Journal of Symbolic Computation 98 (2020) 270–283

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Fast Hermite interpolation and evaluation over finite fields of characteristic two

Nicholas Coxon

INRIA Saclay Île-de-France, Bâtiment Alan Turing, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France

ARTICLE INFO

Article history:
Received 30 November 2017
Accepted 28 February 2019
Available online 15 July 2019

Keywords:
Hermite interpolation
Hermite evaluation
Multiplicity codes

ABSTRACT

This paper presents new fast algorithms for Hermite interpolation and evaluation over finite fields of characteristic two. The algorithms reduce the Hermite problems to instances of the standard multipoint interpolation and evaluation problems, which are then solved by existing fast algorithms. The reductions are simple to implement and free of multiplications, allowing low overall multiplicative complexities to be obtained. The algorithms are suitable for use in encoding and decoding algorithms for multiplicity codes.

1. Introduction

Hermite interpolation is the problem of computing the coefficients of a polynomial given the values of its derivatives up to sufficiently large orders at one or more evaluation points. The inverse problem, that of evaluating the derivatives of the polynomial when given its coefficients, is sometimes referred to as Hermite evaluation. Over fields of positive characteristic p, the ith formal derivative vanishes identically for i greater than or equal to p. Consequently, it is usual to consider Hermite interpolation and evaluation with respect to the Hasse derivative over such fields when the characteristic is small.

For now, let $\mathbb{F}$ simply denote a field. Then, for $i \in \mathbb{N}$, the map $D^i : \mathbb{F}[x] \to \mathbb{F}[x]$ that sends $f \in \mathbb{F}[x]$ to the coefficient of y^i in $f(x+y) \in \mathbb{F}[x][y]$ is called the ith Hasse derivative on $\mathbb{F}[x]$. For distinct evaluation points $\omega_0, \ldots, \omega_{n-1} \in \mathbb{F}$ and positive integer multiplicities $\ell_0, \ldots, \ell_{n-1}$, the Hermite interpolation problem over $\mathbb{F}$ asks that we compute the coefficients of a polynomial $f \in \mathbb{F}[x]$ of degree

E-mail address: nicholas.coxon@inria.fr.

https://doi.org/10.1016/j.jsc.2019.07.014
0747-7171/

strictly less than $\ell = \ell_0 + \cdots + \ell_{n-1}$ when given $(D^i f)(\omega_j)$ for $j \in \{0, \ldots, \ell_i - 1\}$ and $i \in \{0, \ldots, n-1\}$. The corresponding instance of the Hermite evaluation problem asks that we use the coefficients of f to compute the ℓ derivatives of the interpolation problem. Different versions of the problems specify different bases on which the polynomials are required to be represented. This paper considers the problems with respect to the monomial basis $\{x^i \mid i \in \mathbb{N}\}$ of $\mathbb{F}[x]$ only.

In this paper, the complexity of algorithms is measured by counting the number of field operations they perform. Let $\mathsf{M}(\ell)$ denote the number of operations in $\mathbb{F}$ required to multiply two polynomials in $\mathbb{F}[x]$ of degree strictly less than ℓ. Then $\mathsf{M}(\ell)$ may be taken to be in $\mathcal{O}(\ell(\log \ell)\log\log \ell)$ (Schönhage and Strassen, 1971; Schönhage, 1976/1977; Cantor and Kaltofen, 1991), and may be taken to be in $\mathcal{O}(\ell(\log \ell)4^{\log^* \ell})$, where $\log^*$ denotes the iterated logarithm, if the field is finite (Harvey and van der Hoeven, 2017; Harvey et al., 2016, 2017). Throughout the paper, the common assumption is made (used, for instance, by von zur Gathen and Gerhard (2013)) that $\mathsf{M}(\ell)/\ell$ is an increasing function of ℓ.

The boundary case $\ell_0 = \cdots = \ell_{n-1} = 1$ of the Hermite interpolation and evaluation problems corresponds to standard multipoint interpolation and evaluation, allowing the problems to be solved with $\mathcal{O}(\mathsf{M}(\ell)\log \ell)$ operations by the use of remainder trees and fast Chinese remainder algorithms (Fiduccia, 1972; Moenck and Borodin, 1972; Borodin and Moenck, 1974; Bostan et al., 2003, 2004; Bernstein, 2004; see also von zur Gathen and Gerhard, 2013, Chapter 10). If the field admits a suitable "inborn" fast Fourier transform (FFT), as occurs when it is finite, and the evaluation points are fixed, then the algorithms of van der Hoeven (2016) allow a factor of size $\mathcal{O}(\log\log \ell)$ to be removed from these estimates. If the evaluation points form a geometric progression, then the complexity of solving the standard interpolation and evaluation problems reduces to $\mathcal{O}(\mathsf{M}(\ell))$ operations (Bostan and Schost, 2005). Similarly, the cost of solving both problems reduces to $\mathcal{O}(\ell \log \ell)$ operations when the evaluation points coincide with those of a truncated Fourier transform (van der Hoeven, 2004, 2005; Harvey, 2009; Harvey and Roche, 2010; see also Larrieu, 2017).

For the opposing boundary case of $n = 1$, the Hermite interpolation and evaluation problems reduce to computing Taylor expansions. Indeed, it follows directly from the definition of Hasse derivatives that

$$f = \sum_{i \in \mathbb{N}} (D^i f)(\omega)\,(x - \omega)^i \quad \text{for } f \in \mathbb{F}[x] \text{ and } \omega \in \mathbb{F}. \tag{1}$$

Consequently, Hermite interpolation and evaluation at a single evaluation point can be performed with $\mathcal{O}(\mathsf{M}(\ell)\log \ell)$ operations in general (Borodin and Moenck, 1974; von zur Gathen, 1990; von zur Gathen and Gerhard, 1997), $\mathcal{O}(\mathsf{M}(\ell))$ operations if $(\ell - 1)!$ is invertible in the field (Aho et al., 1975; Vari, 1974) (see also von zur Gathen and Gerhard, 1997; Bini and Pan, 1994), and $\mathcal{O}(\ell \log \ell)$ operations if the field has characteristic equal to two (Gao and Mateer, 2010).

The first quasi-linear time algorithms for solving the general Hermite problems were proposed by Chin (1976). Truncating the Taylor expansion (1) after i terms gives the residue of degree less than i of f modulo $(x-\omega)^i$. Based on this observation, Chin's evaluation algorithm begins by using a remainder tree to compute the residues of the input polynomial modulo $(x - \omega_i)^{\ell_i}$ for $i \in \{0, \ldots, n-1\}$. The Taylor expansion of each residue at its corresponding evaluation point is then computed to obtain the truncated Taylor expansion of the input polynomial. The interpolation problem can be solved by reversing these steps, with the residues combined by a fast Chinese remainder algorithm. It follows that the general Hermite interpolation and evaluation problems may be solved with $\mathcal{O}(\mathsf{M}(\ell)\log \ell)$ operations (Chin, 1976; Olshevsky and Shokrollahi, 2000) (see also Bini and Pan, 1994; Pan, 2001).

In this paper, we present new algorithms for Hermite interpolation and evaluation over finite fields of characteristic two. The algorithms require the set of evaluation points to equal the field itself, and their corresponding multiplicities to be balanced, with $|\ell_i - \ell_j| \leq 1$ for $i \neq j$. While not solving the general interpolation and evaluation problems over these fields, the algorithms are suitable for use in multivariate Hermite interpolation and evaluation algorithms (Coxon, 2019), encoding and decoding algorithms for multiplicity codes (Kopparty, 2014; Coxon, 2019) and the codes of Wu (2015), and private information retrieval protocols based on these codes (Woodruff and Yekhanin, 2007; Augot et al., 2014).

When ℓ is a multiple of the order q of the field, as occurs in some encoding and decoding contexts, the Hermite interpolation algorithm presented here performs ℓ/q standard interpolations over the q