Certified Fast Fourier Transforms for Fast Arithmetic

Keywords: Floating-Point Arithmetic, Error Analysis, Fast Fourier Transform, Discrete Cosine Transform, Interval Arithmetic, Polynomial Approximation, Integer Multiplication

Supervisors: Nicolas Brisebarre[1], Claude-Pierre Jeannerod[2], Theo Mary[3], Jean-Michel Muller[4] and Joris Picot[5]

Goal. We aim at improving the best approaches to fast multiplication of big integers and high-degree polynomials. As the best known algorithms for this are based on Fourier transforms (either in $\mathbb{C}$ or in finite fields), the internship aims at improving and certifying the quality of some commonly-used numerical calculation routines, revolving around the Fast Fourier Transform (FFT) and related operations such as the Discrete Cosine Transform (DCT). One of the main difficulties is to keep the accuracy of these operations under control.

Context. When using computers, numerical approximations appear almost everywhere. Usually, numbers are stored and manipulated in finite precision floating-point arithmetic, and they represent only a finite subset of the real axis. For each basic computation (addition, multiplication) a rounding error may occur. Then, most numerical methods introduce errors. How can we then be sure of the number of digits in the answer that are correct? How can we validate from a mathematical point of view what we have computed? These questions of numerical safety are essential for many problems, ranging from computer-aided mathematics to practical applications in critical systems.

Description. The FFT was introduced in 1965 by Cooley and Tukey in its modern form [2, 3, 9], but can be traced back to Gauss [5]. The FFT and the DCT are widely used in digital signal processing [10]. The FFT also plays a central role in fast multiple-precision arithmetic, since it lies at the heart of some of the most efficient big polynomial and big integer multiplication algorithms [15, 8]. There is a large literature on the error analysis of the FFT (see [14, 7, 11, 12]). Most authors bound the relative mean-square error. For our applications, we also need bounds in terms of infinity norm. Henrici [6] gave such a bound. In [1] we have improved Henrici's bound, and built "bad input cases", for which the attained error is around one eighth of the bound.

When the polynomials to be multiplied are represented on the Chebyshev basis, the DCT is often used [16, 13, 4]. The first objective of this internship is to extend and adapt our error analysis of FFT [1] to the DCT. A second and more prospective objective is to adapt FFT/DCT routines to the implementation of a fast and accurate polynomial multiplication routine when the coefficients of the polynomials are intervals. The work will be well balanced between theoretical and algorithmic studies and fine-tuned implementations (in C or Julia).

Location and funding The internship will take place at the LIP lab, ÉNS Lyon. The trainee will receive indemnities if her/his status makes this possible. Depending on the results of the internship, an opportunity to continue with a PhD thesis could be available.

References

[1] N. Brisebarre, M. Joldeş, J.-M. Muller, A.-M. Naneş, and J. Picot. Error analysis of some operations involved in the Cooley-Tukey fast Fourier transform. *ACM Trans. Math. Software*, 46(2):Art. 11, 27, 2020.

[2] J. Cooley and J. Tukey. An algorithm for the machine calculation of complex Fourier series. *Math. Comp.*, 19(90):297–301, 1965.

[1]https://perso.ens-lyon.fr/nicolas.brisebarre/
[2]https://perso.ens-lyon.fr/claude-pierre.jeannerod/
[3]https://perso.lip6.fr/Theo.Mary/
[4]https://perso.ens-lyon.fr/jean-michel.muller/
[5]https://perso.ens-lyon.fr/joris.picot/

[3] P. Duhamel and M. Vetterli. Fast Fourier transforms: a tutorial review and a state of the art. *Signal Process.*, 19:259–299, 1990.

[4] P. Giorgi. On polynomial multiplication in Chebyshev basis. *IEEE Trans. Comput.*, 61(6):780–789, 2012.

[5] M. Heidemann, D. Johnson, and C. Burrus. Gauss and the history of the fast Fourier transform. *IEEE ASSP Magazine*, pages 14–21, October 1984.

[6] P. Henrici. *Applied and Computational Complex Analysis, Vol. 3*. Wiley, New York, 1986.

[7] N. J. Higham. *Accuracy and Stability of Numerical Algorithms*. SIAM, Philadelphia, PA, 2nd edition, 2002.

[8] D. E. Knuth. *The Art of Computer Programming*, volume 2. Addison-Wesley, Reading, MA, 3rd edition, 1998.

[9] C. V. Loan. *Computational Frameworks for the Fast Fourier Transform*. Frontiers in Applied Mathematics. SIAM, 1992.

[10] A. V. Oppenheim and R. W. Schafer. *Discrete-Time Signal Processing*. Prentice-Hall Signal Processing Series. Prentice Hall, 2010.

[11] C. Percival. Rapid multiplication modulo the sum and difference of highly composite numbers. *Math. Comp.*, 72:387–395, 2002.

[12] G. Plonka, D. Potts, G. Steidl, and M. Tasche. *Numerical Fourier Analysis*. Appl. Numer. Harm. Anal. Birkhäuser, 2018.

[13] G. Plonka and M. Tasche. Fast and numerically stable algorithms for discrete cosine transforms. *Linear Algebra Appl.*, 394:309–345, 2005.

[14] G. Ramos. Roundoff error analysis of the fast Fourier transform. *Math. Comp.*, 25(116):757–768, 1971.

[15] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing (Arch. Elektron. Rechnen)*, 7:281–292, 1971. In German.

[16] G. Strang. The discrete cosine transform. *SIAM Review*, 41(1):135–147, 1999.