STUDIA UNIV. BABEŞ-BOLYAI, MATHEMATICA, XXXVI, 3, 1991

FORMAL INTEGRATION OF CERTAIN CLASSES OF FUNCTIONS

DRAGOŞ POP[*]

Received: November 13, 1991
AMS subject classification: 68Q40

REZUMAT. - Integrarea formalǎ a unor clase de funcţii. Lucrarea prezintǎ o metodǎ de determinare analiticǎ a primitivei unei funcţii raţionale. Legat de aceasta, sînt expuşi şi algoritmi de manipulare simbolicǎ a polinoamelor precum şi de factorizare a polinoamelor peste Z[X]. Este descrisǎ de asemenea determinarea substituţiilor prin care problema integrǎrii funcţiilor din anumite clase se poate reduce la cazul raţional.

1. Introduction. The symbolic computation represents the entrance in a new computer usage era, in which the computer becomes smarter and powerful enough to do complex scientific computation, for example the formal integration. We can notice here the software packages for scientific computation MACSYMA, REDUCE, MATHCAD and MATHEMATICA.

In this paper we present the formal integration of rational functions with integer coefficients ($R(x)$) and related to this, the formal integration of functions from the classes R(exp) and R(sin, cos, tan) where the arguments of the exp, sin, cos and tan functions have the form kx with $k\in Z$.

With these algorithms I realized a Pascal program for IBM PC compatible computers running MS-DOS, which can be easily extended for larger classes of functions.

2. Substitutions. Since the problem of the formal integration of rational functions is simpler than the same problem for another function types, we try to reduce the given

[*] *University of Cluj-Napoca, Department of Mathematics and Computer Science, 3400 Cluj-Napoca, Romania*

function to a rational one by using suitable substitutions. For this reason the determination and the effectuation of the suitable substitution represents one of the most important part of a formal integration program.

In our case, we can apply the classical substitutions.

If the function belongs to the $R(\exp)$ class, the suitable substitution is $\exp(x) \to t$ and all the terms $\exp^m(nx)$ become t^{mn}.

If the function belongs to the $R(\sin, \cos, \tan)$ class we can transform the function to a equivalent function f from the $R(\sin, \cos)$ class. We have three cases:

$$f(-\sin, -\cos) = f(\sin, \cos)$$

$$f(-\sin, \cos) = -f(\sin, \cos)$$

$$f(\sin, -\cos) = -f(\sin, \cos)$$

The corresponding substitutions are $\tan(x) \to t$, $\cos(t) \to t$ and $\sin(x) \to t$. If our function doesn't verify any of these conditions, the suitable substitution is $\tan(x/2) \to t$.

Through these substitutions we transform our function in a $R(x)$ class function.

3. **The formal integration of a R(x) class function.** Suppose we have to integrate the function $f(x)=p(x)/q(x)$ where $p,q \in Z[x]$ are primitive polynomials, $\deg p(x) < \deg q(x)$ and $\gcd(p(x), ,q(x))=1$.

Obviously, every polynomial $q \in Z[x]$ has a unique squarefree decomposition:

$$q(x)=q_1(x)(q_2(x))^2 \ldots (q_k(x))^k$$

where $q_i \in Z[x]$ are squarefree polynomials (some of them can be constants 1) and $\gcd(q_i(x), q_j(x))=1$ for $1\le i, j\le k$ and $i\ne j$.

This decomposition can be obtained with Yun's algorithm described in section 4.

Using the simple fraction decomposition method, described in section 5, we obtain the polynomials $p_i(x)$ so that

$$\int\frac{p(x)}{q(x)}dx=\sum_{i=1}^{k}\int\frac{p_i(x)}{(q_i(x))^i}dx$$

Certainly, if $q_i(x)=1$ then $p_i(x)=0$.

In order to reduce the numerator's degree and to extract the rational part of the result we use the Hermite-Ostrogradsky method (described in section 6) and we determine the polynomials $s_i(x)$ and $r_i(x)$ for which:

$$\int\frac{p_i(x)}{(q_i(x))^i}dx=\frac{s_i(x)}{(q_i(x))^{i-1}}+\int\frac{r_i(x)}{q_i(x)}dx\quad 1<i\le k$$

In this moment, $\sum_{i=2}^{k}\frac{s_i(x)}{(q_i(x))^{i-1}}$ represents the rational part of the result. The remainder integrals will give us logarithmic or arctangent terms.

We need now the factorization of the polynomials q_i over $Z[x]$.

$$q_i(x)=q_{i1}(x)\ldots q_{in_i}(x)$$

where $q_{ij}(x)$ are irreducible polynomials over $Z[x]$.

This problem can be solved by using the Berlekamp-Hensel algorithm described in section 7.

Using again the simple fraction decomposition algorithm, we determine the polynomials $r_{ij}(x)$ for which:

$$\frac{r_i(x)}{q_i(x)} = \sum_{i=1}^{n_i} \frac{r_{ij}(x)}{q_{ij}(x)}$$

Now we have to compute $\int \frac{r_{ij}(x)}{q_{ij}(x)} dx \quad 1 \leq i \leq k, \quad 1 \leq j \leq n_i$. If $r_{ij}(x) = a * g'_{ij}(x)$ $(a \in Q)$ then the result is the logarithmic term $a \ln(q_{ij}(x))$. However, if deg $r_{ij}(x)$=deg $q_{ij}(x)-1$ we can extract a logarithmic term $\ln(q_{ij}(x))$ in order to reduce the degree of the numerator at the highest deg $s_{ij}(x)-2$.

If deg $q_{ij}(x)=2$ then we have an arctangent or a logarithmic term depending on the sign of the discriminant.

If deg $q_{ij}(x) \in \{3,4\}$ the equation $q_{ij}(x)$ can be solved through radicals and therefore we can factorize $q_{ij}(x)$ in a product of two polynomials of degree 1 or 2, over a radical extension of $Q[x]$.

If deg $q_{ij}(x)>4$ we shall search for a substitution in order to reduce the denominator's degree. Let's suppose we have to determine:

$$\int \frac{u(x)}{v(x)} dx$$

with $v \in Z[x]$ a irreducible polynomial over $Z[x]$, deg $v(x)>4$ and that we can effectuate the substitution $g(x) \rightarrow t$. In this situation there exist the polynomials $f,h \in Q[x]$ so that:

$$\frac{u(x)}{v(x)} = \frac{g'(x)\, f(g(x))}{h(g(x))}$$

If deg $g(x)$ = a then follows:

deg $u(x)$ = a-1+a deg $f(x)$

deg $v(x)$ = a deg $h(x)$

$$u(x) = g'(x)\ f(g(x))$$

$$v'(x) = g'(x)\ h'(g(x))$$

This relations shows that we can search $g'(x)$ (the derivative of the possible substitution $g(x)$) among the divisors of gcd($u(x)$, $v'(x)$) with the property that 1+deg $g'(x)$ = deg $g(x)$ divides gcd(1+deg $u(x)$, deg $v(x)$).

4. **The squarefree decomposition Yun's algorithm.** It is fairly easy to show that if $q\epsilon Z[x]$ and $q_i(x)$ is a polynomial such that it's roots are the i order roots of q, then $q_i\epsilon Z[x]$, all the roots of $q_i(x)$ have the order 1 and $(q_i(x))^i$ divides $q(x)$.

Let's suppose that all the roots of $q(x)$ have the order less or equal to $k\epsilon$N. In this case:

$$q(x)=q_1(x)\ \ (q_2(x))^2\ldots(q_k(x))^k.$$

Furthermore, since for $i\neq j$ $q_i(x)$ and $q_j(x)$ haven't common roots

$$\gcd(q_i(x),\ q_j(x)) = 1.$$

We can now see that:

$$q'(x) = q_1'(x)\ldots(q_k(x))^k+\ldots+kq_1(x)\ldots q_k'(x)\,(q_k(x))^{k-1}$$

$$c(x) = \gcd(q(x),q'(x)) = q_2(x)\,(q_3(x))^2\ldots(q_k(x))^{k-1}$$

$$r(x) = \frac{q(x)}{c(x)} = q_1(x)\,q_2(x)\ldots q_k(x)$$

$$s(x) = \gcd(c(x),r(x)) = q_2(x)\ldots q_k(x)$$

In this moment $q_1(x) = \dfrac{r(x)}{s(x)}$ and we see that making $q(x)$<- $c(x)$ and repeating the above operations until $q(x)$ become constant, we obtain the polynomials $q_1(x),\ldots,q_k(x)$. We also remark that $r,c,z\epsilon Z[x]$.

The above relations represent the mathematical basis of the

Yun's algorithm. The complete description can be found in [2].

5. **Simple fraction decomposition algorithm.** Assume $p,u,t \in Z[x]$ and $\gcd(u(x),t(x)) = 1$. This algorithm will compute the polynomial $r \in Q[X]$ so that:

$\frac{p(x)}{u(x)t(x)} = \frac{r(x)}{u(x)} + \frac{s(x)}{t(x)}$ and $\deg r(x) < \deg u(x)$, where $s \in Q[x]$ can be computed analogously.

From the above relation we obtain that:

$$p(x) = r(x)t(x) + u(x)s(x)$$

and

$$r(x) \equiv r(x) \bmod u(x).$$

This implies that:

$$\begin{aligned} p(x) \bmod u(x) &\equiv r(x)t(x) \bmod u(x) \\ &\equiv (r(x) \bmod u(x))\ (t(x) \bmod u(x)) \bmod u(x) \\ &\equiv r(x)\ (t(x) \bmod u(x)) \bmod u(x). \end{aligned}$$

Since $\gcd(u(x),\ t(x)) = 1$, there exist the polynomials $v,w \in Q[x]$ such that:

$$u(x)v(x) + w(x)t(x) = 1.$$

(The polynomials v and w can be computed using the Extended GCD Algorithm).

By dividing this relation by $u(x)$ we can see that:

$$w(x) \equiv t(x)^{-1} \bmod u(x)$$

and this tells us that

$$r(x) \equiv (p(x) \bmod u(x))\ w(x) \bmod u(x).$$

6. **The Hermite-Ostrogradski algorithm.** This algorithm computes the polynomials $a,b \in Q[x]$ so that:

$$\int \frac{p(x)}{(q(x))^n} dx = \frac{a(x)}{(q(x))^{n-1}} + \int \frac{b(x)}{q(x)} dx$$

where $p,q \in Z[x]$ and q is squarefree.

It is easy to show that $\gcd(q(x),q'(x)) = 1$ since q is squarefree. Therefore we can use the Extended GCD algorithm in order to determine the polynomials $v,w \in Q[x]$ so that:

$v(x)q'(x) + w(x)q(x) = 1.$

If we multiply this relation with $-p(x)/(n-1)$ and:

$s(x) = -\dfrac{p(x)\,v(x)}{n-1}, \quad t(x) = -p(x)\,w(x)$

we obtain that $s(x)q'(x) + \dfrac{t(x)\,q(x)}{n-1} = -\dfrac{p(x)}{n-1}$ and

$$-(n-1)s(x)q'(x) = p(x) + t(x)q(x).$$

Consequently,

$$\left[\frac{s(x) \cdot}{(q(x))^{n-1}}\right]' = \frac{s'(x)}{(q(x))^{n-1}} - \frac{(n-1)\,s(x)\,q'(x)}{(q(x))^n} =$$

$$= \frac{s'(x)}{(q(x))^{n-1}} + \frac{p(x)+t(x)\,q(x)}{(q(x))^n} = \frac{p(x)}{(q(x))^n} + \frac{s'(x)+t(x)}{(q(x))^{n-1}}$$

This means that if $r(x) = s'(x) + t(x)$ then

$$\int \frac{p(x)}{(q(x))^n} dx = \frac{s(x)}{(q(x))^{n-1}} - \int \frac{r(x)}{(q(x))^{n-1}} dx$$

It is now clear that using this algorithm for $n-1$ times, we will obtain

$$\int \frac{p(x)}{(q(x))^n} dx = \frac{s_1(x)}{(q(x))^{n-1}} + \ldots + \frac{S_{n-1}(x)}{(q(x))} + \int \frac{b(x)}{q(x)} dx$$

and thus $a(x) = s_1(x) + s_2(x)q(x) + \ldots + s_{n-1}(x)(q(x))^{n-2}$.

7. The Berlekamp-Hensel algorithm. Let $f(x) = a_n x^n + \ldots + a_1 x +$

$+ a_0$ be a squarefree and primitive polynomial with integer coefficients.

Also let

$$S = a_0^2+...+a_n^2$$

$$M(f) = 2^n S \qquad (1)$$

$$q \geq M(f),\ q \in Z$$

The algorithm presented here computes $r \in N$ and the polynomials $u_1, ..., u_r \in Z[x]$ irreducible over $Z[x]$, such that

$$f(x) = u_1(x)...u_r(x).$$

It can be prove that if $b \in Z[x]$, $b(x) = b_0+b_1x+...+b_sx^s$ and b divides f then $|b_i| < M(f)$ $i=0,s$. (see [4])

This means that if $b_i>0$ then

$$b_i = b_i \mod q \in \left(0, \frac{q}{2}\right).$$

and if $b_i < 0$ then

$$b_i \mod q = q-b_i \in \left(\frac{q}{2}, q\right) \qquad (2)$$

These observations lead us to the idea that the factorization of f over $Z_q[x]$ could be fairly closed to the factorization of f over $Z[x]$, since if

$$f(x) = p(x)t(x) \quad \text{with } p,t \in Z[x]$$

then

$$f(x) = p(x)t(x) \mod q$$

and according to (2) we can determine the coefficients of $p(x)$ mod q which correspond to negative coefficients of $p(x)$.

The Berlekamp-Hensel algorithm is based on these conclusions and it has the following steps:

S1) Determine a prime number p, the least possible, for which $\deg f(x) = n$ (q doesn't divide the leading coefficient of f) and f remain squarefree in $Z_p[x]$.

S2) Use the Berlekamp's algorithm (see [3]) for the factorization of $f(x)$ over $Z_p[x]$

$$f(x) \equiv u_1(x)\ldots u_s(x) \mod p$$

S3) Compute $M(f)$ given by (1).

S4) Pass from the factorization of f over $Z_p[x]$ to the factorization of f over $Z_{p^2}[x], \ldots, Z_q[x]$ using the formula given by the Hensel's lema (see [3]), until $q=p^k \geq 2M(f)$. This step computes the polynomials $u_{1k}, \ldots, u_{sk} \in Z_q[x]$ such that

$$f(x) \equiv u_{1k}(x)\ldots u_{sk}(x) \mod q$$

$$u_{ik}(x) \equiv u_i(x) \mod p, \quad i=1,s.$$

S5) Compute the product of each possible combination of $1,2,\ldots,s$ $u_{ik}(x)$ polynomials in $Z_q[x]$.

Normalise the coeficients of the product according to (2) by subtracting q from the coefficients greater than $\frac{q}{2}$.

If this normalised product divides f then it represents a factor of f and the $u_{ik}(x)$ polynomials which compose the product will be excluded from further combinations since f is squarefree.

Note that this is a polynomial time algorithm. There also exists the Kronecker's algorithm which is simpler and more intuitive but it requires exponential time and it become very inefficient for polynomials of degree greater than 5.

REFERENCES

1. Purdea,I., Pic,Gh., *Tratat de algebră modernă,* Editura Academiei, Bucureşti, (1977).
2. Davenport,J.H., *Integration Formelle,* Rapport de Recherche Nr. 375, Grenoble, (1983).
3. Knuth,D.E., *Tratat de programarea calculatoarelor.* Algoritmi seminumerici, Editura Tehnică, Bucureşti, (1983).
4. Buchberger,B., Collins,G., Loos,R., (eds), *Computer Algebra.* Symbolical and Algebraic Computation, Springer-Verlag, (1983).