F_n

The key tool used in this section is the computation of Hilbert functions of several graded algebras associated to the ideal of Fermat, by first computing Gröbner bases of these graded algebras and then using the formulae for Hilbert functions of Gröbner bases [B-1]. This method is implemented in the software system Macaylay, implemented by D. A. Bayer and M. Stillman [B-S].

This section is divided in two parts. In the first we compute the multiplicity of ring $\mathbb{Q}[X, Y, Z]/\mathscr{F}$. Since the multiplicity is invariant by field extensions we can do that with classical methods over $\mathbb{C}$.

The second part is devoted to compute the Hilbert function of $\mathbb{Q}[X, Y, Z]/\mathscr{F}$. For this we compute the Hilbert function of $\mathbb{Q}[X, Y, Z]/(F_3, F_4, F_5)$, and then we prove that both Hilbert functions are equal. From this it is easy to see that $(F_3, F_4, F_5) = \mathscr{F}$.

From now on we put $S = \mathbb{Q}[X, Y, Z]$. Let $A = \mathbf{k}[X, Y, Z]/I$ be a graded ring, with $\mathbf{k}$ a field. We will denote by A_n (resp. I_n) the nth graded piece of A (resp. I). We define the Hilbert function of A by $H_A(n) = \dim_{\mathbf{k}}(A_n)$, where A_n is the nth graded piece of A. Recall that if we have a field extension $\mathbf{k} \subset \mathbf{K}$ then $H_A = H_B$ where $B = A \otimes_{\mathbf{k}} K$.

It is well known that there exists a rational polynomial $P_A \in \mathbb{Q}[T]$, the Hilbert polynomial of A, such that $P_A(n) = H_A(n)$ for all $n \gg 0$. We will denote the regularity index of A by $i(A) = \operatorname{Min}\{n \mid \text{for all } t \geqslant n,\ H_A(t) = P_A(t)\}$ [Sch, E-2].

Since the Hilbert function remains constant by field extensions, in order to compute the multiplicity of $\mathbb{Q}[X, Y, Z]/\mathscr{F}$ we only need to compute the multiplicity of $\mathbb{C}[X, Y, Z]/\mathscr{F}$.

Proposition 2.1. *Let $\mathscr{X}$ be the projective $\mathbb{C}$-scheme* $\operatorname{Proj}(\mathbb{C}[X, Y, Z]/\mathscr{F})$. *Then the underlying set of $\mathscr{X}$ is* $\{(1, 0, 1), (0, 1, 1)\}$ *and each of these closed points has length* 3, *so $\mathscr{X}$ has multiplicity* 6.

Proof. Consider the $\mathbb{C}$-scheme $Y = \operatorname{Proj}(\mathbb{C}[X, Y, Z]/(F_3, F_4))$. It is easy to prove that the underlying set has four different points: $P = (1, 0, 1)$, $Q = (0, 1, 1)$, and two complex points. On the other hand, a straightforward computation gives us that the length of Y in P is 3. Thus if we denote by $\mathbf{m}$ the maximal ideal of $\mathscr{O}_{Y,P}$ we have that $\mathbf{m}^n = 0$ for all

$n \geqslant 3$. Hence we get $\mathcal{O}_{Z,P} = \mathcal{O}_{Y,P}$ and then the length of $\mathscr{X}$ in P is 3. A similar result holds for Q. Since the underlying set of $\mathscr{X}$ is $\{P, Q\}$ we obtain the result.

COROLLARY 2.1.1. *The ring* $\mathbb{Q}[X, Y, Z]/\mathscr{F}$ *has multiplicity* 6.

The first step is to compute the Hilbert function of $A = S/(F_3, F_4, F_5)$.

PROPOSITION 2.2. $\{H_A(n)\}_{n \geqslant 0} = \{1, 3, 6, 9, 11, 9, 7, 6, 6, ...\}$. *Hence the multiplicity of A is* 6 *and the regularity index is* 7.

Proof. This can be obtained by a basic feature of the Macaulay program [B-S, 3.7.1].

Remark 1. From Corollary 1.2 and Proposition 2.1 we deduce that $\mathscr{F}_n = (F_3, F_4, F_5)_n$ for all $n \gg 0$. Recall that we want to prove $\mathscr{F} = (F_3, F_4, F_5)$, so we need a deeper link between the Hilbert function of A and $\mathbb{Q}[X, Y, Z]/\mathscr{F}$. For this we will consider degree one superficial elements of A.

DEFINITION. Let D be a graded quotient of S. We say that an element L of D is superficial if and only if there exists an integer n_0 such that for all $n \geqslant n_0$, $D_n \xrightarrow[.L]{} D_{n+1}$ is an isomorphism. Note that L is a degree superficial element in this sense if and only if L is a superficial element of the local ring $D_{(x, y, z)}$ [Z-S, Vol. II, Chap. 8, Sect. 8]. For a degree one superficial element L of D we will consider the integer $q_D(L) = \operatorname{Min}\{n \geqslant 0 \mid \text{for all } t \geqslant n,\ D_t \xrightarrow[.L]{} D_{t+1} \text{ is an isomorphism}\}$.

Remark 2. Let L be a degree one superficial element of A. Since the Hilbert function of A takes values greater than its multiplicity, from [M, Proposition 12.10], we get that A is not Cohen–Macaulay. Hence in order to know $q_A(L)$ we can not apply [E-2, Proposition 1]. To avoid this we will use Macaulay.

PROPOSITION 2.3. *The coset of $X - Y$ in A is a degree one superficial element and the Hilbert function of $B = A/(x-y)$ is $\{H_B(n)\} = \{1, 2, 3, 3, 2, 1, 0, 0, ...\}$. In particular B is an Artinian algebra of multiplicity* 12 *and* $q_A(x-y) = 7$.

Proof. Using Macaulay we find the Hilbert function of B (see the proof of Proposition 2.2), in particular we get that $B_n = 0$, for all $n \geqslant 6$.

Consider the following exact sequence

$$A_r \xrightarrow[.(x-y)]{} A_{r+1} \to (A/(x-y))_{r+1} = B_{r+1} \to 0.$$

Since $B_n = 0$ for all $n \geqslant 6$ we get that

$$A_r \xrightarrow[.(x-y)]{} A_{r+1} \tag{4}$$

is epijective for all $r \geqslant 5$. Recall that the regularity index of A is 7 (Proposition 2.2). Thus we obtain that (4) is an isomorphism for all $n \geqslant 7$. From this we obtain the result.

PROPOSITION 2.4. *The coset of $X - Y$ in $\mathbb{Q}[X, Y, Z]/\mathscr{F}$ is a degree one superficial element and $q_{\mathbb{Q}[X, Y, Z]/\mathscr{F}}(x - y) = 7$. Moreover $H_A = H_{\mathbb{Q}[X, Y, Z]/\mathscr{F}}$.*

Proof. Let J be the ideal of S generated by $(F_n; n = 3, 4, ..., 7)$. If we compute the Hilbert function of S/J, we get that it is equal to the Hilbert function of A. Since $(F_3, F_4, F_5) \subset J$ we have $A = S/J$, so by Proposition 2.2 we obtain that $H_{S/J}(7) = 6$.

Let D be the ring $S/J + (x - y)$. Then we have $H_D(n) \leqslant H_B(n)$ for all $n \geqslant 0$. From Proposition 2.2 we get that $H_D(n) = 0$ for all $n \geqslant 6$. Hence if E is the ring $E = S/\mathscr{F} + (x - y)$ then we have $H_E(6) = H_D(6) = 0$, so $H_E(n) = 0$ for all $n \geqslant 6$. Consider the exact sequence

$$(S/\mathscr{F})_n \xrightarrow[.(x-y)]{} (S/\mathscr{F})_{n+1} \to E_{n+1} \to 0,$$

since $E_n = 0$ for all $n \geqslant 6$ we get that

$$(S/\mathscr{F})_n \xrightarrow[.(x-y)]{} (S/\mathscr{F})_{n+1} \tag{5}$$

is epijective for all $n \geqslant 5$. Recall that $H_{S/\mathscr{F}}(7) = H_{S/J}(7) = 6$, so by Corollary 2.1.1, (5) is an isomorphism for all $n \geqslant 7$. From this it is easy to deduce the claim.

PROPOSITION 2.5. *The set $\{F_3, F_4, F_5\}$ is a minimal basis of $\mathscr{F}$, in particular for all $n \geqslant 3$ there exist α_3^n, α_4^n, $\alpha_5^n \in \mathbb{Q}[X, Y, Z]$ such that $F_n = \sum_{i=3}^{5} F_i \alpha_i^n$.*

Proof. From $H_A = H_{\mathscr{S}/\mathscr{F}}$ (Proposition 2.4), we get $\mathscr{F} = (F_3, F_4, F_5)$. Since $\mathscr{F}$ is not Cohen–Macaulay (see Remark 2) we get that $\mathscr{F}$ is not a complete intersection. Hence a minimal basis of $\mathscr{F}$ has at least three elements, so we get the result.

3. Using Gröbner Bases for Actually Generating the Polynomial Relation

The result of the previous section can be made much more explicit by going into the details of Gröbner bases computations. Let G_n be a Gröbner basis for the ideal generated by F_n, F_{n+1}, F_{n+2}. We will show that F_{n+3} reduces to zero w.r.t. G_n. (This implies that F_{n+3} is in the ideal generated by F_n, F_{n+1}, F_{n+2}, see [B-2].) Subsequently, for obtaining S_1, S_2, S_3, one only has to "collect the multiples of F_n, F_{n+1}, F_{n+2}" that occur in the construction of the Gröbner basis and in the reduction of F_{n+3}. Below, we present this "calculation" with indeterminate n for $n \geqslant 4$. In fact it turns out that for $n \geqslant 4$ it is sufficient to construct the first *two* polynomials of G_n.

(For obtaining the idea for this approach to the solution of the problem, we computed the Gröbner bases for $n = 3, 4, 5, 10$ with the second author's Mathematica implementation of the Gröbner bases method, [B-4]. This implementation allows easy access to all intermediate steps for research purposes. One immediately sees a common pattern in the calculations and subsequently can come up with the derivation shown below for indeterminate n, which is valid for the case $n \geqslant 4$. From the general case with indeterminate n one can immediately conjecture identity (1) for arbitrary $n \geqslant 1$ and prove it. In this stage, of course, one can forget about the derivation by the Gröbner basis method.)

We document the steps of this derivation by the Gröbner bases method. Reduction of the S-Polynomial of F_n and F_{n+1} yields the polynomial

$$K_{n,4} = X \cdot F_n - F_{n+1}.$$

Reduction of the S-Polynomial of F_n and F_{n+2} yields the polynomial

$$\begin{aligned} K_{n,5} = X^2 \cdot F_n - F_{n+2} \\ - X \cdot K_{n,4} \\ - Y \cdot K_{n,4}. \end{aligned}$$

Reduction of F_{n+3} using F_n, F_{n+1}, F_{n+2}, $K_{n,4}$, $K_{n,5}$ yields

$$\begin{aligned} F_{n+3} - X^3 \cdot F_n \\ &+ X^2 \cdot K_{n,4} \\ &+ XY \cdot K_{n,4} \\ &+ X \cdot K_{n,5} \\ &+ Y^2 \cdot K_{n,4} \\ &+ Y \cdot K_{n,5} \\ &+ Z \cdot K_{n,5} \\ &= 0. \end{aligned}$$

From the above reductions one obtains the relations

$$K_{n,4}=X\cdot F_n-F_{n+1}+0\cdot F_{n+2},$$
$$K_{n,5}=-XY\cdot F_n+(X+Y)\cdot F_{n+1}-F_{n+2},$$
$$F_{n+3}=-(S_0\cdot F_n+S_1\cdot F_{n+1}+S_2\cdot F_{n+2}),$$

where

$$S_0=-XYZ,$$
$$S_1=XY+XZ+YZ,$$
$$S_2=-(X+Y+Z).$$

From (1) one may conjecture that a similar relation holds also in the case of more than three variables. In fact, for m variables we will prove the identity

$$F_{m,n+m}=-(S_{m,0}\cdot F_{m,n}+S_{m,1}\cdot F_{m,n+1}+\cdots+S_{m,m-1}\cdot F_{m,n+m-1}),$$

where

$$F_{m,n}=X_1^n+\cdots+X_{m-1}^n-X_m^n$$

and $S_{m,k}$ are the elementary symmetric polynomials in m variables, i.e.,

$$S_{m,0}=(-1)^m(X_1X_2\cdots X_m),$$
$$S_{m,1}=(-1)^{m-1}(X_1X_2\cdots X_{m-1}+X_1X_2\cdots X_{m-2}X_m$$
$$+\cdots+X_2X_3\cdots X_m),$$
$$\vdots$$
$$S_{m,m-2}=X_1X_2+X_1X_3+\cdots+X_{m-1}X_m,$$
$$S_{m,m-1}=-(X_1+X_2+\cdots+X_m).$$

This can be shown by elementary induction on m, see [B-3] or by the following easy derivation, which is due to the second author's student Istvan Nemes, see [N].

With the additional convention $S_{m,m}=1$ the general formula can be written in the compact form

$$\sum_{k=0}^{m} S_{m,k}\cdot F_{m,n+k}=0 \qquad \text{(for all } m\geqslant 1,\ n\geqslant 1). \tag{6}$$

We consider these relations as homogeneous linear recurrences with coefficients $S_{m,k}$, $0\leqslant k\leqslant m$. Since these relations are homogeneous, it is clear that the sum of two solutions and the product of a solution with a polynomial are again solutions, i.e., the solutions form a module over $\mathbb{Q}[X_1, ..., X_m]$. First, it is easy to see that, for $1 \leqslant j \leqslant m$,

$$\sum_{k=0}^{m} S_{m,k} \cdot X_j^k = 0.$$

This can be obtained by substituting X_j for x in the elementary identity

$$(x - X_1) \cdots (x - X_m) = \sum_{k=0}^{m} S_{m,k} \cdot x^k.$$

Now, (6) can be composed from these basic solutions by addition and multiplication with appropriate power products.

Acknowledgments

The first author's work on this paper was sponsored by the "Gröbner Bases Project" of the Austrian Ministry for Science and Research. I also thank my student W. Windsteiger for his help in preparing the manuscript.

The second author's work on this paper was partially sponsored by DGICYT PB88-0224.

References

[B-1] B. Buchberger, "An Algorithm for Finding a Basis for the Residue Class Ring for a Zero-Dimensional Polynomial Ideal," Ph.D. Thesis, Math. Inst., Univ. of Inssbruck, Austria, 1965.

[B-2] B. Buchberger, Gröbner bases: An algorithmic method in polynomial ideal theory, "Multidimensional Systems Theory" (N. K. Bose, Ed.), Chap. 6, pp. 184–232, Reidel, Dordrecht, 1985.

[B-3] B. Buchberger, "Fermat's Ideal Can Be Generated by the First Three Fermat Polynomials," RISC-Linz Tech. Rep. No. 90-44, 1990,

[B-4] B. Buchberger, "An Implementation of Gröbner Bases in Mathematica," RISC-Linz Tech. Rep. No. 90-58, 1990.

[B-S] D. A. Bayer and M. Stillman, Macaulay system and implementation, manual, 1986.

[C] J. C. Capdegelle, Sur une nouvelle approche du "dernier théorème" de Fermat, Manuscript, Paris, 1989.

[E-1] J. Elias, On Fermat's ideal, preprint, 1988.

[E-2] J. Elias, On the analytic equivalence of curves, *Math. Proc. Cambridge Philos. Soc.* **100** (1986), 57.

[M] E. Matlis, 1-Dimensional Cohen–Macaulay rings, *in* "Lecture Notes in Math.," Vol. 327, Springer-Verlag, New York/Berlin, 1977.

[N] I. Nemes, "Linear Recurrences with Symmetric Polynomial Coefficients," Tech. Rep., RISC-Institute, University of Linz, 1990.

[Sch] P. Schenzel, Uber die freien Auflösungen extremaler Cohen Macaulay Ringe, *J. Algebra* **64** (1980), 94–101.

[Z-S] O. Zariski and P. Samuel, "Commutative Algebra," Vols. I, II, Van Nostrand, Princeton, NJ, 1958, 1960.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium