Symbolic Integration

Victor Adamchik

Carnegie Mellon University

Squarefree Factorization

Integration - the main idea

The idea is to find $a, \ b, \ c, \ d \in F[x]$ such that

$$\int \frac{p}{q}\, dx = \frac{c}{d} + \int \frac{a}{b}\, dx$$

where $\deg(a) < \deg(b)$ and b is squarefree ($i.e.$ $\mathrm{GCD}(b, \ b') = 1$).

In other words, we split the integral into a rational and logarithmic parts.

We compute as much of integrand as possible in a given field and then compute the minimal extension (algebraic and/or log) necessary to express the integral.

The algorithm proceeds as follows. Applying Euclidean division

$$p = q * s + r,$$

$$\gcd(r, \ q) = 1, \ \ \deg(r) < \deg(q)$$

or

$$\frac{p}{q} = s + \frac{r}{q}$$

we have

$$\int \frac{p}{q} = \int s + \int \frac{r}{q}$$

Polynomial integration $\int s$ is trivial. We compute the squarefree factorization of q

$$q = q_1 * q_2{}^2 * \ldots q_m{}^m$$

$$\int \frac{r}{q} = \int \frac{r}{q_1 * q_2{}^2 * \ldots q_m{}^m}$$

where $m \geq 2$ (otherwise, q is squarefree). The next step is to decrease the degree of a denominator

$$\int \frac{1}{q_1 * q_2{}^2 * \ldots q_m{}^{\mathbf{m}}} \to \int \frac{1}{q_1 * q_2{}^2 * \ldots q_m{}^{\mathbf{m-1}}} \to \ldots \to \int \frac{1}{q_1 * q_2 * \ldots q_m}$$

Hermite-Ostrogradsky's Algorithm reduces exponents of each irreducible q_k to 1

We compute as much of integrand as possible in a given field and then compute the minimal extension (algebraic and/or log) necessary to express the integral.

Squarefree Factorization

Definition. We say that f is *squarefree* if it has no proper quadratic divisors.

Definition.The *squarefree factorization* of $f(x)$ is

$$f(x) = \prod_{k=1}^{n} g_k(x)^k = g_1(x)\, g_2(x)^2\, g_3(x)^3 \ldots g_n(x)^n$$

where each g_i is a squarefree polynomial and $\mathrm{GCD}(g_i,\ g_k) = 1$

The squarefree part of a polynomial can be calculated without actually factoring the polynomial into irreducibles. We will see how to do this for fields of characteristic zero.

Definition. A field F is of characteristic zero, if for all $a \in F$, $a \neq 0$ and $n \in \mathbb{Z}$, $n \neq 0$ we have $n\, a \neq 0$.

Lemma. Let F be a field of characteristic zero. Then f is square-free $\Longleftrightarrow \mathrm{GCD}(f,\ f') = 1$.

Example. Consider

$$f = x^6 + 2\, x^3 + 1$$

over Z_3.

$$D(f) = 6\, x^5 + 6\, x^2 = 0 \ (\mathrm{mod}\ 3)$$

■ Squarefree factorization algorithm

This is Musser's algorithm originall presented in

D. R. Musser, *Algorithms for Polynomial Factorization*, Ph.D. thesis, University of Wisconsin, 1971.

Take

$$f(x) = \prod_{k=1}^{n} g_k(x)^k$$

find derivative

$$f'(x) = \sum_{k=1}^{n} g_1(x) \ldots k\, g_k(x)^{k-1}\, g_k'(x) \ldots g_n(x)$$

Hence

$$c(x) = \mathrm{GCD}(f(x),\ f'(x)) = \prod_{k=2}^{n} g_k(x)^{k-1}$$

Then

$$w(x) = \frac{f(x)}{\mathrm{GCD}(f(x),\ f'(x))} = \prod_{k=1}^{n} g_k(x)$$

is a product of squarefree factors. Calculating (if $c(x)$ is not 1, because otherwise $f(x)$ is squarefree)

$$y(x) = \mathrm{GCD}(c(x),\ w(x)) = \prod_{k=2}^{n} g_k(x)$$

and observing that

$$g_1(x) = \frac{w(x)}{y(x)}$$

or

$$g_1(x) = \frac{\frac{f(x)}{c(x)}}{\mathrm{GCD}\left(c(x),\ \frac{f(x)}{c(x)}\right)}$$

we find the first squarefree factor.

To find $g_2(x)$, we observe that it is the first factor of $c(x)$. Thus

$$f(x) \longleftarrow c(x)$$

$$\text{new\_c}\,(x) = \mathrm{GCD}(c(x),\ c'(x)) = \prod_{k=3}^{n} g_k(x)^{k-2} = \frac{c(x)}{y(x)}$$

$$w(x) = \frac{c(x)}{\mathrm{GCD}(c(x),\ c'(x))} = \frac{c(x)}{\text{new\_c}\ (x)} = \frac{c(x)}{\frac{c(x)}{y(x)}} = y(x)$$

In short

$$c(x) = \frac{c(x)}{y(x)}$$

$$w(x) = y(x)$$

$$y(x) = \mathrm{GCD}(c(x),\ w(x))$$

$$g_2(x) = \frac{w(x)}{y(x)}$$

Applying these recursively, we find all g_k

■ **Example.**

$$f(x) = x^9 + x^8 - 2\,x^7 - 2\,x^6 + 2\,x^3 + 2\,x^2 - x - 1$$

$$f'(x) = 9\,x^8 + 8\,x^7 - 14\,x^6 - 12\,x^5 + 6\,x^2 + 4\,x - 1$$

$$c(x) = \mathrm{GCD}(f(x),\ f'(x)) = x^5 + x^4 - 2\,x^3 - 2\,x^2 + x + 1$$

```
PolynomialGCD[x^9 + x^8 - 2 x^7 - 2 x^6 + 2 x^3 + 2 x^2 - x - 1,
 9 x^8 + 8 x^7 - 14 x^6 - 12 x^5 + 6 x^2 + 4 x - 1]
```

$$w(x) = \frac{f(x)}{\mathrm{GCD}(f(x),\ f'(x))} = x^4 - 1$$

Entering the main loop: $k = 1$

$$y(x) = \mathrm{GCD}(c(x),\ w(x)) = x^2 - 1$$

```
PolynomialGCD[x^5 + x^4 - 2 x^3 - 2 x^2 + x + 1, x^4 - 1]
```

$$g_1(x) = \frac{w(x)}{y(x)} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1$$

$$w(x) \longleftarrow y(x) = x^2 - 1$$

$$c(x) \longleftarrow \frac{c(x)}{y(x)} = x^3 + x^2 - x - 1$$

Entering the main loop: $k = 2$

$$y(x) = \mathrm{GCD}(c(x),\, w(x)) = x^2 - 1$$

$$g_2(x) = \frac{w(x)}{y(x)} = 1$$

$$w(x) \longleftarrow y(x) = x^2 - 1$$

$$c(x) \longleftarrow \frac{c(x)}{y(x)} = x + 1$$

Entering the main loop: $k = 3$

$$y(x) = \mathrm{GCD}(c(x),\, w(x)) = x + 1$$

$$g_3(x) = \frac{w(x)}{y(x)} = x - 1$$

$$w(x) \longleftarrow y(x) = x + 1$$

$$c(x) \longleftarrow \frac{c(x)}{y(x)} = 1$$

Since $c(x) = 1$, we stop and return $\left(x^2 + 1\right) * 1 * (x - 1)^3 * (x + 1)^4$

Code

```
factorsquareFree[pol_, x_] :=
 Module[{f, fpr, c, w, y, g, k},
   f = pol;
   fpr = D[pol, x];
   c = PolynomialGCD[f, fpr];
   w = PolynomialQuotient[f, c, x];
   out = k = 1;
   While[c =!= 1,
     y = PolynomialGCD[c, w];
     g = PolynomialQuotient[w, y, x];
     out *= g^k;
     k++;
     w = y;
     c = PolynomialQuotient[c, y, x];
   ];
    out *= w^k
  ] /; PolynomialQ[pol, x]
```

Z_p

If the polynomial is in $Z_p[x]$, the situation is slightly more complex.

Compute

$$c(x) = \text{GCD}(f(x),\ f'(x))$$

There are choices

$c(x) = 1$ then $f(x)$ is squrefree

$c(x) \neq 1$ and $c(x) \neq f(x)$ then we continue with the algorithm...

$c(x) \neq 1$ and $c(x) = f(x)$ and this is what makes a difference! We must have $f'(x) = 0$. Therefore, $f(x)$ contains exponents that are multiple of p. We can write $f(x) = b(x)^p$ and reduce problem to squarefree factorization of $b(x)$.

The algorithm was presented by Akritas in

A. G.. Akritas, *Elements of computer algebra with applications*, Wiley, NY, 1989.

Exercise

Let $p(x) = 112\,x^4 + 58\,x^3 - 31\,x^2 + 107\,x - 66$. What is the squarefree factorization modulo 3?

Compare

```
FactorSquareFree[112 x^4 + 58 x^3 - 31 x^2 + 107 x - 66]
```

$$-66 + 107\,x - 31\,x^2 + 58\,x^3 + 112\,x^4$$

with

```
FactorSquareFree[112 x^4 + 58 x^3 - 31 x^2 + 107 x - 66, Modulus → 3]
```

$$x\,(1 + x)^2\,(2 + x)$$

We proceed as in Musser's algorithm

```
f := 112 x^4 + 58 x^3 - 31 x^2 + 107 x - 66
```

```
c = PolynomialGCD[f, D[f, x], Modulus → 3]
```

```
1 + x
```

$$w(x) = \frac{f(x)}{c(x)}$$

```
w = PolynomialQuotient[f, c, x, Modulus → 3]
```

```
2 x + x^3
```

Entering the main loop: $k = 1$

$$y(x) = \text{GCD}(c(x),\ w(x))$$

```
y  = PolynomialGCD[c, w, Modulus → 3]
```

```
1 + x
```

$$g_1(x) = \frac{w(x)}{y(x)}$$

```
g1 = PolynomialQuotient[w, y, x, Modulus → 3]
```

```
2 x + x^2
```

$$w(x) \longleftarrow y(x)$$

$$c(x) \longleftarrow \frac{c(x)}{y(x)}$$

```
w = y; c = c/y
```

Since $c(x) = 1$, stop and return `g1[x] w[x]^2`

Yun's squar-free factorization in characteristic zero.

Yun presented a more efficient algorithm

D. Y. Yun, On square-free decomposition algorithms, *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation*, (1976), pp. 26-25.

Take

$$f(x) = \prod_{k=1}^{n} g_k(x)^k$$

find derivative

$$f'(x) = \sum_{k=1}^{n} g_1(x) \ldots k\, g_k(x)^{k-1}\, g_k{}'(x) \ldots g_n(x)$$

Hence

$$c(x) = \mathrm{GCD}(f(x),\ f'(x)) = \prod_{k=2}^{n} g_k(x)^{k-1}$$

Then

$$w(x) = \frac{f(x)}{\mathrm{GCD}(f(x),\ f'(x))} = \prod_{k=1}^{n} g_k(x)$$

is a product of square-free factors. No difference so far with the previous algorithm.

We compute $y(x)$ in a different way

$$y(x) = \frac{f'(x)}{c(x)} = \frac{f'(x)}{\mathrm{GCD}(f(x),\ f'(x))}$$

$$y(x) = g_1{}'(x) \ldots g_n(x) + 2\, g_1(x)\, g_2{}'(x) \ldots g_n(x) + \ \ldots\ + n\ g_1(x) \ldots g_{n-1}(x)\, g_n{}'(x)$$

We must eliminate the first term! It contains $g_1{}'(x)$.

Elimination can be done by means of $w'(x)$:

$$y(x) - w'(x) = g_1(x)[g_2{}'(x) \ldots g_n(x) + (n-1)\, g_2(x) \ldots g_n{}'(x)]$$

Therefore, we find the first squarefree factor as

$$g_1(x) = \mathrm{GCD}(w(x),\ \ y(x) - w'(x))$$

Note that $g_2{}'(x) \ldots g_n(x) + (n-1)\, g_2(x) \ldots g_n{}'(x)$ is not divisible by $w(x)$, since each g_i is a square-free polynomial with $\mathrm{GCD}(g_k,\ g_k{}') = 1$.

To find $g_2(x)$, we do the following

$$\text{new\_w}\,(x) = \frac{w(x)}{g_1(x)}$$

$$\text{new\_y}\,(x) = \frac{y(x) - w'(x)}{g_1(x)}$$

$$\text{new\_y}\,(x) - \text{new\_w}'\,(x) \ldots$$

and so on...

Code

```
YunFactorSquareFree[pol_, x_] :=
 Module[{f, fpr, c, w, y, g, k, out},
   f = pol; fpr = D[pol, x];
    c = PolynomialGCD[f, fpr];
    w = PolynomialQuotient[f, c, x];
    y = PolynomialQuotient[fpr, c, x];
    out = k = 1;
    z =  y - D[w, x];
    While[z =!= 0,
       g = PolynomialGCD[w, z];
       out *= g^k;
       k++;
       w = PolynomialQuotient[w, g, x];
       y = PolynomialQuotient[z, g, x];
       z = y - D[w, x];
     ];
     out *= w^k
  ] /; PolynomialQ[pol, x]
```

Hermite-Ostrogradsky's Algorithm

E. Hermite, Sur l'intégration des fractions rationelles, *Nouvelles Annales de Mathématiques*, **11**(1872), 145-148.

M. W. Ostrogradsky, De l'intégration des fractions rationelles, *Bulletin de la Classe Physico-Mathématiques de l'Académie Impériale des Sciences de St. Pétersburg*, IV, 1845, pp.145-167, 286-300.

Given

$$\int \frac{p}{q}\, dx$$

where $\deg(p) < \deg(q)$ and $\mathrm{GCD}(p,\ q) = 1$. The idea of the algorithm is to find $a,\ b \in F[x]$ such that

$$\int \frac{p}{q}\,dx = \text{Rational\_Function} + \int \frac{a}{b}\,dx$$

where b is squarefree. We will use another algorithm to compute $\int \frac{a}{b}\,dx$.

We start with computing a squarefree factorization of q

$$q = q_1 * {q_2}^2 * \ldots {q_m}^m$$

where $m \geq 2$ (otherwise, q is squarefree):

$$\int \frac{p}{q} = \int \frac{p}{q_1 * {q_2}^2 * \ldots {q_m}^m}$$

Hermite-Ostrogradsky's algorithm reduces exponents of each irreducible q_k to 1

$$\int \frac{1}{q_1 * {q_2}^2 * \ldots {q_m}^{\mathbf{m}}} \to \int \frac{r_1}{q_1 * {q_2}^2 * \ldots {q_m}^{\mathbf{m-1}}} \to \ldots \to \int \frac{r_k}{q_1 * q_2 * \ldots q_m}$$

The algorithm proceeds as follows. Let

$$q \;=\; q_1 * {q_2}^2 * \ldots {q_m}^m$$

$$v \;=\; q_m$$

$$u \;=\; \frac{q}{v^m} = q_1 * {q_2}^2 * \ldots {q_{m-1}}^{m-1}$$

Since

$$\text{GCD}(u\;v',\,v) \;=\; \text{GCD}\big(q_1 * {q_2}^2 * \ldots {q_{m-1}}^{m-1}\,{q_m}',\;q_m\big) \;=\; 1$$

using the extended Euclidean algorithm we find $a,\ b \in F[x]$ such that

$$p \;=\; u\,v'\,a \;+\; v\,b, \qquad \deg(a) \;\leq\; \deg(v) - 1$$

See the proof below. Dividing both parts by $q = u * v^m$ gives

$$\frac{p}{q} = \frac{a\,v'}{v^m} + \frac{b}{u\,v^{m-1}} \tag{1}$$

Next we observe that

$$\frac{a\;v'}{v^m} = \frac{1}{1-m}\left[\left(\frac{a}{v^{m-1}}\right)' - \frac{a'}{v^{m-1}}\right]$$

Thus, equation (1) can be rewritten as

$$\frac{p}{q} = \frac{1}{1-m}\left(\left(\frac{a}{v^{m-1}}\right)' - \frac{a'}{v^{m-1}}\right) + \frac{b}{u\,v^{m-1}}$$

or

$$\frac{p}{q} = \frac{1}{1-m}\left(\frac{a}{v^{m-1}}\right)' + \frac{1}{1-m} * \frac{b\,(1-m) - a'\,u}{u\,v^{m-1}}$$

Integrating both sides, yields

$$\int \frac{p}{q} = \frac{1}{1-m}\,\frac{a}{v^{m-1}} + \frac{1}{1-m}\int \frac{b\,(1-m) - u\,a'}{u\,v^{m-1}}$$

The integrand is reduced to one with a smaller multiplicity. We repeat this process until the denominator is squarefree.

■ Theorem

Let $a,\ b \in\ F[x]$ and $GCD(a, b) = 1$. Then for any given polynomial $c \in\ F[x]$ there exist unique polynomials σ and $\tau \in\ F[x]$ such that

$$\sigma * a + \tau * b = c, \qquad deg(\sigma) \leq\ deg(b) - 1$$

Proof.

From the extended Euclidean algorithm

$$s * a + t * b = 1 = \gcd(a, b)$$

or

$$s * w * a + t * w * b = w$$

We need to lower the degree of $s * w$.

$$s * w = q * b + r \qquad \text{where} \qquad \deg(r) \leq \deg(b) - 1$$

and substituting it back to the previous equation

$$(q * b + r) * a + t * w * b = w$$

Collecting terms by b,

$$r * a + (q * a + t * w) * b = w$$

we obtain

$$\sigma * a + \tau * b = c$$

where $\tau = q * a + t * c$ and $\sigma = r$. Since

$$\deg(\sigma) = \deg(r) \leq \deg(b) - 1$$

we complete the proof. QED.

■ Example

$$\int \frac{x^3 + \frac{3}{2}\, x^2}{\left(x^3 + x + 1\right)^2}\, dx$$

```
p = x^3 + 3 x^2/2;
q = (x^3 + x + 1)^2;
v = x^3 + x + 1; (* the last factor *)
m = 2;
u = q/v^m;
```

We need to find such a and b that

$$u\, v' * a + v * b = r, \quad \deg(a) < \deg(v)$$

Using PolynomialExtendedGCD we find p_1 and p_2, such that

$$u\, v' * p_1 + v * p_2 = 1$$

```
PolynomialExtendedGCD[u * D[v, x], v]
```

$$\left\{1, \left\{\frac{4}{31} - \frac{9\,x}{31} + \frac{6\,x^2}{31}, \frac{27}{31} - \frac{18\,x}{31}\right\}\right\}$$

```
{p1, p2} = %[[2]];
```

Multiply this

$$u\, v' * p_1 + v * p_2 = 1$$

by p

$$p * u\, v' * p_1 + p * v * p_2 = p$$

and then decreasing the order of $p_1 * p$

$$p * p_1 = x * v + y$$

```
PolynomialRemainder[p1 * p, v, x]
```

$\frac{1}{2} + \frac{x}{2}$

```
PolynomialQuotient[p1 * p, v, x]
```

$-\frac{1}{2} + \frac{6 x^2}{31}$

It follows

$$p_1 * p = \left(\frac{6 x^2}{31} - \frac{1}{2}\right) * v + \left(\frac{x}{2} + \frac{1}{2}\right)$$

Substituting this into

$$p * u v' * p_1 + p * v * p_2 = p$$

and collecting terms wrt v, we get

$$\underbrace{(\frac{x}{2} + \frac{1}{2})}_{a} * u * v' + (p_2 * p + \underbrace{\left(\frac{6 x^2}{31} - \frac{1}{2}\right) * u * v'}_{b}) * v = p$$

where

```
a = PolynomialRemainder[p1 * p, v, x]
```

$\frac{1}{2} + \frac{x}{2}$

```
b = Expand[PolynomialQuotient[p1 * p, v, x] * u * D[v, x] +
    p2 * p]
```

$-\frac{1}{2}$

Thus, by Hermite-Ostrogradsky's algorithm

$$\int \frac{p}{q} = \frac{1}{1-m} * \frac{a}{v^{m-1}} + \frac{1}{1-m} * \int \frac{b*(1-m) - u*a'}{u*v^{m-1}}$$

we obtain

$$\int \frac{x^3 + \frac{3}{2}x^2}{\left(x^3+x+1\right)^2}\,dx = -\frac{\frac{x}{2}+\frac{1}{2}}{x^3+x+1}$$

since

$$\frac{b\,(1-m) - u\,D[a,\,x]}{u\,v^{m-1}}$$

$$0$$

and

$$\frac{a}{(1-m)\,v^{m-1}}$$

$$\frac{\frac{1}{2}+\frac{x}{2}}{-1-x-x^3}$$

References

D. R. Musser, *Algorithms for Polynomial Factorization*, Ph.D. thesis, University of Wisconsin, 1971.

A. G.. Akritas, *Elements of computer algebra with applications*, Wiley, NY, 1989.

D. Y. Yun, On square-free decomposition algorithms, *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation*, (1976), pp. 26-25.

E. Hermite, Sur l'intégration des fractions rationelles, *Nouvelles Annales de Mathématiques*, **11**(1872), 145-148.

M. W. Ostrogradsky, De l'intégration des fractions rationelles, *Bulletin de la Classe Physico-Mathématiques de l'Académie Impériale des Sciences de St. Pétersburg*, IV, 1845, pp145-167, 286-300.

M. Bronstein, *Symbolic Integration - Transcendental Functions*, Algorithms and Computations in Mathematics, Vol 1, Springer-Verlag, 1996.