Fürer's algorithm

From Wikipedia, the free encyclopedia

Fürer's algorithm is an integer multiplication algorithm for very large numbers possessing a very low asymptotic complexity. It was created in 2007 by Swiss mathematician Martin Fürer of Pennsylvania State University[1] as an asymptotically faster (when analysed on a multitape Turing machine) algorithm than its predecessor, the Schönhage–Strassen algorithm published in 1971.[2]

The predecessor to the Fürer algorithm, the Schönhage–Strassen algorithm, used fast Fourier transforms to compute integer products in time $O(n \log n \log \log n)$ (in big O notation) and its authors, Arnold Schönhage and Volker Strassen, also conjectured a lower bound for the problem of $\Omega(n \log n)$. Here, n denotes the total number of bits in the two input numbers. Fürer's algorithm reduces the gap between these two bounds: it can be used to multiply binary integers of length n in time $n \log n\, 2^{O(\log^* n)}$ (or by a circuit with that many logic gates), where log*n represents the iterated logarithm operation. However, the difference between the $\log \log n$ and $2^{\log^* n}$ factors in the time bounds of the Schönhage–Strassen algorithm and the Fürer algorithm for realistic values of n is very small.[1]

In 2008, Anindya De, Chandan Saha, Piyush Kurur and Ramprasad Saptharishi[3] gave a similar algorithm that relies on modular arithmetic instead of complex arithmetic to achieve the same running time.

In 2014, David Harvey, Joris van der Hoeven, and Grégoire Lecerf[4] showed that an optimized version of Fürer's algorithm achieves a running time of $O(n \log n 2^{4 \log^* n})$, making the implied constant in the $O(\log^* n)$ exponent explicit. They also gave a modification to Fürer's algorithm that achieves $O(n \log n 2^{3 \log^* n})$

In 2015 Svyatoslav Covanov and Emmanuel Thomé provided another modifications that achieves same running time.[5] Yet, as all the other implementation, it's still not practical.[*citation needed*]

See also [edit]

- Number-theoretic transform

References [edit]

1. ^ *a* *b* Fürer, M. (2007). "Faster Integer Multiplication" in Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, June 11–13, 2007, San Diego, California, USA
2. ^ A. Schönhage and V. Strassen, "Schnelle Multiplikation großer Zahlen", Computing 7 (1971), pp. 281–292.
3. ^ Anindya De, Piyush P Kurur, Chandan Saha, Ramprasad Saptharishi. Fast Integer Multiplication Using Modular Arithmetic. Symposium on Theory of Computation (STOC) 2008. arXiv:0801.1416
4. ^ David Harvey, Joris van der Hoeven, and Grégoire Lecerf, "Even faster integer multiplication", 2014, arXiv:1407.3360
5. ^ Svyatoslav Covanov and Emmanuel Thomé, "Fast arithmetic for faster integer multiplication", 2015 arXiv:1502.02800

V · T · E	Number-theoretic algorithms [hide]
Primality tests	AKS TEST · APR TEST · Baillie–PSW · ECPP TEST · Elliptic curve · Pocklington · Fermat · Lucas · *Lucas–Lehmer* · *Lucas–Lehmer–Riesel* · *Proth's theorem* · *Pépin's* · Quadratic Frobenius test · Solovay–Strassen · Miller–Rabin
Prime-generating	Sieve of Atkin · Sieve of Eratosthenes · Sieve of Sundaram · Wheel factorization
Integer factorization	Continued fraction (CFRAC) · Dixon's · Lenstra elliptic curve (ECM) · Euler's · Pollard's rho · *p* − 1 · *p* + 1 · Quadratic sieve (QS) · General number field sieve (GNFS) · *Special number field sieve (SNFS)* · Rational sieve · Fermat's · Shanks' square forms · Trial division · Shor's
Multiplication	Ancient Egyptian · Long · Karatsuba · Toom–Cook · Schönhage–Strassen · **Fürer's**
Discrete logarithm	Baby-step giant-step · Pollard rho · Pollard kangaroo · Pohlig–Hellman · Index calculus · Function field sieve
Greatest common divisor	Binary · Euclidean · Extended Euclidean · Lehmer's
Modular square root	Cipolla · Pocklington's · Tonelli–Shanks

Other algorithms	Chakravala · Cornacchia · Integer relation · Integer square root · Modular exponentiation · Schoof's
Italics indicate that algorithm is for numbers of special forms · SMALLCAPS indicate a deterministic algorithm	

This algorithms or data structures-related article is a stub. You can help Wikipedia by expanding it.

Categories: Computer arithmetic algorithms | Algorithms and data structures stubs | Computer science stubs