A Note on Sparse Polynomial Interpolation in Dickson Polynomial Basis*

Erdal Imamoglu$^1$ and Erich L. Kaltofen$^2$

$^1$Department of Mathematics, Kirklareli University
Kirklareli, Turkey
eimamoglu@klu.edu.tr

$^2$Department of Mathematics, North Carolina State University
Raleigh, North Carolina, USA

Department of Computer Science, Duke University
Durham, North Carolina, USA
kaltofen@ncsu.edu; https://kaltofen.math.ncsu.edu/
kaltofen@cs.duke.edu; https://users.cs.duke.edu/~elk27

Let $(P_n(x))_{n=0,1,2,...}$ be a (vector-space) basis for the univariate polynomials $K[x]$ over a field $K$ such as the rational numbers or integers modulo a prime number. Examples of bases are standard terms $P_n(x) = x^n$ or orthogonal polynomials: Chebyshev Polynomials of four kinds. Any polynomial $f(x) \in K[x]$ is then represented as a linear combination of basis terms,

$$f(x) = \sum_{j=1}^{t} c_j P_{\delta_j}(x), \quad 0 \leq \delta_1 < \delta_2 < \cdots < \delta_t = \deg(f), \forall j: c_j \neq 0.$$  

(1)

The sparsity $t \ll \deg(f)$ with respect to the basis $P_n$ has been exploited—since $[9]$—in interpolation algorithms that reconstruct the degree/coefficient expansion $(\delta_j, c_j)_{1 \leq j \leq t}$ from values $a_i = f(\gamma_i)$ at the arguments $x \leftarrow \gamma_i \in K$. Current algorithms for standard and Chebyshev bases use $i = 1, \ldots, N = t + B$ values when an upper bound $B \geq t$ is provided on input. The sparsity $t$ can also be computed “on-the-fly” from $N = 2t + 1$ values by a randomized algorithm which fails with probability $O(\epsilon \deg(f)^3)$, where $\epsilon \ll 1$ can be chosen on input. See $[3]$ for a list of references.

This note considers Dickson Polynomials for the basis in which a sparse representation is sought. Wang and Yucas $[10$, Remark 2.5] define the $n$-th degree Dickson Polynomials $D_{n,k}(x,a) \in K[x]$ of the $(k+1)$'st kind for a parameter $a \in K, a \neq 0$, and $k \in \mathbb{Z}_{\geq 0}, k \neq 2$ recursively as follows:

$$D_{0,k}(x,a) = 2 - k; \quad D_{1,k}(x,a) = x; \quad D_{n,k}(x,a) = xD_{n-1,k}(x,a) - aD_{n-2,k}(x,a), \forall n \geq 2.$$  

(2)

Here $k = 0$ and $k = 1$ yield Dickson Polynomials of the First Kind and the Second Kind, respectively, denoted by $D_{n,0}(x,a) = D_n(x,a)$ and $D_{n,1}(x,a) = E_n(x,a)$ $[8]$.

$^*$Supported by the Scientific and Technological Research Council of Turkey under Project 119F426 (Imamoglu) and by the National Science Foundation (USA) under Grant CCF-1717100 (Kaltofen).
Sparse Polynomials in Dickson Basis

In [3, Section 5], a parameterized basis for the polynomial ring $\mathbb{K}[x]$ is introduced:

$$V_0^{[u,v,w]}(x) = 1; \quad V_1^{[u,v,w]}(x) = ux + w; \quad V_n^{[u,v,w]}(x) = vx V_{n-1}^{[u,v,w]}(x) - V_{n-2}^{[u,v,w]}(x), \forall n \geq 2 \quad (3)$$

where $u, v \in \mathbb{K}\setminus\{0\}, w \in \mathbb{K}$. In Table 1 we give the specific settings of the parameters for which one obtains the Chebyshev Polynomials of all four Kinds and the Dickson Polynomials of the $(k+1)$st Kind for all $k \neq 2$.

<table>
<thead>
<tr>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Chebyshev-1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2. Chebyshev-2</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3. Chebyshev-3</td>
<td>2</td>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>4. Chebyshev-4</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5. Dickson-1</td>
<td>$\frac{1}{2b}$</td>
<td>$\frac{1}{b}$</td>
<td>0</td>
</tr>
<tr>
<td>6. Dickson-2</td>
<td>$\frac{1}{b}$</td>
<td>$\frac{1}{b}$</td>
<td>0</td>
</tr>
<tr>
<td>7. Dickson-$(k + 1)$</td>
<td>$\frac{1}{(2-k)b}$</td>
<td>$\frac{1}{b}$</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1: Recurrence parameters for basis polynomials

From Table 1, Row 5, we get that a $t$-sparse polynomial in Dickson Basis of the First Kind is a $t$-sparse polynomial in Chebyshev Basis of the First Kind, namely,

$$\sum_{j=1}^{t} c_j D_{\delta_j}(x, a) = \sum_{j=1}^{t} (2b^{\delta_j}c_j) V_{\delta_j}^{[\frac{1}{2b}, \frac{1}{b}, 0]}(x) = \sum_{j=1}^{t} (2b^{\delta_j}c_j) T_{\delta_j}(y), \quad y = \frac{x}{2b}, \quad b^2 = a. \quad (4)$$

Therefore, if on input we have the squareroot $b$ of the Dickson Polynomial parameter $a$, all the algorithms for sparse interpolation in Chebyshev Basis of the First Kind [7, 4, 1, 3, 6] can be used to reconstruct the left-side (4). Table 1, Row 6, yields a similar transfer to Dickson Polynomials of the Second Kind Chebyshev Polynomials of the Second Kind. We also give algorithms for arbitrary parameters $u, v, w$, which apply to Dickson Polynomial of the $(k+1)$st Kind by Row 7. In particular, we can compute an integer $k$ and a value $b$ that yields the sparsest representation (1) [3, Section 6].

A remaining problem is when the squareroot of $a$ cannot be computed, or does not exist in $\mathbb{K}$. One may then proceed in two ways. First, one can appeal to a square-free transfer to polynomials $\in \mathbb{K}[x, \frac{1}{x}]$ (Laurent polynomials). In [3, Fact 5.1.ii] we give a transform of parameterized basis polynomials $V_n^{[u,v,w]}(x)$ (3) to Laurent polynomials:

$$\forall n \in \mathbb{Z}: \quad \left(y - \frac{1}{y}\right)V_n^{[u,v,w]}(\frac{y + \frac{1}{y}}{v}) = \frac{u}{v} \left(y^{n+1} - \frac{1}{y^{n+1}}\right) + w \left(y^n - \frac{1}{y^n}\right) + \left(\frac{u}{v} - 1\right) \left(y^{n-1} - \frac{1}{y^{n-1}}\right). \quad (5)$$

Substituting in Table 1, Row 7, $x = (y + 1/y)/v = b(y + 1/y) = z + b^2/z = z + a/z$ we obtain

$$\left(z - \frac{a}{z}\right) D_{n,k}(z + \frac{a}{z}, a) = z^{n+1} - \frac{a^{n+1}}{z^{n+1}} + (k-1)az^{-1} - \frac{(k-1)a^n}{z^{n-1}} \quad [10]. \quad (6)$$
The identity (6) specializes for $k = 0$ and $k = 1$ to
\[ D_n \left( z + \frac{a}{z}, a \right) = z^n + \frac{a^n}{z^n} \quad \text{and} \quad \left( z - \frac{a}{z} \right) E_n \left( z + \frac{a}{z}, a \right) = z^{n+1} - \frac{a^{n+1}}{z^{n+1}} \quad [10]. \]

Therefore, \( \sum_{j=1}^t c_j D_{\delta_j}(z + a/z, a) \) and \( (z - a/z) \sum_{j=1}^t c_j E_{\delta_j}(z + a/z, a) \) are Laurent polynomials of sparsity \( 2t \), and \( (z - a/z) \sum_{j=1}^t c_j D_{\delta_j,k}(z + a/z, a) \) is by (6) a Laurent polynomial of sparsity \( \leq 4t \).

The sparse interpolation algorithms in [4, 5, 6] can recover \( t \), \( c_j \) and \( \delta_j \) from a black box for \( f \), using at the minimum \( 4t \) and \( 8t \) evaluations, respectively. Note that by (6) there can be overlaps of power terms. One recovers \( c_j(z - a/z)D_{\delta_j,k}(z + a/z, a) \) from the sparse Laurent representation of \( (z - a/z)f(z + a/z, a) \) iteratively from \( j = t \) down to \( j = 1 \) using (6).

With an element \( b \in K \) for which \( b^2 = a \) on input, half as many black box evaluations of \( f \) are needed, because the transfer to Laurent polynomials by substituting \( y = (z + 1/z)/2 \) in (4) so that \( T_{\delta_j}((z+1/z)/2) = (z^{\delta_j} + 1/z^{\delta_j})/2 \) has the advantage that evaluations at \( z = \omega^i \) for \( i = 0, 1, \ldots, 2t-1 \) produce values at \( z = \omega^\ell \) for \( \ell = -2t+1, -2t+2, \ldots, -1, 0, 1, \ldots, 2t-1 \). Therefore, at the minimum only \( 2t \) evaluations are required to recover the sparse representation (4) if one has \( b \) [7, 3]. For the special case \( a = -1 \) and \( \delta_1 \equiv \cdots \equiv \delta_t \) (mod 2), a similar savings is possible without a squareroot \( b \) for Dickson Polynomials of the First and Second Kind, because, for example,
\[ D_n \left( z - \frac{1}{z}, -1 \right) = z^n + \frac{(-1)^n}{z^n} = \begin{cases} 2T_n \left( z + \frac{1}{z} \right)/2 & \text{if } n \text{ is even}, \\ (z - \frac{1}{z})U_{n-1} \left( z + \frac{1}{z} \right)/2 & \text{if } n \text{ is odd}, \end{cases} \]

and our algorithms in [3] can be applied.

A second way is to use pseudo-complex numbers \( \alpha + i\beta \) where \( \alpha, \beta \in K \) and \( i^2 = a \). Then \( b \) is the symbol \( i \). Evaluation of the black box for \( f \) modulo \( i^2 - a \) is possible, for example, for black boxes that are straight-line programs. Such approach is used in [2].

References


