Fast Derivatives for Multilinear Polynomials

Valeri Aronov

November 7, 2019

Abstract

The article considers linear functions of many \( n \) variables - multilinear polynomials (MP) \[3\]. The three-steps evaluation is presented that uses the minimal possible number of floating point operations for non-sparse MP at each step. The minimal number of additions is achieved in the algorithm for fast MP derivatives (\textit{FMPD}) calculation. The cost of evaluating all first derivatives approaches to only 1/8 of MP evaluation with a growing number of variables. The \textit{FMPD} algorithm structure exhibits similarity to the Fast Fourier Transformation (FFT) algorithm.

Contents

1 Introduction 1

2 Algorithm for Multilinear Polynomial Derivatives Calculation 1

3 Floating Point Operation Number in Multilinear Polynomial Derivatives Calculation 4

4 Fast Multilinear Polynomial Derivatives and FFT 7

References 7

1 Introduction

This is a linear function of \( n \) variables:

\[ a(x) = \sum_{i=0}^{2^n-1} r_i \cdot \prod_{k=1}^{n} x_k^{i_k}, \text{ where } \{x, r \in \mathbb{R}^n\} \]  

(1)

It is called a multilinear polynomial (MP) \[3\].

For example (for \( n=2 \)):

\[ a(x) = r_{002} + r_{012} \cdot x_1 + r_{102} \cdot x_2 + r_{112} \cdot x_1 \cdot x_2 \]

The binary notation for \( i \) is natural for the fast MP derivatives (\textit{FMPD}) algorithm presented in this article. The transfer function of linear analog electric circuits has MPs of circuit parameters in its numerator and denominator with coefficients being complex polynomials of frequency and \( x \) - values of the circuit parameters. Some software systems for linear circuit analysis generate and use symbolic (analytical) parameters presentation of the transfer functions for fast multiple transfer function evaluations \[4\]. It makes it possible to build a symbolic presentation for for derivatives of transfer functions as well. \textit{FMPD} algorithm was first introduced in \[6\] for the linear circuit parameters optimization.

2 Algorithm for Multilinear Polynomial Derivatives Calculation

This article uses \( q_i(x) \) designation:

\[ q_i(x) = r_i \cdot \prod_{k=1}^{n} x_k^{i_k}, \]  

(2)
Their derivatives then are:

\[(q_i(x))'_{x_k} = q_i(x)/x_k\]

for all \(i_k = 1\). \(q_i(x)\) does not depend on those \(x_k\) which have \(i_k = 0\) and corresponding derivatives are equal 0.

The following definitions of full and partial sums of \(q_i(x)\) are used here:

\[a_0 = a(x)\]

\[a_{0...1_k} = \sum_{i=(i_n...i_k1)_2} 2^{n-1} q_i\]

\[a_{0...0_k} = \sum_{i=(i_n...i_k01)_2} 2^{n-1} q_i\]

For two \(n\)-bit integers \(j = (j_1,...,j_n)_2\) and \(i = (i_1,...,i_n)_2\) we write \(j < i\) if their binary digits satisfy \(j_\nu \leq i_\nu, \nu = 1,...,n\). Then

\[a_i = \sum_{j<i} q_j\] (3)

\[a_{1...1} = q_{1...1}\]

Given integers \(1 \leq k_1 < ... < k_m \leq n\) we denote by \(t(k_1,...,k_m)\) the \(n\)-bit integer having 1 at positions \(k_1,...,k_m\) and 0 at all other positions. Then MP derivatives are:

\[\left(\frac{a(x)}{x_{k_1}...x_{k_m}}\right)^{\{m\}} = a_{t(k_1,...,k_m)}(x)/\prod_{j=1}^{m} x_{k_j}\] (4)

The task of MP derivatives calculation is: given \(r\) and \(x\) and using MP presentation [1] calculate all derivatives as in [4] including the evaluation of MP itself. MPs in this article are considered to be ‘non-sparse’. It means that either \(r_i \neq 0\) for all \(i\) or the savings in MP and its derivatives calculation due to omission of \(r_i = 0\) are negligible.

Execute the task in three steps:

1. Calculate all items as in [2]
2. Calculate all \(a_i\) as in [3]
3. Calculate all derivatives as in [4]

The following algorithm calculates all products of \(x_i\) in step 1:

**GetProducts**(*x, products*)

1. \(k = 1\)
2. \(products[0] = 0\)
3. \(products[1] = x[1]\)
4. for \(i = 2\) to sizeof(*x*)
   5. {
      6. \(products[k + 1] = x[i]\)
      7. for \(j = 1\) to \(k\)
      8. \(products[k + j + 1] = x[i] * x[j]\)
      9. \(k = k + 2 + 1\)
   10. }

Note that an item \(i\) of \(products\) in **GetProducts** and the items \(i\) of \(q_i(x)\) and \(r_i\) arrays in [2] relate to the this product:

\[\prod_{k=1}^{n} x_{i_k}^{j_k}\]

Note also that first \(n + 1\) items in \(products\) do not require multiplications.

Getting the results in [2] after having all the products is straightforward and requires \(2^n - 1\) multiplications more.
Let us apply ‘divide and conquer’ algorithm to the Step 2. Split all $q_j$ for $j = (j_p \ldots j_1)_2$ into two groups $q(j_{n-1} \ldots j_1)_2$ and $q(j_{n-1} \ldots j_1)_2'$. Assume that the Step 2 for $(p - 1)$ is executed for both halves and the results are $a(j_{p-1} \ldots j_1)_2$ and $\tilde{a}(j_{p-1} \ldots j_1)_2'$. Then the following operations produce the results for $p$:

$$a(j_{p-1} \ldots j_1)_2 = \tilde{a}(j_{p-1} \ldots j_1)_2$$
$$a(j_{p-1} \ldots j_1)_2 = a(j_{p-1} \ldots j_1)_2 + \tilde{a}(j_{p-1} \ldots j_1)_2'$$

GetPartialSums implements this algorithm:

GetPartialSums($q2a, xSize$)
1. $addendPositionsDifference = 1$
2. $clusterPositionsDifference = 2$
3. $q2aSizeMinusOne = sizeof(q2a) - 1$
4. $lastSumPositionLimitInSilo = q2aSizeMinusOne$
5. for $iSilo = 1$ to $xSize$
   6.   
      for $i = 0$ by $clusterPositionsDifference$ to $lastSumPositionLimitInSilo$
      7.     
         for $j = 0$ to $addendPositionsDifference - 1$
         8.           $q2a[i + j] = q2a[i + j] + q2a[i + j + addendPositionsDifference]$
         9.     
      10. $lastSumPositionLimitInSilo = q2aSizeMinusOne - clusterPositionsDifference$
      11. $addendPositionsDifference = clusterPositionsDifference$
      12. $clusterPositionsDifference = 2 * clusterPositionsDifference$
    13. }

It starts with $q2a$ containing all $q_i$ and finishes with $q2a$ containing all $a_i$. $xSize = n$ and $q2aSizeMinusOne = 2^n - 1$ here. Once the memory for $q_i$ is allocated this algorithm does not require any additional memory except of several scalar variables.

This figure presents the GetPartialSums diagrams for $n = 2, 3, 4$:
\( q_i \) input data are located along the left vertical line. \( a_i \) output data are located along the right vertical line. An arrow represents an addition where addends are taken at the levels of the arrow’s end points and the sum is placed into the location of the addend the arrow points to. The additions are executed silo-by-silo from the left silo to the right one. The top-left parts of the figure outlined by the broken lines represent diagrams for \( n = 2 \) and \( n = 3 \).

As it is proven in the next section the algorithm implemented by \textsc{GetPartialSums} requires a minimal number of floating point additions. The adjective ‘fast’ is appropriate here then.

**Definition 2.1.** The algorithm implemented by \textsc{GetPartialSums} is called a Fast Multilinear Polynomial Derivatives (\textsc{FMPD}) algorithm.

Having \textit{products} calculated in Step 1 and \( q2a \) calculated in Step 2 the last Step 3 gets derivatives of \textsc{MP} dividing each corresponding \( q2a[i] \) containing \( a_i \) by associated \textit{products}[i].

### 3 Floating Point Operation Number in Multilinear Polynomial Derivatives Calculation

Consider floating point operation numbers in Steps 1-3. Step 1 requires \( (2^n - n - 1) \) multiplications at least to produce \( (2^n - n - 1) \) different products. \textsc{GetProducts} achieves this minimum because it produces one product per multiplication. Overall Step 1 requires

\[
2^n - n - 1 + 2^n - 1 = 2^{n+1} - n - 2
\]

multiplications.

Step 3 requires \( (2^n - 2) \) divisions because \( a_0 \) and \( a_{2^n-1} = r_{2^n-1} \) do not require divisions. It achieves the minimal floating point complexity because it produces the rest of \( (2^n - 2) \) derivatives - one derivative per division.

Step 2 \textsc{FMPD} requires \( n \cdot 2^{n-1} \) additions. Its asymptotic complexity is the greatest out of all Steps. The following statement holds:

**Theorem 1.** The \textsc{FMPD} algorithm uses the minimal number of floating point additions for \( 3 \) evaluation out of all algorithms using additions only.

**Proof.** The theorem proposition about the algorithms under consideration contains the ‘additions only’ restriction. It is an open question if the proposition holds for algorithms using additions and subtractions. Let us call an algorithm to be a direct one if it uses for each \( a_i \) only the addends in \([\text{3}]\) and only once each. The direct algorithms never add an \( a_0 \) item to \( a_{11} \), for example. Note that otherwise it has to be removed from \( a_0 = a_{10} \) using subtraction. The ‘additions only’ restriction is equivalent to the direct algorithms only’ restriction. The \textsc{FMPD} algorithm uses \( n \cdot 2^{n-1} \) additions. Below we prove that this is the minimal number of additions required for \([\text{3}]\).

The theorem is valid for \( n = 2 \). Indeed, four different numbers \( a_0, a_1, a_{10} \) and \( a_{11} \) are produced by four additions used by \textsc{FMPD}. One needs at least one operation to produce one number. The \textsc{FMPD}’s number of additions for \( n = 2 \) is \( n \cdot 2^{n-1} = 4 \) and is equal to the minimal required.

Assume that the theorem in valid for \( k \) and prove that then it is valid for \( k + 1 \) as well.

Let us split all additions into three sets:

- those with both addends being \( q_{11k} \ldots i_0 \) (lower half of \( q_i \) in the diagram) or the sums of them (the 1st set);
- those with exactly one addend being \( q_{11k} \ldots i_0 \) or the sums of them (the 2nd set);
- the rest of additions (the 3rd set).

Note that these three sets do not overlap and their superset includes all additions used in \([\text{3}]\).

Let us introduce \( b_j \):

\[
b_{jk} \ldots j_0 = a_{11k} \ldots i_0
\]

Any algorithm evaluating \( a_{11k} \ldots i_0 \) does not use additions where the addends are \( q_{0jk} \ldots i_0 \) or their sums according to \([\text{3}]\). Otherwise the use of subtractions is necessary to remove \( q_{0jk} \ldots i_0 \) from the result. The first set execution obtains \( b_j \) and according to our assumption contains \( k \cdot 2^{k-1} \) additions at least.

Consider the 2nd set of additions. Each \( a_{01k} \ldots i_0 \) has to use at least one additions from the 2nd set hence there are at least \( 2^k \) additions because there are exactly \( 2^k a_{01k} \ldots i_0 \) items.
Let us prove that the 3rd set has to have at least \((k + 1) \cdot 2^k\) additions. If there is an algorithm \(A\) for \((k + 1)\) that needs lesser number of additions consider its application to \(x^* = \{0, x_k, \ldots, x_1\}\). Only additions from 3rd set remain because each addition from first two sets will have at least one 0 addend. A application to \(x^*\) reduces original target dimension from \((k + 1)\) to \(k\) and it can’t use less than \(k \cdot 2^{k-1}\) additions because it contradicts our assumption about the minimal number of additions for \(k\).

Finally, we have minimal numbers of additions for all three sets. These sets do not overlap and their superset is a set of all additions used for \(FMPD\) evaluation. Thus the total number of additions in the three sets is:

\[
A_{k+1} \geq k \cdot 2^{k-1} + k \cdot 2^{k-1} + 2^k = 2k \cdot 2^{k-1} + 2^k = k \cdot 2^k + 2^k = (k + 1) \cdot 2^k
\]

The right hand side of the above is exactly the number of additions used by \(FMPD\) for \((k + 1)\) meaning that it uses the minimal number of the required additions.

An \(FMPD_{l}\) analog of \(FMPD\) for derivatives up to \(l\)th order \((l < n)\) can be produced by omitting in \(FMPD\) the additions that do not contribute to the required partial sums. In the last silo the omitted additions will be those which arrows point to \(a_i\) that have the number of 1s in the binary presentation of \(i\) greater than \(l\). In the last but one silo the omitted arrows in the top cluster will be those pointing to \(a_i\) with the number of 1s in \(i\) greater than \(l + 1\). The lower cluster repeats the the mission pattern of the top cluster. For an \(i\)Silo the omitted arrows in the top cluster will point to \(a_i\) with the number of 1s in \(i\) greater than \(l + 1\). The rest of cluster in this cluster repeat the mission pattern of the first one. The first silo with omissions is \(i\)Silo\(_{first} = l + 2\). This figure presents the \(FMPD_{l}\) diagram for \(n = 5, l = 2\) (the omitted additions are presented with the broken line):

Note that the above omission can be precalculated for the usage in the internal loop of \texttt{GetPartialSums} and have a negligible effect on the overall execution time.

The number of floating point additions for \((k + 1)\) evaluation by \(FMPD_{l}\) \(5\):

\[
A_{FMPD_{l}} = \begin{cases} 
(l + 1) \cdot 2^{n-1} + \sum_{k=l+2}^{n} \left[ \frac{l}{i} \right] \cdot 2^{n-k} & \text{if } l < n - 1, \\ 
n \cdot 2^{n-1} & \text{if } l = n - 1.
\end{cases}
\]  

An important particular case of \((5)\) is an evaluation of a gradient along with the polynomial itself. Let us estimate the relative increase in the number of additions required for obtaining the gradient in comparison with
products in (2) are evaluated the multiplications by $A$ processors. per processor, where $O$ processor asymptotic complexity is

\[ \sum_{i=0}^{\infty} i \cdot 2^{-i} = 2 \]

we are getting:

\[ \lim_{n \to \infty} R_1(n) = 1/8 \]

Thus the cost of evaluating all partial sums for first derivatives approaches to only 1/8 of MP evaluation cost with a growing number of variables.

Similarly:

\[ \lim_{n \to \infty} R_2(n) = \text{const} \]

The number of additions in the algorithm calculating partial sums in (4) for each $i$ separately is:

\[ A_{\text{naive}} = \sum_{i=0}^{n} \binom{n}{i} \cdot (2^{n-i} - 1) = 2^n \cdot \sum_{i=0}^{n} \binom{n}{i} \cdot 2^{-i} - 2^n = 3^n - 2^n \]

The particular variant of the binomial formula was used here:

\[ \sum_{i=0}^{n} \binom{n}{i} \cdot u^i = (1 + u)^n \]

The number of additions in the algorithm calculating partial sums in (4) for each $i$ separately for the up to and including $l$ derivatives is:

\[ A_{\text{naive}_l} = \sum_{i=0}^{l} \binom{n}{i} \cdot (2^{n-i} - 1) \]

The number of additions in the algorithm calculating partial sums in (4) for each $i$ separately for the up to and including 2 derivatives is:

\[ A_{\text{naive}_2} = 1 + n \cdot 2^{n-1} + \binom{n}{2} \cdot 2^{n-2} = 1 + n \cdot 2^{n-1} + 2^{n-2} \cdot n!/(2! \cdot (n-2)!) = 1 + n \cdot 2^{n-1} + n^2 \cdot 2^{n-3} - n \cdot 2^{n-3} \]

The asymptotic complexity expressions of these algorithms are:

\[ O_{\text{FMPD}}(n) = n \cdot 2^n \]
\[ O_{\text{FMPD}_l}(n) = 2^n \]
\[ O_{\text{naive}_n}(n) = 3^n \]
\[ O_{\text{naive}_l}(n) = n^l \cdot 2^n \]

FMPD has a substantially lower complexity than the naive algorithm. The exponential complexity of FMPD and FMPD\(_l\) allow their practical usage only for relatively low $n$ values. Still it is noticeably faster than its naive counterpart. For example, for $n = 8$ FMPD uses 1024 additions vs. 6305 used by the naive algorithm. The table below compares number of additions in FMPD and FMPD\(_l\) against their naive counterparts:

| $n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $O(n)$ |
|-----|---|---|---|---|---|---|---|---|----|-------|
| $A_{\text{naive}_n}/A_{\text{FMPD}}$ | 1.25 | 1.58 | 2.0 | 2.6 | 3.5 | 4.6 | 6.2 | 8.3 | 11.3 | 1.5\(^n\) |
| $A_{\text{naive}_2}/A_{\text{FMPD}_2}$ | 1.25 | 1.58 | 2.0 | 2.4 | 2.8 | 3.5 | 4.2 | 5.0 | 5.5 | $n$ |

Now consider parallelization opportunities for the floating point operations in Steps 1-3.

Step 1. The body of the internal loop of GetProducts can be split across $m$ processors. If a single processor asymptotic complexity is $O_1(n)$ then the one for $m$ processors is $O_m(n) = O_1(n)/m$.

Step 2. As it is illustrated by FMPD diagram all additions in a silo can be executed in parallel because each addition has its own separate addends and the result. Then $A_m(n) = [A_1(n)/m] + 1$, where $A_1(n)$ and $A_m(n)$ are the number of additions for a single processor and each of $m$ processors.

Step 3. All multiplications may be executed in parallel. It requires $M_m(n) = [M_1(n)/m] + 1$ multiplications.
4 Fast Multilinear Polynomial Derivatives and FFT

The simplified FFT algorithm [1] has the following diagram:

where the solid line arrows mean the same as ones in FMPD diagram and the broken line arrows turn into void operations if \( \omega = 0 \). Comparison of FFT (\( \omega = 0 \)) with the FMPD diagram reveals their structural similarity. Note that a somewhat simpler MP derivatives problem allowed to achieve the minimal possible number of operations whereas only a complexity lower bound for FFT [5] is established.

Acknowledgements

The author would like to thank Joris van der Hoeven and Igor Shparlinski for constructive criticism of the article and advise.

References

[1] A.Aho, J.Hopcroft, J.Ullman, The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974
[2] L.O. Chua, Pen-Min Lin, Computer-aided analysis of electronic circuits: algorithms and computational techniques. Englewood Cliffs, N.J.: Prentice-Hall, 1975.
[3] A. Giambruno and M. Zaicev, Polynomial Identities and Asymptotic Methods. AMS Bookstore. Section 1.3, 2005
[4] G. Gielen and W. Sansen, Symbolic Analysis for Automated Design of Analog Integrated Circuits. Boston: Kluwer Academic Publishers, 1991.
[5] J. Morgenstern, Note on a Lower Bound of the Linear Complexity of Fast Fourier Transform. Journal of the ACM. Vol.20. N.2, 1973.
[6] В.Б.Аронов, Исследование и разработка алгоритмов и пакета прикладных программ нелинейного программирования для САПР. Автореферат диссертации. Киевский политехнический институт. Киев, 1981.