Fast computation of the trace vector

Jörg Arndt, ANU, Canberra, arndt@jjj.de

ABSTRACT. For a finite field $\mathrm{GF}(p^n)$ where p is prime and $n \geq 1$, with field polynomial C, we give an algorithm to compute the traces of the powers a^k of a root a of C, for $0 \leq k < n$. The computational cost is that of one classical multiplication, with space requirement proportional to n. Finally we give a variant of the algorithm the requires just one division of power series. Thereby we obtain a computational cost that is at most 3 times of the cost of multiplying two power series up to the n-th term.

Let $C(x)$ be a polynomial of degree n in the indeterminate x with n roots a_0, a_1, ..., a_{n-1}

$$C(x) \quad = \quad \prod_{k=0}^{n-1} (x - a_k) \;=\; \sum_{k=0}^{n} c_k\, x^k \tag{1}$$

We define (following [**6**, sec.32])

$$s_k \quad := \quad a_0^k + a_1^k + \ldots + a_{n-1}^k \tag{2}$$

Then, for $m = 1, \ldots, n$, we have Newton's formula:

$$m\, c_{n-m} \quad = \quad -\sum_{j=0}^{m-1} s_{m-j}\, c_{n-j} \tag{3}$$

Now let $C = c_0 + c_1\, x + c_2\, x^2 + \ldots + c_n\, x^n$ be an irreducible polynomial over $\mathrm{GF}(p)$ with roots $a_0 = a$, $a_1 = a^p$, $a_2 = a^{p^2}$, $a_3 = a^{p^3}$, ..., $a_{n-1} = a^{p^{n-1}}$. We want to compute the trace vector $[t_k]_{0 \leq k < n}$, where $t_k = \mathrm{Tr}(a^k)$, and Tr is the absolute trace as defined in [**4**, p.51]. Let z be a field element z in polynomial basis representation $z = \sum_{j=0}^{n-1} e_j\, a^j$. Given the trace vector, the trace $\mathrm{Tr}(z)$ can be computed in linear time as the inner product $\mathrm{Tr}(z) = \sum_{j=0}^{n-1} e_j\, t_j$.

Using $c_n = 1$ (monic polynomial C) and $t_j = s_j$ we rewrite Newton's formula as

$$\begin{aligned}
&\text{(4a)} \qquad & t_1 &= -1\,c_{n-1} \\
&\text{(4b)} \qquad & t_2 &= -c_{n-1}\,t_1 - 2\,c_{n-2} \\
&\text{(4c)} \qquad & t_3 &= -c_{n-1}\,t_2 - c_{n-2}\,t_1 - 3\,c_{n-3} \\
&\text{(4d)} \qquad & t_4 &= -c_{n-1}\,t_3 - c_{n-2}\,t_2 - c_{n-3}\,t_1 - 4\,c_{n-4} \\
& & &\vdots \\
&\text{(4e)} \qquad & t_k &= -c_{n-1}\,t_{k-1} - c_{n-2}\,t_{k-2} - \ldots - c_{n-k-1}\,t_1 - k\,c_{n-k} \\
& & &\vdots
\end{aligned}$$

To compute the trace vector, make the assignments in the given order, and finally compute $t_0 = n \bmod p$. The computational cost is n^2 field operations and does not involve any polynomial modular reduction so the method can be worthwhile even for the determination of the trace of just one element. While the computation by the definition is proportional to n^2 in theory, the practical cost is of order n^3 due to the modular reductions, unless the polynomial C is very sparse.

In [**1**] the relations (4a. . . 4e) are used to determine certain properties of the trace vector. For example, the binary polynomials with just one nonzero entry in the trace vector are characterized. The use for the computation of the trace vector, however, was not considered.

The following variant of the algorithm, suggested by Richard Brent, shows that the computation is equivalent to a division of power series. Let R be the reciprocal polynomial of C, then (see [**3**, p.135])

$$\log\left(R(x)\right) \quad = \quad -\sum_{j=1}^{\infty} t_j\, x^j / j \tag{5}$$

Differentiating both sides gives

$$\frac{R'(x)}{R(x)} \quad = \quad -\sum_{j=1}^{\infty} t_j\, x^{j-1} \tag{6}$$

While equation 5 is only valid over characteristic zero, equation 6 holds for finite fields, as can be verified by multiplying both sides by $R(x)$ and equating coefficients. Using Newton's method for the inversion we obtain a computational cost of $\gamma\, M(n)$ where $M(n)$ is the cost for the multiplication of two power series up to order x^n and γ is a constant. The constant γ equals at most three: if the division is performed by one inversion, which is about the same cost as two multiplications with the second order Newton iteration, and one final multiplication with $R'(x)$. There are techniques to lower the constant for the division. For large n the multiplications should be done by one of the splitting schemes suggested in [**2**] or by FFT methods such as given in [**5**].

References

[1] Omran Ahmadi, Alfred Menezes: **On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$**, Designs, Codes and Cryptography, vol.37, no.3, pp.493-507, December-2005.

[2] Marco Bodrato: **Towards Optimal Toom-Cook Multiplication for Univariate and Multivariate Polynomials in Characteristic 2 and 0**, Lecture Notes in Computer Science, vol.4547, pp.116-133, 2007.

[3] Richard P. Brent: **On computing factors of cyclotomic polynomials**, Mathematics of Computation, vol.61, no.203, pp.131-149, July-1993.

[4] Rudolf Lidl, Harald Niederreiter: **Introduction to finite fields and their applications**, Cambridge University Press, revised edition, 1994.

[5] Arnold Schönhage: **Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2**, Acta Informatica, vol.7, no.4, pp.395-398, December-1977.

[6] H. W. Turnbull: **Theory of Equations**, (fifth edition), Oliver and Boyd, Edinburgh, 1952.