ACM Communications in Computer Algebra, Vol. 54, No. 4, Issue 214, December 2020

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

$$f(x) = \sum_{j=1}^{t} c_j \mathcal{P}_{\delta_j}(x), 0 \le \delta_1 < \delta_2 < \cdots < \delta_t = \deg(f), \forall j\colon c_j \ne 0. \tag{1}$$

The sparsity $t \ll \deg(f)$ with respect to the basis $\mathcal{P}_n$ has been exploited—since [9] —in interpolation algorithms that reconstruct the degree/coefficient expansion $(\delta_j, c_j)_{1\le j\le t}$ from values $a_i = f(\gamma_i)$ at the arguments $x \leftarrow \gamma_i \in \mathsf{K}$. Current algorithms for standard and Chebyshev bases use $i = 1, \ldots, N = t + B$ values when an upper bound $B \ge t$ 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 $D_{n,k}(x, a) \in \mathsf{K}[x]$ of the $(k + 1)$'st kind for a parameter $a \in \mathsf{K}, a \ne 0$, and $k \in \mathbb{Z}_{\ge 0}, k \ne 2$ recursively as as follows:

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

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).

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

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

where $u, v \in \mathsf{K} \setminus \{0\}, w \in \mathsf{K}$. 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 $k \neq 2$.

	u	v	w					
1. Chebyshev-1	1	2	0	$T_n(x)$	$=$	$V_n^{[1,2,0]}(x)$		
2. Chebyshev-2	2	2	0	$U_n(x)$	$=$	$V_n^{[2,2,0]}(x)$		
3. Chebyshev-3	2	2	-1					
4. Chebyshev-4	2	2	1					
5. Dickson-1	$\frac{1}{2b}$	$\frac{1}{b}$	0	$D_n(x, b^2)$	$=$	$2b^n\, V_n^{[\frac{1}{2b},\frac{1}{b},0]}(x)$	$=$	$2b^n\, T_n\big(\frac{x}{2b}\big)$
6. Dickson-2	$\frac{1}{b}$	$\frac{1}{b}$	0	$E_n(x, b^2)$	$=$	$b^n\, V_n^{[\frac{1}{b},\frac{1}{b},0]}(x)$	$=$	$b^n\, U_n\big(\frac{x}{2b}\big)$
7. Dickson-$(k+1)$	$\frac{1}{(2-k)b}$	$\frac{1}{b}$	0	$D_{n,k}(x, b^2)$	$=$	$(2-k)b^n\, V_n^{[\frac{1}{(2-k)b},\frac{1}{b},0]}(x)$		

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,

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

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 K. One may then proceed in two ways. First, one can appeal to a square-free transfer to polynomials $\in \mathsf{K}[x, \frac{1}{x}]$ (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:

$$\forall n \in \mathbb{Z}\colon \Big(y - \frac{1}{y}\Big) V_n^{[u,v,w]}\Big(\frac{y + \frac{1}{y}}{v}\Big) = \frac{u}{v}\Big(y^{n+1} - \frac{1}{y^{n+1}}\Big) + w\Big(y^n - \frac{1}{y^n}\Big) + \Big(\frac{u}{v} - 1\Big)\Big(y^{n-1} - \frac{1}{y^{n-1}}\Big). \tag{5}$$

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

$$\Big(z - \frac{a}{z}\Big)\, D_{n,k}\Big(z + \frac{a}{z}, a\Big) = z^{n+1} - \frac{a^{n+1}}{z^{n+1}} + (k-1)az^{n-1} - \frac{(k-1)a^n}{z^{n-1}} \quad [10]. \tag{6}$$

The identity (6) specializes for $k = 0$ and $k = 1$ to

$$D_n\Big(z + \frac{a}{z}, a\Big) = z^n + \frac{a^n}{z^n} \quad \text{and} \quad \Big(z - \frac{a}{z}\Big) E_n\Big(z + \frac{a}{z}, a\Big) = z^{n+1} - \frac{a^{n+1}}{z^{n+1}} \quad [10]. \tag{7}$$

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 δ_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 $b \in \mathsf{K}$ 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 $\delta_1 \equiv \cdots \equiv \delta_t \pmod 2$, a similar savings is possible without a squareroot b for Dickson Polynomials of the First and Second Kind, because, for example,

$$D_n\Big(z - \frac{1}{z}, -1\Big) = z^n + \frac{(-1)^n}{z^n} = \begin{cases} 2T_n\Big((z + \frac{1}{z})/2\Big) & \text{if } n \text{ is even,} \\ (z - \frac{1}{z})U_{n-1}\Big((z + \frac{1}{z})/2\Big) & \text{if } n \text{ is odd,} \end{cases}$$

and our algorithms in [3] can be applied.

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

References

[1] Andrew Arnold and Erich L. Kaltofen. Error-correcting sparse interpolation in the Chebyshev basis. In *ISSAC'15 Proc. 2015 ACM Internat. Symp. Symbolic Algebraic Comput.*, pages 21–28, New York, N. Y., 2015. Association for Computing Machinery. URL: http://users.cs.duke.edu/~elk27/bibliography/15/ArKa15.pdf.

[2] S. Garg and É. Schost. Interpolation of polynomials given by straight-line programs. *Theoretical Computer Science*, 410(27-29):2659–2662, 2009.

[3] Erdal Imamoglu, Erich L. Kaltofen, and Zhengfeng Yang. Sparse polynomial interpolation with arbitrary orthogonal polynomial bases. In Carlos Arreche, editor, *ISSAC '18 Proc. 2018 ACM Internat. Symp. Symbolic Algebraic Comput.*, pages 223–230, New York, N. Y., 2018. Association for Computing Machinery. In memory of Bobby F. Caviness (3/24/1940–1/11/2018). URL: http://users.cs.duke.edu/~elk27/bibliography/18/IKY18.pdf.

[4] Erich Kaltofen and Wen-shin Lee. Early termination in sparse interpolation algorithms. *J. Symbolic Comput.*, 36(3–4):365–400, 2003. Special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti & L. M. Pardo. URL: http://users.cs.duke.edu/~elk27/bibliography/03/KL03.pdf.

[5] Erich L. Kaltofen and Clément Pernet. Sparse polynomial interpolation codes and their decoding beyond half the minimal distance. In Katsusuke Nabeshima, editor, *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.*, pages 272–279, New York, N. Y., 2014. Association for Computing Machinery. URL: http://users.cs.duke.edu/~elk27/bibliography/14/KaPe14.pdf.

[6] Erich L. Kaltofen and Zhi-Hong Yang. Sparse interpolation with errors in Chebyshev basis beyond redundant-block decoding. *IEEE Trans. Information Theory*, accepted, September 2020. URL: http://users.cs.duke.edu/~elk27/bibliography/19/KaYa19.pdf, https://arxiv.org/abs/1912.05719.

[7] Lakshman Y. N. and B. D. Saunders. Sparse polynomial interpolation in non-standard bases. *SIAM J. Comput.*, 24(2):387–397, 1995.

[8] Rudolf Lidl, Gary L. Mullen, and Gerhard Turnwald. *Dickson polynomials*, volume 65. Chapman & Hall/CRC, 1993.

[9] R. Prony. Essai expérimental et analytique sur les lois de la Dilatabilité de fluides élastiques et sur celles de la Force expansive de la vapeur de l'eau et de la vapeur de l'alkool, à différentes températures. *J. de l'École Polytechnique*, 1:24–76, Floréal et Prairial III (1795). R. Prony is Gaspard(-Clair-François-Marie) Riche, baron de Prony.

[10] Qiang Wang and Joseph L. Yucas. Dickson polynomials over finite fields. *Finite Fields and Their Applications*, 18(4):814 – 831, 2012.