Efficient Deterministic Interpolation of Multivariate Polynomials over Finite Fields

Michael Clausen
Department of Computer Science
University of Karlsruhe

Johannes Grabmeier
Heidelberg Scientific Center
IBM Germany

Marek Karpinski
Department of Computer Science
University of Bonn

Abstract

We present an efficient interpolation scheme for n-variate k-sparse polynomials f over a finite field with q elements. The polynomial time interpolation algorithm uses $2k - \lfloor (2k-1)/q \rfloor$ evaluations and is efficiently parallelizable (NC) within polynomial number of processors and squared-logarithmic parallel time.

Introduction

The ring of polynomial functions in n variables over the finite field $GF(q)$ of prime power order q is isomorphic to $GF(q)[X_0, \ldots, X_{n-1}]$, the polynomial ring in n indeterminates modulo the ideal generated by $X_0^q - X_0, \ldots, X_{n-1}^q - X_{n-1}$. Taking this into account a possible variant of the interpolation problems of polynomials over finite fields is as follows:

Let $f \in GF(q)[X_0, \ldots, X_{n-1}]$ be a polynomial satisfying $\deg_{X_i}(f) < q$, for all i. How many evaluations $f(a_0, \ldots, a_{n-1})$, a_i in a suitable finite extension field of $GF(q)$, are sufficient to reconstruct f? In the sequel we fix a positive integer k satisfying $2k - \lfloor (2k-1)/q \rfloor < q^n$. y Taking for granted that f is k-sparse, i.e. k is an upper bound for the number of non-zero coefficients of f, we shall show that $2k - \lfloor \frac{2k-1}{q} \rfloor$ evaluations of f over $GF(q^n)$ enable us to reconstruct f.

This paper continues the work of Grigoriev–Karpinski [GK86] and Ben-Or–Tiwari [BT87], [T87]. Referring to the work of Grigoriev and Karpinski, Ben-Or and Tiwari took $(p_0^i, \ldots, p_{n-1}^i), 0 \leq i < 2k$, as evaluation points, to solve the interpolation problem for k-sparse multivariate polynomials over rings of characteristic zero. Here, $p_0, \ldots, p_{n-1}$ are pairwise different primes and the crucial point is the uniqueness of the prime factorization of integers.

In our context we combine three tools in order to recover f: generalized Newton identities, uniqueness of the q-adic representation of the exponents of non-zero elements in $GF(q^n)$ with respect to a primitive element, and finally, the Frobenius automorphism $y \mapsto y^q$ of $GF(q^n)$ which keeps fixed all elements of $GF(q)$.

1 Results

In this section the following result is proved.

Theorem. *Let $f \in GF(q)[X_0, \ldots, X_{n-1}]$ be a k-sparse polynomial satisfying $\deg_{X_i}(f) < q$, for all i, and let ω be a primitive element of $GF(q^n)$. Then*

1. *f is the zero-polynomial if and only if $f_i := f(\omega^{iq^0}, \omega^{iq^1}, \ldots, \omega^{iq^{n-1}}) = 0$, for all i satisfying $0 \le i < k$ and $q \not| i$.*

2. *in order to construct f it suffices to know the values f_i for all i satisfying $0 \le i < 2k$ and $q \not| i$.*

Proof. If $f \in GF(q)[X_0, \ldots, X_{n-1}]$ satisfies $\deg_{X_i}(f) < q$, for all i, then f is a linear combination over $GF(q)$ of the q^n monomials $X^\alpha := X_0^{\alpha_0} \cdot \ldots \cdot X_{n-1}^{\alpha_{n-1}}$, where α ranges over all functions in $\mathbf{q}^\mathbf{n} := \{0, \ldots, q-1\}^{\{0,\ldots,n-1\}}$:

$$f = \sum_{\alpha \in \mathbf{q}^\mathbf{n}} c_\alpha X^\alpha.$$

The mapping $\Omega \colon \mathbf{q}^\mathbf{n} \to GF(q^n)$ defined by

$$\Omega_\alpha := \begin{cases} \prod_{0 \le \nu < n} \omega^{\alpha_\nu \cdot q^\nu}, & \text{if } \alpha \neq 0 \\ 0, & \text{if } \alpha = 0 \end{cases}$$

is bijective since $\Omega_\alpha = \omega^{(\sum \alpha_\nu q^\nu)}$ for $\alpha \neq 0$, and from the q-adic expansion of the exponent we can recover α. Let A be any k-subset of $\mathbf{q}^\mathbf{n}$ containing the support $\operatorname{supp}(f) := \{\alpha \colon c_\alpha \neq 0\}$ of f. Then

$$f_i = \sum_{\alpha \in \mathbf{q}^\mathbf{n}} c_\alpha \Omega_\alpha^i = \sum_{\alpha \in A} c_\alpha \Omega_\alpha^i.$$

Thus we obtain the following matrix equation

$$(\Omega_\alpha^i)_{0 \le i < k, \alpha \in A} \cdot (c_\alpha)_{\alpha \in A} = (f_i)_{0 \le i < k}. \tag{1}$$

The k-square matrix (Ω_α^i) is a non-singular Vandermonde matrix since the Ω_α are pairwise different. Hence f is the zero-polynomial if and only if $(f_i)_{0 \le i < k} = 0$. Finally, by the properties of the Frobenius automorphism

$$f_{i \cdot q} = (f_i)^q,$$

for all $i < q^n$. Altogether, this proves the first assertion of the theorem. Our next goal is to derive an efficient interpolation scheme for k-sparse multivariate polynomials f.

For any subset A of $\mathbf{q}^{\mathbf{n}}$ we denote by $e_i(A)$ the i-th elementary symmetric polynomial in $|A|$ indeterminates evaluated at all $\Omega_\alpha, \alpha \in A$. Now substituting Ω_α, $\alpha \in A$, for X in the polynomial

$$\prod_{\beta \in A} (X - \Omega_\beta) = \sum_{j=0}^{|A|} (-1)^{|A|-j} e_{|A|-j}(A) \cdot X^j \in GF(q^n)[X]$$

yields the generalized Newton identities [MS72, p. 244]

$$0 = \sum_{j=0}^{|A|} (-1)^{|A|-j} e_{|A|-j}(A) \Omega_\alpha^j, \quad \alpha \in A.$$

Fixing an i $(0 \le i < q^n)$, multiplying the equation corresponding to α by $c_\alpha \Omega_\alpha^i$ and summing over all $\alpha \in A$ results in the following system of equations

$$0 = \sum_{j=0}^{|A|} (-1)^{|A|-j} e_{|A|-j}(A) f_{i+j}, \quad 0 \le i < q^n.$$

As $e_0 = 1$, for an arbitrary superset A of $\mathrm{supp}(f)$ the equations for $0 \le i < |A|$ are equivalent to the matrix equation

$$(f_{i+j})_{0 \le i,j < |A|} \cdot \left((-1)^{|A|-j}\, e_{|A|-j}\,(A) \right)_{0 \le j < |A|} = -(f_{i+|A|})_{0 \le i < |A|}. \tag{2}$$

The matrix $(f_{i+j})_{0 \le i,j < |A|}$ equals $(\Omega_\alpha^i) D_A (\Omega_\alpha^i)^t$, where $D_A = \mathrm{diag}((c_\alpha)_{\alpha \in A})$ is a $|A|$-square diagonal matrix, see [LN83, 9.48, 9.49]. Hence the cardinality k of $\mathrm{supp}(f)$ equals the rank of the k-square matrix $(f_{i+j})_{0 \le i,j < k}$; furthermore $(f_{i+j})_{0 \le i,j < k}$ is non-singular and we can calculate the polynomial $\prod_{\alpha \in \mathrm{supp}(f)} (X - \Omega_\alpha)$ from (2) for $A = \mathrm{supp}(f)$. Finding all the roots gives $\{\Omega_\alpha : \alpha \in \mathrm{supp}(f)\}$ which enables us to recover $\mathrm{supp}(f)$. The solution of (1) gives the complete polynomial f. This proves our second claim. □

2 The Algorithm

In this section we present and analyze the algorithm, which can be derived from section 1.

Interpolation Algorithm. *Let $f \in GF(q)[X_0, \ldots, X_{n-1}]$ be a k-sparse polynomial satisfying $\deg_{X_i}(f) < q$, for all i; $2k < q^n$.*

INPUT: *Oracle for f.*

step 1. *Take a primitive element ω in $GF(q^n)$.*

step 2. *Ask the oracle for the $2k - \lfloor \frac{2k-1}{q} \rfloor$ values f_i, where $0 \leq i < 2k$ and $q \not| \, i$.*

step 3. *For all $0 \leq i < 2k$ which satisfy $i = q^s \cdot i_0$, $1 \leq s$, s maximal, calculate $f_i = {f_{i_0}}^{(q^s)}$.*

step 4. *Determine $\tilde{k}$, which is the rank of the matrix $(f_{i+j})_{0 \leq i,j < k}$.*

step 5. *Solve the equation $(f_{i+j})_{0 \leq i,j < \tilde{k}} \cdot ((-1)^{\tilde{k}-j} e_{\tilde{k}-j}(\mathrm{supp}(f))_{0 \leq j < \tilde{k}} = -(f_{\tilde{k}+i})_{0 \leq i < \tilde{k}}$.*

step 6. *Find all the roots Ω_α $(\alpha \in \mathrm{supp}(f))$ of the polynomial $\sum_{i=0}^{\tilde{k}} (-1)^{\tilde{k}-i} e_{\tilde{k}-i}(\mathrm{supp}(f)) \cdot X^i$.*

step 7. *Calculate the q-adic expansion of the exponents of the Ω_α with respect to ω to get $\mathrm{supp}(f)$.*

step 8. *Solve the system of linear equations $(\Omega_\alpha^i)_{0 \leq i < \tilde{k},\ \alpha \in A} \cdot (c_\alpha)_{\alpha \in A} = (f_i)_{0 \leq i < \tilde{k}}$, for $A := \mathrm{supp}(f)$.*

OUTPUT: $(c_\alpha, \alpha)_{\alpha \in \mathrm{supp}(f)}$.

Once a primitive element ω is given, we compute the rank of the k-square matrix (f_{i+j}) within $O(k^{4.5})$ arithmetic processors and $O(log^2 k)$ parallel time [M86]. The same bounds are valid for step 5. We use [G84] for factoring the univariate polynomial of step 6. This costs $O(log^2 k)$ parallel time and roughly the same number of processors as above. Steps 7 and 8 are of $O(k^{4.5})$ size and $O(log^2 k)$ parallel time.

The algorithm is optimal in case $n = 1$ and $2k < q$. To see this let A be a subset of $GF(q)$ with at most $2k-1$ elements. Then $Q := \prod_{a \in A}(X - a)$ is a non-zero polynomial in $GF(q)[X]$ of degree at most $2k - 1 < q$. Q has at most $2k$ monomials and vanishes on A. Now split Q into two different parts, $Q = f - g$, each part having at most k monomials. Then f and g are different and k-sparse, but they coincide on A.

Acknowledgements

We would like to thank T. Beth, J. von zur Gathen, A. Shokrollahi and P. Tiwari for helpful discussions and comments.

References

[AL86] **Adleman, L.M., Lenstra, H.K.:** *Finding Irreducible Polynomials over Finite Fields,* Proc. STOC ACM, (1986), 350–355.

[B81] **Ben-Or, M.:** *Probablistic Algorithms in Finite Fields,* Proc. 22^{nd}IEEE FOCS (1981), 394–398.

[BT87] **Ben-Or, M., Tiwari, P.:** *A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation,* Proc. Bonn Workshop on Foundations of Computing, Bonn, June 28 - July 3, 1987 .

[G83] **von zur Gathen, J. :** *Factoring Sparse Multivariate Polynomials,* Proc. 24^{th} IEEE FOCS (1983), 172–179..

[G84] **von zur Gathen, J. :** *Parallel algorithm for Algebraic Problems,* SIAM J. Comput., Vol. 13. 1984, 808–824.

[GK87] **Grigoriev, D.Y., Karpinski, M. :** *The Matching Problem for Bipartite Graphs with Polynomially Bounded Permanents is in NC,* to appear in Proc. 28^{th} IEEE FOCS (1987), Los Angeles, Oct. 12–14, 1987.

[IM83] **Ibarra, O.H., Moran, S.:** *Probabilistic Algorithms for Deciding Equivalence of Straight-Line Programs,* J. ACM, 30,1, (1983), 189–192.

[K85] **Kaltofen, E.:** *Computing with Polynomials Given by Straight-Line Programs I Greatest Common Divisors,* Proc. 17th ACM STOC (1985), 131–142.

[L83] **Lenstra, A.K.:** *Factoring Multivariate Polynomials over Finite Fields,* Proc. 15th ACM STOC (1983), 189–192.

[LN83] **Lidl, H., Niederreiter, H.:** *Finite Fields,* Encyclopedia of Mathematics and its Applications, Vol.10, Cambridge University Press 1983.

[MS72] **MacWilliams, F.J., Sloane, N.J.A.:** *The Theory of Error Correcting Codes,* North Holland (1972).

[M86] **Mulmuley, K.:** *A Fast Parallel Algorithm to Compute the Rank of a Matrix over an Arbitrary Field,* Proc. STOC ACM (1986), 338–339.

[S80] **Schwartz, J.T.:** *Fast Probabilistic Algorithms for Verification of Polynomial Identities,* JACM, 27, 4(1980),701–717.

[T87] **Tiwari, P.:** *Deterministic Algorithm for Multivariate Polynomial Interpolation,* preliminary draft, IBM Thomas J. Watson Research Center (June, 1987).

[Z79] **Zippel, R.E.:** *Probabilistic Algorithms for Sparse Polynomials,* Proc. EUROSAM'79, Springer Lec. Notes Comp. Sci., 72, (1979), 216–226.