Computer Algebra
Lecture 9

James Davenport

University of Bath

13 September 2018

Derivatives

Definition (Lecture 8 Slide 10)

The *derivative* of $f := \sum_{i=0}^{n} a_i x^i$ is $f' := \sum_{i=i}^{n} i a_i x^{i-1}$

Corollary

$(f+g)' = f' + g'$; $(fg)' = f'g + fg'$.

Definition (Alternative)

The derivative (with respect to x) satisfies $x' = 1$ and $(f+g)' = f' + g'$; $(fg)' = f'g + fg'$.

Corollary

The derivative of $f := \sum_{i=0}^{n} a_i x^i$ *is* $f' := \sum_{i=i}^{n} i a_i x^{i-1}$

Derivatives continued

Corollary

$\left(\frac{p}{q}\right)' = \frac{p'q-pq'}{q^2}$

Proof. [No calculus needed]

$$
\begin{aligned}
q\left(\frac{p}{q}\right) &= p \\
q'\left(\frac{p}{q}\right) + q\left(\frac{p}{q}\right)' &= p' \\
q\left(\frac{p}{q}\right)' &= p' - q'\left(\frac{p}{q}\right) = \frac{p'q-pq'}{q} \\
\left(\frac{p}{q}\right)' &= \frac{p'q-pq'}{q^2}
\end{aligned}
$$

Integrals

Notation (Fundamental Theorem of Calculus)

(Indefinite) integration is the inverse of differentiation, i.e.

$$F = \int f \Leftrightarrow F' = f. \tag{1}$$

"Where did $\mathrm{d}x$ go?", but x is, from this point of view, merely that object such that $x' = 1$, i.e. $x = \int 1$.

Proposition

If $\theta = \mathrm{RootOf}(p(z))$ *with* $p = \sum_{i=0}^{n} a_i z^i$, *then* $\theta' = -\frac{\sum_{i=0}^{n} a_i' \theta^i}{\sum_{i=0}^{n} i a_i \theta^{i-1}}$.

Integration of Rational Functions

The integration of polynomials is trivial:

$$\int \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} \frac{1}{i+1} a_i x^{i+1}. \tag{2}$$

Since any rational expression $f(x) \in K(x)$ can be written as

$$f = p + \frac{q}{r} \text{ with } \left\{ \begin{array}{l} p, q, r \in K[x] \\ \deg(q) < \deg(r) \end{array} \right. , \tag{3}$$

and p is always integrable by (2), we have proved

Proposition (Decomposition Lemma (rational expressions))

In the notation of (3), f is integrable if, and only if, q/r is.

$\frac{q}{r}$ is a *proper rational*.

Integration of Proper Rationals

In fact, the integration of proper rational expressions is conceptually trivial (we may as well assume r is monic, absorbing any constant factor in q):

1. perform a square-free decomposition of $r = \prod_{i=1}^{n} r_i^i$;
2. factorize each r_i completely, as $r_i(x) = \prod_{j=1}^{n_i}(x - \alpha_{i,j})$;
3. perform a partial fraction decomposition of q/r as

$$\frac{q}{r} = \frac{q}{\prod_{i=1}^{n} r_i^i} = \sum_{i=1}^{n} \frac{q_i}{r_i^i} = \sum_{i=1}^{n} \sum_{j=i}^{n_i} \sum_{k=1}^{i} \frac{\beta_{i,j,k}}{(x - \alpha_{i,j})^k}; \qquad (4)$$

4. integrate this term-by-term, obtaining

$$\int \frac{q}{r} = \sum_{i=1}^{n} \sum_{j=i}^{n_i} \sum_{k=2}^{i} \frac{-\beta_{i,j,k}}{(k-1)(x - \alpha_{i,j})^{k-1}} + \sum_{i=1}^{n} \sum_{j=i}^{n_i} \beta_{i,j,1} \log(x - \alpha_{i,j}). \qquad (5)$$

Problems?

From a practical point of view, this approach has several snags:

1. we have to factor r, and even the best algorithms from the previous chapter can be expensive;
2. we have to factor each r_i *into linear factors*, which might necessitate the introduction of algebraic numbers to represent the roots of polynomials;
3. These steps might result in a complicated expression of what is otherwise a simple answer.

These are practical problems

$$\int \frac{5x^4 + 60x^3 + 255x^2 + 450x + 274}{x^5 + 15x^4 + 85x^3 + 225x^2 + 274x + 120} \mathrm{d}x$$
$$= \log(x^5 + 15x^4 + 85x^3 + 225x^2 + 274x + 120)$$
$$= \log(x + 1) + \log(x + 2) + \log(x + 3) + \log(x + 4) + \log(x + 5) \tag{6}$$

is pretty straightforward, but adding 1 to the numerator gives

$$\int \frac{5x^4 + 60x^3 + 255x^2 + 450x + 275}{x^5 + 15x^4 + 85x^3 + 225x^2 + 274x + 120} \mathrm{d}x$$
$$= \frac{5}{24} \log(x^{24} + 72x^{23} + \cdots + 102643200000x + 9331200000)$$
$$= \frac{25}{24} \log(x + 1) + \frac{5}{6} \log(x + 2) + \frac{5}{4} \log(x + 3) + \frac{5}{6} \log(x + 4) + \frac{25}{24} \log(x \tag{7}$$

Adding 1 to the denominator is pretty straightforward,

$$\int \frac{5x^4+60x^3+255x^2+450x+274}{x^5+15x^4+85x^3+225x^2+274x+121}\mathrm{d}x = \log(x^5+15x^4+85x^3+225x^2+274x+121), \tag{8}$$

but adding 1 to both gives

$$\int \frac{5x^4+60x^3+255x^2+450x+275}{x^5+15x^4+85x^3+225x^2+274x+121}\mathrm{d}x = 5\sum_{\alpha} \alpha \ln\Big(x+\frac{2632025698}{289}\alpha^4-\frac{2086891452}{289}\alpha^3+ \frac{608708804}{289}\alpha^2-\frac{4556915}{17}\alpha+\frac{3632420}{289}\Big), \tag{9}$$

where

$$\alpha = \mathrm{RootOf}\left(38569\,z^5-38569\,z^4+15251\,z^3-2981\,z^2+288\,z-11\right). \tag{10}$$

The challenge

Hence the challenge is to produce an algorithm that achieves (6) and (8) simply, preferably gives us the second form of the answer in (7), *but* is still capable of solving (9).
We might also wonder where (9) came from: see later.

We can write our integral as

$$\int \frac{q}{r} = \frac{s_1}{t_1} + \int \frac{s_2}{t_2}, \tag{11}$$

where the integral on the right-hand resolves itself as *purely* a sum of logarithms, i.e. is the $\sum_{i=1}^{n} \sum_{j=i}^{n_i} \beta_{i,j,1} \log(x - \alpha_{i,j})$ term.
Galois Theory shows that (11) can be written without any α_i: Can we find it without involving them?
We can perform a square-free decomposition of r as $\prod r_i^i$, and then a partial fraction decomposition to write

$$\frac{q}{r} = \sum \frac{q_i}{r_i^i} \tag{12}$$

and, since each term is a rational expression and therefore integrable, it suffices to integrate (12) term-by-term.

Hermite's Algorithm continued

Now r_i and r_i' are relatively prime, so, by Extended Euclid, there are polynomials a and b satisfying $ar_i + br_i' = 1$. Therefore

$$\begin{aligned}
\int \frac{q_i}{r_i^i} &= \int \frac{q_i(ar_i + br_i')}{r_i^i} &(13)\\
&= \int \frac{q_i a}{r_i^{i-1}} + \int \frac{q_i b r_i'}{r_i^i} &(14)\\
&= \int \frac{q_i a}{r_i^{i-1}} + \int \frac{(q_i b/(i-1))'}{r_i^{i-1}} - \left(\frac{q_i b/(i-1)}{r_i^{i-1}}\right)' &(15)\\
&= -\left(\frac{q_i b/(i-1)}{r_i^{i-1}}\right) + \int \frac{q_i a + (q_i b/(i-1))'}{r_i^{i-1}}, &(16)
\end{aligned}$$

and we have reduced the exponent of r_i by one.

When programming this method one may need to take care of the fact that, while $\frac{q_i}{r_i^i}$ is a proper rational expression, $\frac{q_i b}{r_i^{i-1}}$ may not be, but the excess is precisely compensated for by the other term in (16).

Hence, at the cost of a square-free decomposition and a partial fraction decomposition, but *not* a factorization, we have found the rational part of the integral, i.e. performed the decomposition of (11).

In fact, we have done somewhat better, since the $\int \frac{s_2}{t_2}$ term will have been split into summands corresponding to the different r_i.

It follows from (16) that, in the notation of (12) $t_1 = \prod r_i^{i-1}$. Furthermore every factor of t_2 arises from the r_i, and is not repeated. Hence we can choose

$$t_1 = \gcd(r, r') \text{ and } t_2 = r/t_1. \tag{17}$$

Having done this, we can solve for the coefficients in s_1 and s_2, and the resulting equations are linear in the unknown coefficients. More precisely, the equations become

$$q = s_1' \frac{r}{t_1} - s_1 \frac{t_1' t_2}{t_1} + s_2 t_1, \tag{18}$$

where the polynomial divisions are exact, and the linearity is now obvious. The programmer should note that s_1/t_1 is guaranteed to be in lowest terms, but s_2/t_2 is not (and indeed will be 0 if there is no logarithmic term)

The Trager–Rothstein Algorithm [Rot76, Tra76]

We still have to integrate the logarithmic part. (6)–(9) shows that this may, but need not, require algebraic numbers. How do we tell? The answer is provided by the following observation; if we write the integral of the logarithmic part as $\sum c_i \log v_i$, we can determine the equation satisfied by the c_i, i.e. the analogue of (10), by purely rational computations.

So write

$$\int \frac{s_2}{t_2} = \sum c_i \log v_i, \tag{19}$$

where we can assume

1. $\frac{s_2}{t_2}$ is in lowest terms;
2. the v_i are polynomials (using $\log \frac{f}{g} = \log f - \log g$);
3. the v_i are square-free (using $\log \prod f_i^i = \sum i \log f_i$);
4. the v_i are relatively prime (using $c \log pq + d \log pr = (c + d) \log p + c \log q + d \log r$);
5. the c_i are all different (using $c \log p + c \log q = c \log pq$);
6. the c_i generate the smallest possible extension of the original

The Trager–Rothstein Algorithm (continued)

(19) can be rewritten as

$$\frac{s_2}{t_2} = \sum c_i \frac{v_i'}{v_i}. \tag{20}$$

Hence $t_2 = \prod v_i$ and, writing $u_j = \prod_{i \neq j} v_i$, we can write (20) as

$$s_2 = \sum c_i v_i' u_i. \tag{21}$$

Furthermore, since $t_2 = \prod v_i$, $t_2' = \sum v_i' u_i$. Hence

$$\begin{aligned}
v_k &= \gcd(0, v_k) \\
&= \gcd\left(s_2 - \sum c_i v_i' u_i, v_k\right) \\
&= \gcd\left(s_2 - c_k v_k' u_k, v_k\right) \\
&\qquad \text{since all the other } u_i \text{ are divisible by } v_k \\
&= \gcd\left(s_2 - c_k \sum v_i' u_i, v_k\right) \\
&\qquad\qquad\qquad \text{for the same reason} \\
&= \gcd\left(s_2 - c_k t_2', v_k\right).
\end{aligned}$$

But if $l \neq k$,

$$\begin{aligned}\gcd\left(s_2 - c_k t_2', v_l\right) &= \gcd\left(\sum c_i v_i' u_i - c_k \sum v_i' u_i, v_l\right)\\ &= \gcd\left(c_l v_l' u_l - c_k v_l' u_l, v_l\right)\\ &\quad \text{since all the other } u_i \text{ are divisible by } v_l\\ &= 1.\end{aligned}$$

Since $t_2 = \prod v_l$, we can put these together to deduce that

$$v_k = \gcd(s_2 - c_k t_2', t_2). \tag{22}$$

Given c_k, this will tell us v_k. But we can deduce more from this: the c_k are precisely those numbers λ such that $\gcd(s_2 - \lambda t_2', t_2)$ is non-trivial. Hence t λ must be such that

$$P(\lambda) := \mathrm{Res}_x(s_2 - \lambda t_2', t_2) = 0. \tag{23}$$

If t_2 has degree n, $P(\lambda)$ is the determinant of a $2n-1$ square matrix, n of whose rows depend linearly on λ, and thus is a polynomial of degree n in λ.

Complex Numbers?

The same process also leads to

$$\int \frac{1}{x^2+1}\mathrm{d}x = \frac{i}{2}\left(\ln\left(1-ix\right)-\ln\left(1+ix\right)\right), \qquad (24)$$

at which point the reader might complain "I asked to integrate a *real* function, but the answer is coming back in terms of *complex* numbers". The answer is, of course, *formally correct*: differentiating the right-hand side of (24) yields

$$\frac{i}{2}\left(\frac{-i}{1-ix}-\frac{i}{1+ix}\right)=\frac{i}{2}\left(\frac{-i(1+ix}{1+x^2}-\frac{i(1-ix)}{1+x^2}\right)=\frac{1}{1+x^2}:$$

the issue is that the reader, *interpreting* the symbols log etc. as the usual functions of calculus, is surprised.

Bibliography I

M. Rothstein.
Aspects of Symbolic Integration and Simplification of Exponential and Primitive Functions.
PhD thesis, Univ. of Wisconsin, 1976.

B.M. Trager.
Algebraic Factoring and Rational Function Integration.
In R.D. Jenks, editor, *Proceedings SYMSAC 76*, pages 219–226, 1976.