THE WORK OF RICHARD P. BRENT

1969 — 2016

Introduction. Brent's work in Computer Science and Mathematics is well-known and widely cited [192]. This document outlines his contributions to parallel algorithms, analysis of algorithms, pseudo-random number generation, number-theoretic and high-precision computations, optimisation, zero-finding, combinatorics, etc. Brent's work has been influential in the development of several of these fields.

Early Papers. Brent's first paper [1] is on software for automatic contouring, and dates from the period in 1968 when he was working as a programmer in the Monash University Computer Centre before starting his studies at Stanford [193].

Brent's second publication [2] is a report on a project done at Stanford in 1969–70. It considers the (then new) algorithm for matrix multiplication by Strassen [178], and similar algorithms. Although never submitted to a journal, it is still quoted as it contains the first floating-point error analysis of such algorithms. The error analysis of Strassen's algorithm shows that, although it is not as stable componentwise as the normal algorithm, it is sufficiently stable to be usable in implementations of Level 3 Basic Linear Algebra Subroutines (BLAS) [194]. The conjecture [2, pg. 42] that 3×3 matrix multiplication can be performed with 23 multiplications was later proved by Laderman [148]. Stability results for an algorithm of Winograd [190] were published in Brent's fourth paper [4].

Brent's third paper [3] resulted from an assignment at Stanford [195]. In it, an upper bound is derived for the time required to add n-bit numbers modulo 2^n, using circuit elements with a limited fan-in and unit delay, and assuming that all numbers have the usual binary encoding. The upper bound is within a factor $1 + o(1)$ of Winograd's lower bound [188] (which holds for all encodings) as $n \to \infty$, and only $O(n \log n)$ circuit elements are required. It was discovered later that this result had been proved independently by Ofman [167].

While at Stanford (1968–1971), Brent considered the distribution of gaps between primes, but this work was not published until later. His Ph.D. thesis was on a quite different topic: optimisation and zero-finding algorithms. Brent's book *Algorithms for Minimization without Derivatives* [6] was a revision of his thesis, the main change being that the programs were translated from Algol into Fortran.

Parallel Algorithms. Parallel computation is one of the most active areas of Computer Science. Brent is a pioneer in the development and analysis of parallel algorithms.

Brent's results [12, 15] on parallel evaluation of arithmetic expressions show that arithmetic expressions in n distinct variables can be evaluated in $O(\log n)$ parallel steps using $O(n/\log n)$ processors. The result is the best possible, up to small constant factors. It should be compared with the well-known result of Valiant *et al* [184] that any multivariate polynomial of degree d that can be evaluated sequentially in n steps can also be evaluated in $O((\log d)(\log nd))$ parallel steps using $O(n^3d^6)$ processors [196]. Valiant's result is more general, but weaker, because of the $\log d$ terms in the time bound and the much larger number of processors. Both results apply to Boolean expressions, so they have implications for the design of circuits with small depth, i.e. small delay. Brent's result improved on earlier joint work with Kuck and Maruyama [9, 197] and various results for restricted classes of expressions, for example [161]. It inspired further work by Winograd [191], Muller and Preparata [160], Preparata, Muller and Barak [170], Miller and Reif [155], Miller, Ramachandran and Kaltofen [156], Miller and Teng [157], and others.

The *systolic array* [198, 199] is a particularly simple form of parallel computer. In joint work with H. T. Kung and Franklin T. Luk, Brent obtained several important results for computations on systolic arrays. In [41, 42], he showed how integer and polynomial greatest common divisor (GCD) problems could be evaluated in linear time on a linear systolic array. The polynomial GCD problem has applications to decoding of Reed-Solomon and other error-detecting codes [121, 171]. The integer GCD problem is of interest because it is not known whether it is in the class NC [200]. In fact, the fastest known parallel algorithm for the integer GCD problem is only slightly faster than the Brent-Kung algorithm, although it uses many more processors [122].

Jointly with Luk, Brent pioneered the use of Jacobi-like algorithms for the singular value decomposition (SVD) and symmetric eigenvalue problem on systolic arrays [4, 201]. These algorithms are competitive with more traditional algorithms [202] on local-memory computers, and have good numerical properties [135]. Brent and Luk [43, 44] also gave practical linear-time algorithms for the solution of Toeplitz systems on linear systolic arrays. The results of Brent and Luk have many applications in digital signal processing [137].

Brent's work on parallel algorithms includes the development of practical algorithms for linear algebra [73] and sorting [80] on distributed-memory MIMD computers.

In the 1990s, Brent was joint leader (with Robin B. Stanton) of the ANU-Fujitsu CAP Project [203], a collaborative R&D project to develop systems and applications software for MIMD computers such as the Fujitsu AP1000/AP3000. Some highlights of this project were the implementation of parallel Linux, parallel file systems, and parallel sorting algorithms. At that time, Brent was also joint leader (with Michael R. Osborne) of a project [204] to develop scientific subroutine libraries on parallel/vector computers such as the Fujitsu VPP300.

VLSI Design and Area-Time Bounds. Early results [205] on the complexity of computational circuits counted *gates* and *gate delays* but ignored *wires* and *propagation delays.* With the introduction of "very large scale integration" (VLSI), a more realistic model which took wires into account was required. Brent and Kung introduced such a model in an influential paper [33] which established a lower bound $AT = \Omega(n^{3/2})$ on the product of the area A and time T required for the fundamental problem of n-bit binary multiplication [206]. The technique was extended to decision problems in [39]. The results give nontrivial examples of a common phenomenon: there is usually a tradeoff between the area A and time T required for a computation on a VLSI chip [183].

Binary trees are fundamental data structures. Brent and Kung [34] used geometric arguments to obtain a lower bound on the area of binary tree layouts, with significant practical implications for VLSI design.

Parallel prefix computation is a fundamental technique in parallel processing [141, 149]. Brent and Kung [37] showed how to apply it to the design of VLSI carry-lookahead adders. At the time the use of carry-lookahead in VLSI designs was unpopular [154], but the Brent-Kung design technique has been applied widely in VLSI implementations of adders [139, 182, 187].

Computational Complexity and Analysis of Algorithms. "Hash coding" (aka "scatter storage") is an important programming technique, described for example by Knuth [146, Ch. 6]. In [7], Brent describes and analyses an algorithm that reduces the retrieval time at the expense of increasing the cost of insertion. This is worthwhile in many applications where items are, on average, retrieved several times.

In an early and significant paper on the *analytic* [207] computational complexity of approximating zeros of functions of one variable, Brent, Winograd and Wolfe [10] showed that locally convergent iterations which use only evaluations of $f, f', \ldots, f^{[d]}$ have order bounded above by $d+2$. This result is best possible [208] and attainable.

Symbolic computation often involves the manipulation of formal power series in one or more variables. Brent and Kung [28] established the best known upper bounds on the complexity of *composition* and *reversion* of power series in one variable, and showed the equivalence of the composition and reversion problems, up to constant factors [209]. For power series satisfying first and second-order ordinary differential equations, which includes most power series of interest in computation,

$O(n \log n)$ algorithms were given. The results were later extended to dense multivariate power series [24] and to generalised composition [31].

The Euclidean algorithm for finding greatest common divisors is one of the first and best-analysed of algorithms. An interesting variant is the *binary* Euclidean algorithm, which has potential advantages on a binary computer because the only divisions required are by powers of two. Brent was the first to give a realistic model for the binary Euclidean algorithm, in his 1976 paper [23]. This paper made some assumptions and conjectures that have taken almost forty years to resolve satisfactorily, see [210].

Floating-Point Arithmetic and High-Precision Computations. Brent's interest in *arithmetic* covers a broad range, from computer hardware to software for high-precision computations. Results on binary addition [3, 37] are discussed above. A non-trivial bound on the error in floating-point *complex* multiplication is given in [93], improving on well-known bounds [140, 168].

Brent [11] was one of the first papers to show clearly the advantages of binary rounded arithmetic over other systems (e.g. base 16) which were popular at the time for floating-point arithmetic [211].

Brent [22] established the best known upper bounds on the complexity of high precision evaluation of elementary functions. Essentially, an n-bit result can be obtained with $O(\log n)$ multiplications of $O(n)$-bit numbers. Special cases include the evaluation of constants such as π. The idea is to use quadratically convergent iterations such as Gauss's arithmetic-geometric mean or Landen transformations. The elegant quadratically convergent algorithm for π (discovered independently by Brent [19, 22] and Salamin [174]) motivated the Borwein brothers' book *Pi and the AGM* [123].

No quadratically convergent algorithm is known for the computation of Euler's constant γ. A fast algorithm [212] was given by Brent and McMillan [30, 142, 213]. It has never been proved that γ is irrational, but [30] shows that, if $\gamma = p/q$ is rational, then $|q| > 10^{15000}$.

The paper [32] described the principal approaches possible for *unrestricted* numerical algorithms for the computation of elementary and special functions. Here *unrestricted* means that no *a priori* bounds are placed on the precision required [214]. The algorithms of [32] are generally more practical and cover a wider class of functions than those of [22].

Algorithms intended for digital computers are of little practical use without reliable software implementations. Brent's MP package [26, 27] for multiple-precision floating-point arithmetic implemented the algorithms of [32] (and some of [21]). The algorithms used in MP have been adopted in several other software packages [215]. MP has been used, for example, in work by Briggs [124] on the Feigenbaum constants, Odlyzko and te Riele [166] in their disproof of the Mertens conjecture, Odlyzko [163, 165] on the zeros of the Riemann zeta function, and Csordas *et al* [133, 164] on the computation of the de Bruijn-Newman constant.

In high-precision computations, Bernoulli numbers are often required because of their appearance in the Euler-Maclaurin formula. Brent and Harvey [102] gave asymptotically fast algorithms for the computation of the first n Bernoulli, Tangent, and Secant numbers.

Collaboration with Paul Zimmermann. Since about 1998, Brent collaborated extensively with Paul Zimmermann (Nancy) on topics related to multiple-precision arithmetic (e.g. in the specification and analysis of algorithms used in the MPFR package [216]). One outcome of this collaboration was the book *Modern Computer Arithmetic*, published by Cambridge University Press [95]. This was an attempt to present concisely all important state-of-the-art algorithms for multiple precision arithmetic. Thus, it provides an update to the parts of Knuth [145, Ch. 4] that deal with this topic. Several new algorithms were discovered while the book was being written, e.g. an asymptotically fast algorithm for computing the Jacobi symbol [99], and fast in-place algorithms for computing Tangent and Secant numbers [95, §4.7.2].

Another part of the collaboration with Zimmermann was the computation of primitive trinomials of high (Mersenne exponent) degree over GF(2). This started with a paper [88] on trinomiais of degree 3021377, which were tested using a "classical" $O(n^2)$ algorithm. Fortunately, faster algorithms were soon found, allowing the search for primitive trinomials to keep up with the Mersenne exponents being found by the GIMPS project [217]. For a summary, see the *AMS Notices* paper [98], and for a more recent update, see [115]. Perhaps more significant than the computation of specific primitive trinomials was the development of algorithms and software for efficient computation in the polynomial ring GF(2)[x], see for example [96, 97]. Also important was the emphasis on verifiability of the computational results – for example by publishing "certificates" that could easily be verified by an independent computation. Brent was aware of the need for verifiability since his contribution to the discovery of the "Pentium bug" by Nicely [218].

Pseudo-Random Number Generators. The fundamental results on linear recurrences of integers mod m were obtained many years ago [186]. Brent [70] obtained a surprising new result on the period of three-term linear recurrences mod 2^w. The result has applications to the popular class of "generalised Fibonacci" pseudo-random number generators, which are one application of his work with Zimmermann on the computation of primitive trinomials, mentioned above. Brent has made significant contributions to the development of uniform [69, 92, 94, 100] and normal [16, 75, 83, 90] random number generators. He has also considered efficient algorithms for random number generation on different computer architectures, e.g. vector and parallel computers [69, 86] and GPUs [101].

Number Theory. The *Riemann Hypothesis* (RH) is a famous open problem with many consequences in analytic number theory. If false, it could (in principle) be disproved by numerical computations with rigorous error bounds. Using an improvement of a method due to Lehmer, Turing and Littlewood, Brent [29] showed that the first $75,000,000$ zeros $\sigma + it$ of the Riemann zeta function $\zeta(s)$ in the upper half-plane are simple and lie on the critical line $\sigma = \frac{1}{2}$. This is as expected if RH is true. Various interesting empirical results on the distribution of the zeros were obtained in the course of the computation. Using essentially the same method, the result was extended to the first 200,000,000 zeros in [40, 46]. It has been extended even further by later authors.

Brent's papers related to the theory of $\zeta(s)$ include [105, 106], which consider the sign of $\Re(\zeta(s))$ in the region to the right of the critical line, and [116], which gives error bounds on asymptotic approximations to the Riemann-Siegel theta function.

Several of Brent's papers considered the empirical distribution of (rational) primes. For example, in [17] he showed that primes and twin primes behave in a very different manner (at least up to 10^{11}), and obtained an estimate for Brun's constant [218]. Related papers are [14] on a consequence of the conjecture of Hardy and Littlewood [138] on the distribution of *small* gaps between primes, and [13, 35] on *large* gaps between consecutive primes.

Brent has made significant contributions to the theory and implementation of integer factorisation algorithms, a topical subject given the ubiquity of "public key" cryptosystems whose security depends on the (assumed) difficulty of integer factorisation [66, 173]. The papers [61, 63] announced the complete factorisation of the Fermat number $F_{11} = 2^{2^{11}} + 1$ by Brent's variant [54, 57] of Lenstra's *elliptic curve method* (ECM) [151]. This was a surprise, since Brent and Pollard [38] had factored F_8 (by a different method), but F_9 and F_{10} had not been completely factored [219]. The factorisation of F_{10} was completed by Brent in October 1995: see [81].

The factorisation of F_{10} and F_{11} used Brent's improvement of the elliptic curve method. Brent has also contributed to the development of the *number field sieve* (NFS). In fact, two of Brent's students (Brian Murphy and Shi Bai) wrote their Ph.D. theses on polynomial selection in NFS. See, for example, the joint papers [84, 108].

The existence of odd perfect numbers is an old open problem [220]. Brent, Cohen and te Riele [55, 64] extended the lower bound on an odd perfect number (if one exists) from 10^{50} to 10^{300}. This required both new mathematical results [221] and good implementations of modern integer factorisation algorithms [222].

The factorisations required for [64] formed the basis for a significant extension, by Brent, Montgomery and te Riele [71, 89], of the "Cunningham" tables [125] of factors of integers of the form $a^n \pm 1$.

The cyclotomic polynomials $\Phi_n(z)$ satisfy well-known identities of Gauss, Aurifeuille and Lucas [172, 176]. Brent [68, 72] gave efficient algorithms for computing the polynomials occurring in these identities. He also gave explicit generating functions for these polynomials, and closed-form expressions for the corresponding Aurifeuillian factors of certain integers of the form $a^n \pm 1$. The generating functions display an interesting connection with Dirichlet L-functions and the theory of quadratic fields.

Most of Brent's number-theoretic work has had a computational flavour, but recently he collaborated with Michael Coons and Wadim Zudilin to give a new method for algebraic independence results in the context of Mahler's method [112, 152]. It should be noted that Kurt Mahler provided some motivation for the development of the MP package (described above) by asking computational questions that were too difficult for his calculator to solve. Mahler was interested in the accurate computation of $e^{\pi\sqrt{r}}$ for certain rational r. One example is $e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999925$, which is known to be a transcendental number, but is very close to an integer. This can be explained by the theory of modular forms [127].

Solution of Structured Linear Systems. Brent has made several significant contributions to algorithms for the solution of Toeplitz [223] systems of linear equations and Toeplitz least squares problems. Linear-time algorithms for systolic arrays are mentioned above.

By classical results of Kolmogorov, Wiener and Levinson [224], n by n Toeplitz linear systems can be solved in $O(n^2)$ operations. Brent, Gustavson and Yun [36] showed that $O(n(\log n)^2)$ algorithms exist. The algorithms depend on the close connection between computation of the Padé table, or the continued fraction expansion, of a power series, and the solution of a Toeplitz system. The result motivated the development of several other $O(n(\log n)^2)$ algorithms [58, 118, 120, 134]. The algorithms just mentioned are generally numerically unstable unless special conditions (e.g. positive definiteness) are imposed. There is much interest in the stable solution of unsymmetric or indefinite n by n Toeplitz systems $Ax = b$ in $o(n^3)$ operations. Bojanczyk, Brent and de Hoog [52] showed how the orthogonal factorisation $A = QR$ of the Toeplitz matrix A could be computed in $O(n^2)$ steps on a sequential computer, and in $O(n)$ steps on a parallel computer with $O(n)$ processors [225]. The algorithm is a significant improvement over an earlier (unstable and inherently sequential) algorithm of Sweet [180], and gives a weakly stable [226] algorithm for the solution of Toeplitz linear systems and linear least squares problems [59]. Later work on the stability of fast algorithms for Toeplitz and related matrix problems, in collaboration with Bojanczyk, de Hoog and Sweet, may be found in [76, 77, 79]. For example, in [77] the stability of the Bareiss (Schur) algorithm was shown to be similar to that of Gaussian elimination [227].

Optimisation and Solution of Nonlinear Algebraic Systems. The monograph *Algorithms for Minimization without Derivatives* [6] considers algorithms for zero-finding and optimisation under the constraint that only function (not derivative) evaluations are permitted. It improves on Dekker's algorithm for the problem of finding a zero of a function of one variable, and gives an analogous algorithm for minimisation of a function of one variable. Implementations of these algorithms are still in wide use. Other problems considered in [6] include the global optimisation of a function of a small number of variables, given bounds on derivatives; and the unconstrained optimisation of a function of several variables. Some modifications to Powell's (1964) algorithm [169] are suggested.

In [8] Brent considered efficient methods for approximating the solution of a system of nonlinear equations, using only function evaluations. He improved on the method of Brown and Conte [126] by using (numerically stable) orthogonal transformations and optimising the Ostrowski efficiency. Brent's method is still widely used and recommended [158].

Other papers on zero-finding algorithms include [5, 18, 19].

Training Neural Networks. In [65], Brent described a fast training algorithm for multi-layer feed-forward neural nets [132]. The algorithm is much faster than the popular but inefficient "back propagation" algorithm. It also demonstrates a close connection between neural nets and older classification and data retrieval methods in common use by statisticians and computer scientists.

Combinatorics. Brent and McKay [56] is an early work with a combinatorial flavour. It considers the distribution of ranks of random $n \times n$ symmetric matrices in the ring $\mathbb{Z}_m$.

Since 2008, Brent has collaborated with Judy-anne Osborn, Will Orrick, Warren Smith and Paul Zimmermann on the *Hadamard maximal determinant problem*, which asks for bounds on the maximal determinant of a square $\{\pm 1\}$-matrix [228]. Results of this collaboration were the determination of the "maxdet" matrices of orders 19 and 37 in [103], the development of randomised switching algorithms to search large spaces [104], and the proof of new bounds on the maxdet problem by both deterministic [107] and probabilistic [110, 113] methods. In general, the probabilistic method gives sharper results.

The work on probabilistic lower bounds has had some surprising spinoffs, including new bounds on determinants of perturbations of the identity matrix [111], and the discovery of a family of discrete analogues of Macdonald-Mehta integrals [114] that can be expressed as products of Gamma functions.

Biblography, Notes and References. In the following list, the first part has selected publications by Brent, the second part has references to other authors, and the third part has additional notes. A complete list of Brent's publications is available online [229].

[1] M. P. C. Legg and R. P. Brent, Automatic contouring, *Proceedings of the Fourth Australian Computer Conference*, Australian Computer Society, Adelaide, 1969, 467–468.

[2] R. P. Brent, *Algorithms for matrix multiplication*, Report TR-CS-70-157, DCS, Stanford (March 1970), 52 pp. Available from `http://elib.stanford.edu/`.

[3] R. P. Brent, On the addition of binary numbers, *IEEE Transactions on Computers* C-19 (1970), 758–759.

[4] R. P. Brent, Error analysis of algorithms for matrix multiplication and triangular decomposition using Winograd's identity, *Numerische Mathematik* 16 (1970), 145–156.

[5] R. P. Brent, An algorithm with guaranteed convergence for finding a zero of a function, *Computer J.* 14 (1971), 422–425.

[6] R. P. Brent, *Algorithms for Minimization without Derivatives*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973, 195 pp.

[7] R. P. Brent, Reducing the retrieval time of scatter storage techniques, *Communications of the ACM* 16 (1973), 105–109.

[8] R. P. Brent, Some efficient algorithms for solving systems of nonlinear equations, *SIAM J. Numerical Analysis* 10 (1973), 327–344.

[9] R. P. Brent, D. J. Kuck and K. Maruyama, The parallel evaluation of arithmetic expressions without division, *IEEE Transactions on Computers* C-22 (1973), 532–534.

[10] R. P. Brent, S. Winograd and P. Wolfe, Optimal iterative processes for rootfinding, *Numerische Mathematik* 20 (1973), 327–341.

[11] R. P. Brent, On the precision attainable with various floating-point number systems, *IEEE Transactions on Computers* C-22 (1973), 601–607.

[12] R. P. Brent, The parallel evaluation of arithmetic expressions in logarithmic time, in *Complexity of Sequential and Parallel Numerical Algorithms* (edited by J. F. Traub), Academic Press, New York, 1973, 83–102.

[13] R. P. Brent, The first occurrence of large gaps between successive primes, *Mathematics of Computation* 27 (1973), 959–963.

[14] R. P. Brent, The distribution of small gaps between successive primes *Mathematics of Computation* 28 (1974), 315–324.

[15] R. P. Brent, The parallel evaluation of general arithmetic expressions, *J. ACM* 21 (1974), 201–206.

[16] R. P. Brent, Algorithm 488: A Gaussian pseudo-random number generator [G5], *Communications of the ACM* 17 (1974), 704–706.

[17] R. P. Brent, Irregularities in the distribution of primes and twin primes, *Mathematics of Computation* 29 (1975), 43–56.

[18] R. P. Brent, Some high-order zero-finding methods using almost orthogonal polynomials, *J. Australian Mathematical Society (Series B)* 19 (1975), 1–29.

[19] R. P. Brent, Multiple-precision zero-finding methods and the complexity of elementary function evaluation, in *Analytic Computational Complexity* (edited by J. F. Traub), Academic Press, New York, 1975, 151–176.

[20] R. S. Anderssen and R. P. Brent (editors), *The Complexity of Computational Problem Solving*, University of Queensland Press, Brisbane, 1976, 262 pp.

[21] R. P. Brent, The complexity of multiple-precision arithmetic, in [20], 126–165. arXiv:1004.3608v1.

[22] R. P. Brent, Fast multiple-precision evaluation of elementary functions, *J. ACM* 23 (1976), 242–251.

[23] R. P. Brent, Analysis of the binary Euclidean algorithm, in *New Directions and Recent Results in Algorithms and Complexity* (edited by J. F. Traub), Academic Press, New York, 1976, 321–355. For errata see [85].

[24] R. P. Brent and H. T. Kung, Fast algorithms for composition and reversion of multivariate power series, in *Proceedings of a Conference on Theoretical Computer Science* held at the University of Waterloo, DCS, University of Waterloo, Waterloo, Ontario (August 1977), 149–158.

[25] R. P. Brent, Computation of the regular continued fraction for Euler's constant, *Mathematics of Computation* 31 (1977), 771–777.

[26] R. P. Brent, A Fortran multiple-precision arithmetic package, *ACM Transactions on Mathematical Software* 4 (1978), 57–70.

[27] R. P. Brent, Algorithm 524: MP, a Fortran multiple-precision arithmetic package [A1], *ACM Transactions on Mathematical Software* 4 (1978), 71–81.

[28] R. P. Brent and H. T. Kung, Fast algorithms for manipulating formal power series, *J. ACM* 25 (1978), 581–595.

[29] R. P. Brent, On the zeros of the Riemann zeta function in the critical strip, *Mathematics of Computation* 33 (1979), 1361–1372.

[30] R. P. Brent and E. M. McMillan, Some new algorithms for high-precision computation of Euler's constant, *Mathematics of Computation* 34 (1980), 305–312.

[31] R. P. Brent and J. F. Traub, On the complexity of composition and generalized composition of power series, *SIAM J. Computing* 9 (1980), 54–66.

[32] R. P. Brent, Unrestricted algorithms for elementary and special functions, in *Information Processing 80* (edited by S. H. Lavington), North-Holland, Amsterdam, 1980, 613–619.

[33] R. P. Brent and H. T. Kung, The area-time complexity of binary multiplication, *J. ACM* 28 (1981), 521–534.

[34] R. P. Brent and H. T. Kung, On the area of binary tree layouts, *Information Processing Letters* 11 (1980), 46–48.

[35] R. P. Brent, The first occurrence of certain large prime gaps, *Mathematics of Computation* 35 (1980), 1435–1436.

[36] R. P. Brent, F. G. Gustavson and D. Y. Y. Yun, Fast solution of Toeplitz systems of equations and computation of Padé approximants, *J. Algorithms* 1 (1980), 259–295.

[37] R. P. Brent and H. T. Kung, A regular layout for parallel adders, *IEEE Transactions on Computers* C-31 (1982), 260–264.

[38] R. P. Brent and J. M. Pollard, Factorization of the eighth Fermat number, *Mathematics of Computation* 36 (1981), 627–630.

[39] R. P. Brent and L. M. Goldschlager, Some area-time tradeoffs for VLSI, *SIAM J. on Computing* 11 (1982), 737–747.

[40] R. P. Brent, J. van de Lune, H. J. J. te Riele and D. T. Winter, On the zeros of the Riemann zeta function in the critical strip, II, *Mathematics of Computation* 39 (1982), 681–688.

[41] R. P. Brent and H. T. Kung, Systolic VLSI arrays for polynomial GCD computation, *IEEE Transactions on Computers* C-33 (1984), 731–736.

[42] R. P. Brent and H. T. Kung, A systolic VLSI array for integer GCD computation, in *ARITH-7, Proceedings of the Seventh Symposium on Computer Arithmetic* (edited by K. Hwang), IEEE/CS Press, 1985, 118–125.

[43] R. P. Brent and F. T. Luk, A systolic array for the linear-time solution of Toeplitz systems of equations, *J. of VLSI and Computer Systems* 1, 1 (1983), 1–23.

[44] R. P. Brent, H. T. Kung and F. T. Luk, Some linear-time algorithms for systolic arrays, in *Information Processing 83* (edited by R.E.A. Mason), North-Holland, Amsterdam, 1983, 865–876.

[45] R. P. Brent, F. T. Luk and C. F. Van Loan, Computation of the singular value decomposition using mesh-connected processors, *J. of VLSI and Computer Systems* 1, 3 (1983–1985), 242–270.

[46] R. P. Brent, J. van de Lune, H. J. J. te Riele and D. T. Winter, The First $200,000,001$ zeros of Riemann's zeta function, in *Computational Methods in Number Theory* (edited by H. W. Lenstra, Jr. and R. Tijdeman), Mathematical Centre Tracts 154, Mathematisch Centrum, Amsterdam, 1982, 389–403.

[47] R. P. Brent and H. T. Kung, Systolic VLSI arrays for linear-time GCD computation, in *VLSI 83* (edited by F. Anceau and E. J. Aas), North-Holland, Amsterdam, 1983, 145–154.

[48] R. P. Brent, F. T. Luk and C. F. Van Loan, Computation of the generalized singular value decomposition using mesh-connected processors, *Proceedings SPIE, Volume 431, Real Time Signal Processing VI* (edited by Keith Bromley), Society of Photo-Optical Instrumentation Engineers, Bellingham, Washington, 1983, 66–71.

[49] R. P. Brent and F. T. Luk, The solution of singular-value and symmetric eigenvalue problems on multiprocessor arrays, *SIAM J. Scientific and Statistical Computing* 6 (1985), 69–84.

[50] R. P. Brent and F. T. Luk, The solution of singular-value problems using systolic arrays, *Proceedings SPIE, Volume 495, Real Time Signal Processing VII*, Society of Photo-Optical Instrumentation Engineers, Bellingham, Washington, 1984, 7–12.

[51] R. P. Brent, Efficient implementation of the first-fit strategy for dynamic storage allocation, *ACM Trans. on Programming Languages and Systems* 11 (1989), 388–403.

[52] A. W. Bojanczyk, R. P. Brent and F. R. de Hoog, QR factorization of Toeplitz matrices, *Numerische Mathematik* 49 (1986), 81–94.

[53] A. W. Bojanczyk and R. P. Brent, A systolic algorithm for extended GCD computation, *Comput. Math. Applic.* 14 (1987), 233–238.

[54] R. P. Brent, *Some integer factorization algorithms using elliptic curves*, Report CMA-R32-85, CMA, ANU, September 1985, 20 pp. A revision appeared as [57].

[55] R. P. Brent and G. L. Cohen, A new lower bound for odd perfect numbers, *Mathematics of Computation* 53 (1989), 431–437.

[56] R. P. Brent and B. D. McKay, On determinants of random symmetric matrices over $\mathbb{Z}_m$, *Ars Combinatoria* 26A (1988), 57–64. arXiv:1004.5440v1.

[57] R. P. Brent, Some integer factorization algorithms using elliptic curves, *Proceedings of the Ninth Australian Computer Science Conference*, *Australian Computer Science Communications* 8 (1986), 149–163. Also arXiv:1004.3366v1.

[58] R. P. Brent, Old and new algorithms for Toeplitz systems (keynote address), *Proceedings SPIE, Volume 975, Advanced Algorithms and Architectures for Signal Processing III* (edited by F. T. Luk), Society of Photo-Optical Instrumentation Engineers, Bellingham, Washington, 1989, 2–9.

[59] R. P. Brent, Parallel algorithms for Toeplitz systems, *Numerical Linear Algebra, Digital Signal Processing and Parallel Algorithms* (edited by G. H. Golub and P. Van Dooren), Springer-Verlag, 1991, 75–92.

[60] R. P. Brent, F. T. Luk and C. J. Anfinson, Checksum schemes for fault tolerant systolic computing, *Mathematics in Signal Processing II* (edited by J. G. McWhirter), Clarendon Press, Oxford, 1990, 791–804.

[61] R. P. Brent, Factorization of the eleventh Fermat number (preliminary report), *AMS Abstracts* 10 (1989), 89T-11-73.

[62] R. P. Brent, F. T. Luk and C. J. Anfinson, Choosing small weights for multiple error detection, *Proceedings SPIE, Volume 1058, High Speed Computing II*, Society of Photo-Optical Instrumentation Engineers, Los Angeles, 1989, 130–136.

[63] R. P. Brent, Parallel algorithms for integer factorisation, *Number Theory and Cryptography* (edited by J. H. Loxton), London Mathematical Society Lecture Note Series 154, Cambridge University Press, 1990, 26–37.

[64] R. P. Brent, G. L. Cohen and H. J. J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Mathematics of Computation* 57 (1991), 857–868.

[65] R. P. Brent, Fast training algorithms for multi-layer neural nets, *IEEE Transactions on Neural Networks* 2 (1991), 346–354.

[66] R. P. Brent, Primality testing and integer factorisation, in *The Role of Mathematics in Science* (Proceedings of a Symposium held at the Australian Academy of Science, Canberra, 20 April 1990), Australian Academy of Science, 1991, 14–26.

[67] D. L. Boley, R. P. Brent, G. H. Golub and F. T. Luk, Algorithmic fault tolerance using the Lanczos method, *SIAM J. Matrix Analysis and Applications* 13 (1992), 312–332.

[68] R. P. Brent, Computing Aurifeuillian factors, in *Computational Algebra and Number Theory* (edited by W. Bosma and A. van der Poorten), Mathematics and its Applications, vol. 325, Kluwer Academic Publishers, Boston, 1995, 201–212.

[69] R. P. Brent, Uniform random number generators for supercomputers, *Proc. Fifth Australian Supercomputer Conference*, Melbourne, December 1992, 95–104.

[70] R. P. Brent, On the periods of generalized Fibonacci recurrences, *Mathematics of Computation* 63 (1994), 389–401.

[71] R. P. Brent and H. J. J. te Riele, Factorizations of $a^n \pm 1$, $13 \le a < 100$, Report NM-R9212, Centrum voor Wiskunde en Informatica, Amsterdam, June 1992, v+363 pp.

[72] R. P. Brent, On computing factors of cyclotomic polynomials, *Mathematics of Computation* 61 (1993), 131–149.

[73] R. P. Brent and P. E. Strazdins, Implementation of the BLAS level 3 and Linpack benchmark on the AP 1000, *Fujitsu Scientific and Technical Journal* 29, 1 (March 1993), 61–70.

[74] R. P. Brent, An asymptotic expansion inspired by Ramanujan, *Austral. Math. Soc. Gazette* 20 (December 1993), 149–155.

[75] R. P. Brent *Fast normal random number generators on vector processors,* Technical Report TR-CS-93-04, CSL, ANU, March 1993, 6 pp. arXiv:1004.3105v2.

[76] A. W. Bojanczyk, R. P. Brent and F. R. de Hoog, Stability analysis of a general Toeplitz system solver, *Numerical Algorithms* 10 (1995), 225–244.

[77] A. W. Bojanczyk, R. P. Brent, F. R. de Hoog and D. R. Sweet, On the stability of the Bareiss and related Toeplitz factorization algorithms, *SIAM J. Matrix Analysis and Applications* 16 (1995), 40–57.

[78] R. P. Brent, A. J. Cleary, M. Hegland, J. H. Jenkinson, Z. Leyk, M. Nakanishi, M. R. Osborne, P. J. Price, S. Roberts and D. B. Singleton, Implementation and performance of scalable scientific library subroutines on Fujitsu's VPP500 parallel-vector supercomputer, *Proceedings of the Scalable High Performance Computing Conference*, (Knoxville, Tennessee, 23–25 May, 1994), IEEE Computer Society Press, Los Alamitos, California, 1994, 526–533.

[79] D. R. Sweet and R. P. Brent, Error analysis of a fast partial pivoting method for structured matrices, *Proceedings SPIE, Volume 2363, Advanced Signal Processing Algorithms*, (edited by F. Luk), Society of Photo-Optical Instrumentation Engineers, Bellingham, Washington, 1995, 266–280. arXiv:1005.0667v1.

[80] A. Tridgell and R. P. Brent, A general-purpose parallel sorting algorithm, *International J. of High Speed Computing* 7 (1995), 285–301.

[81] R. P. Brent, Factorization of the tenth Fermat number, *Mathematics of Computation* 68 (1999), 429–451.

[82] R. P. Brent, A. J. van der Poorten and H. J. J. te Riele, A comparative study of algorithms for computing continued fractions of algebraic numbers (extended abstract), in *Algorithmic Number Theory* (edited by Henri Cohen), *Lecture Notes in Computer Science*, Vol. 1122, Springer-Verlag, Berlin, 1996, 35–47.

[83] R. P. Brent, *A fast vectorised implementation of Wallace's normal random number generator,* Technical Report TR-CS-97-07, CSL, ANU, April 1997, 9 pp. arXiv:1004.3114v1.

[84] B. A. Murphy and R. P. Brent, On quadratic polynomials for the number field sieve, *Australian Computer Science Communications* 20, 3 (1998), 199–215.

[85] R. P. Brent, Twenty years' analysis of the binary Euclidean algorithm, in *Millennial Perspectives in Computer Science: Proceedings of the 1999 Oxford – Microsoft Symposium in honour of Professor Sir Antony Hoare* (edited by J. Davies, A. W. Roscoe and J. Woodcock), Palgrave, New York, 2000, 41–53. Extended version: arXiv:1303.2772v1.

[86] R. P. Brent, Random number generation and simulation on vector and parallel computers (extended abstract), *Lecture Notes in Computer Science* 1470, Springer-Verlag, Berlin, 1998, 1–20.

[87] R. P. Brent, L. Grosz, D. L. Harrar II, M. Hegland, M. H. Kahn, G. Keating, G. J. Mercer, M. Nakanishi, M. R. Osborne, and B. B. Zhou, Design of the scientific subroutine library for the Fujitsu VPP300, *Proc. Third High Performance Computing Asia Conference and Exhibition*, Singapore, Sept. 1998, 424–438.

[88] R. P. Brent, S. Larvala and P. Zimmermann, A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377, *Mathematics of Computation* 72 (2003), 1443–1452.

[89] R. P. Brent, P. L. Montgomery and H. J. J. te Riele, Factorizations of Cunningham numbers with bases 13 to 99, Report PRG TR-14-00, 31 December 2000, vii+502 pp. arXiv:1004.3169v2. Abridged version appeared as Report MAS-R0107, CWI, Amsterdam, July 2001, 28 pp.

[90] R. P. Brent, Some comments on C. S. Wallace's random number generators, *Computer Journal* 51 (2008), 579–584. arXiv:1005.2314v1.

[91] R. P. Brent, S. Larvala and P. Zimmermann, A primitive trinomial of degree 6972593, *Mathematics of Computation* 74 (2005), 1001–1002.

[92] R. P. Brent, Note on Marsaglia's xorshift random number generators, *Journal of Statistical Software* 11, 5 (2004), 1–4.

[93] R. P. Brent, Colin Percival and P. Zimmermann, Error bounds on complex floating-point multiplication, *Mathematics of Computation* 76 (2007), 1469–1481.

[94] R. P. Brent, Some long-period random number generators using shifts and xors, *ANZIAM J.* 48 (CTAC2006), C188–C202, 2007. arXiv:1004.3115v1.

[95] R. P. Brent and P. Zimmermann, *Modern Computer Arithmetic*, Cambridge Monographs on Applied and Computational Mathematics (No. 18), Cambridge University Press, 2010, 236 pages. arXiv:1004.4710v1.

[96] R. P. Brent and P. Zimmermann, A multi-level blocking distinct-degree factorization algorithm, in *Finite Fields and Applications* (edited by G. Mullen, D. Panario, and I. Shparlinski), *Contemporary Mathematics*, Vol. 461, 2008, 47–58. arXiv:0710.4410v1.

[97] R. P. Brent, Pierrick Gaudry, Emmanuel Thomé and P. Zimmermann, Faster Multiplication in $\mathrm{G}F(2)[x]$, *ANTS VIII 2008*, edited by A. J. van der Poorten and A. Stein, *Lecture Notes in Computer Science* 5011, 153–166.

[98] R. P. Brent and P. Zimmermann, The great trinomial hunt, *Notices of the American Mathematical Society* 58 (2011), 233–239.

[99] R. P. Brent and P. Zimmermann, An $O(M(n)\log n)$ algorithm for the Jacobi symbol, *Lecture Notes in Computer Science* 6197 (2010), 83–95. arXiv:1004.2091v2.

[100] R. P. Brent, The myth of equidistribution for high-dimensional simulation, 8 May 2010, 8 pp. arXiv:1005.1320v1.

[101] N. Nandapalan, R. P. Brent, L. M. Murray and A. Rendell, High-performance pseudo-random number generation on graphics processing units, *Lecture Notes in Computer Science*, Vol. 7203 (2012), 609–618. arXiv:1108.0486v1.

[102] R. P. Brent and D. Harvey, Fast computation of Bernoulli, Tangent and Secant numbers, *Proceedings of a Workshop on Computational and Analytical Mathematics in honour of Jonathan Borwein's* 60*-th birthday,* D. H. Bailey et al. (eds.), *Springer Proceedings in Mathematics & Statistics*, Vol. 50, 2013, 127–142. arXiv:1108.0286v3.

[103] R. P. Brent, J. Osborn, W. Orrick and P. Zimmermann, Maximal determinants and saturated D-optimal designs of orders 19 and 37, arXiv:1112.4160v1, Dec. 2011.

[104] R. P. Brent, Finding D-optimal designs by randomised decomposition and switching, *Australasian Journal of Combinatorics*, 55 (2013), 15–30. arXiv:1112.4671v5.

[105] J. Arias de Reyna, R. P. Brent and J. van de Lune, A note on the real part of the Riemann zeta-function, *Herman J. J. te Riele Liber Amicorum*, CWI, Amsterdam, Dec. 2011, 30–36. arXiv:1112.4910v2.

[106] J. Arias de Reyna, R. P. Brent and J. van de Lune, On the sign of the real part of the Riemann zeta-function, *Number Theory and Related Fields (in memory of Alf van der Poorten)*, edited by J. M. Borwein, I. Shparlinski

and W. Zudilin, Springer Proceedings in Mathematics and Statistics Vol. 43, Springer, New York, 2013, 75–97. arXiv:1205:4423v2.

[107] R. P. Brent and J. H. Osborn, General lower bounds on maximal determinants of binary matrices, *The Electronic Journal of Combinatorics* 20(2), 2013, #P15, 12 pp. arXiv:1208.1805v6.

[108] Shi Bai, R. P. Brent and E. Thomé, Root optimization of polynomials in the number field sieve, *Mathematics of Computation* 84 (2015), 2447–2457.

[109] R. P. Brent and F. Johansson, A bound for the error term in the Brent-McMillan algorithm, *Mathematics of Computation* 84 (2015), 2351–2359.

[110] R. P. Brent, J. H. Osborn and W. D. Smith, Lower bounds on maximal determinants of binary matrices via the probabilistic method, arXiv:1402.6817v5, 26 Jan. 2016.

[111] R. P. Brent, J. H. Osborn and W. D. Smith, Note on best possible bounds for determinants of matrices close to the identity matrix, *Linear Algebra and its Applications* 466 (2015), 21–26. Longer version: arXiv:1401.7084v7.

[112] R. P. Brent, M. Coons and W. Zudilin, Algebraic independence of Mahler functions via radial asymptotics, *International Mathematics Research Notices* 2016:2 (2016), 571–603. arXiv:1412.7906v2.

[113] R. P. Brent, J. H. Osborn and W. D. Smith, Probabilistic lower bounds on maximal determinants of binary matrices, *Australasian Journal of Combinatorics*, to appear. arXiv:1501.06235v5.

[114] R. P. Brent, C. Krattenthaler and [S.] O. Warnaar, Discrete analogues of Mehta-type integrals, *J. Combin. Theory Ser. A* (2016), `http://dx.doi.org/10.1016/j.jcta.2016.06.005`. arXiv 1601.06536.

[115] R. P. Brent and P. Zimmermann, Twelve new primitive binary trinomials, arXiv:1605.09213v1, 24 May 2016, 2 pp.

[116] R. P. Brent, On asymptotic approximations to the log-Gamma and Riemann-Siegel theta functions, arXiv:1609.03682, 13 Sept. 2016, 19 pp.

---

[117] H. Abelson and P. Andreae, Information transfer and area-time tradeoffs for VLSI multiplication, *Comm. ACM* 23, 1980, 20–23.

[118] G. S. Ammar and W. B. Gragg, Superfast solution of real positive definite Toeplitz systems, *SIAM J. Matrix Anal. Appl.* 9 (1988), 61–76.

[119] D. H. Bailey, Multiprecision translation and execution of Fortran programs, *ACM Transactions on Mathematical Software* 19 (1993), 288–319.

[120] R. R. Bitmead and B. D. O. Anderson, Asymptotically fast solution of Toeplitz and related systems of linear equations, *J. Linear Algebra Appl.* 34 (1980), 103–116.

[121] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, Reading, Mass., 1983. See also [60, 62, 67].

[122] A. Borodin, J. von zur Gathen and J. Hopcroft, Parallel matrix and GCD computations, *Proc. 23rd Annual IEEE Symposium on Foundations of Computer Science*, IEEE, New York, 1982, 65–71.

[123] J. M. Borwein and P. B. Borwein, *Pi and the AGM*, John Wiley and Sons, New York, 1987.

[124] K. Briggs, A precise calculation of the Feigenbaum constants, *Mathematics of Computation* 57, 1991, 435–439.

[125] J. Brillhart, H. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, American Math. Soc., Providence, Rhode Island, 2nd edition, 1985.

[126] K. M. Brown and S. D. Conte, The solution of simultaneous nonlinear equations, *Proc. 22nd National Conference of the ACM*, Thompson Book Co., Washington, D.C., 1967, 111–114.

[127] J. H. Bruinier, G. van der Geer, Günter Harder and Don Zagier, *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeld, Norway*, Springer-Verlag, Berlin, 2008, pp. 73–74.

[128] J. R. Bunch, Stability of methods for solving Toeplitz systems of equations, *SIAM J. Scientific and Statistical Computing* 6 (1985), 349–364.

[129] S. Chandrasekaran and A. H. Sayed, Stabilizing the generalized Schur algorithm, *SIMAX* 17 (1996), 950–983;

[130] C. W. Clenshaw and F. W. J. Olver, An unrestricted algorithm for the exponential function, *SIAM J. Numer. Anal.* 17, 1980, 310-331.

[131] S. A. Cook, An overview of computational complexity, *Comm. ACM* 26, 1983, 401–408.

[132] F. Crick, The recent excitement about neural networks, *Nature* 337 (1989), 129–132.

[133] G. L. Csordas, A. M. Odlyzko, W. Smith and R. S. Varga, A new Lehmer pair of zeros and a new lower bound for the de Bruijn-Newman constant Λ, *Electronic Transactions on Numerical Analysis* 1 (1993), 104–111.

[134] F. R. de Hoog, A new algorithm for solving Toeplitz systems of equations, *J. Linear Algebra Appl.* 88/89 (1987), 122–138;

[135] J. Demmel and K. Veselić, Jacobi's method is more accurate than QR, *SIAM J. Sci. Stat. Computing* 11, 1992, 1204–1246.

[136] J. Dongarra and D. Sorensen, A fully parallel algorithm for the symmetric eigenvalue problem, *SIAM J. Scientific and Statistical Computing* 8, 1987, 139–154.

[137] G. H. Golub and P. Van Dooren, *Numerical Linear Algebra, Digital Signal Processing and Parallel Algorithms*, Springer-Verlag, 1990, 93–110.

[138] G. H. Hardy and J. E. Littlewood, Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.* 44, 1923, 1–70.

[139] J. L. Hennessy, D. A. Patterson and D. Goldberg, *Computer Architecture: A Quantitative Approach*, second edition, Morgan Kaufmann, San Mateo, California, 1996, A67-A69.

[140] N. J. Higham, *Accuracy and Stability of Numerical Algorithms*, 2nd ed., SIAM, 2002.

[141] W. D. Hillis and G. Steele, Data parallel algorithms, *Comm. ACM* 12, 1986, 1170–1183.

[142] J. D. Jackson and W. K. H. Panofsky, Edwin Mattison McMillan 1907–1991, *Biographical Memoirs Nat. Acad. Sci. (USA)*, 69 (1996), 213–241.

[143] F. Johansson, A fast algorithm for reversion of power series, *Mathematics of Computation* 84 (2015), 475–484.

[144] D. E. Knuth, Euler's constant to 1271 places, *Math. Comp.* 16, 1962, 275–281.

[145] D. E. Knuth, *The Art of Computer Programming*, Vol. 2: Seminumerical Algorithms, 3rd ed., Addison-Wesley, 1997.

[146] D. E. Knuth, *The Art of Computer Programming*, Vol. 3: Sorting and Searching, 2nd ed., Addison-Wesley, 1998.

[147] H. T. Kung, Why systolic architectures?, *IEEE Computer* 15, Jan. 1982, 37–45.

[148] J. D. Laderman, A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications, *Bull. Amer. Math. Soc.* 82, (1976), 126–128.

[149] R. Ladner and M. Fischer, Parallel prefix computation, *J. ACM* 27, 1980, 831–838.

[150] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, The factorization of the ninth Fermat number, *Mathematics of Computation* 61 (1993), 319–349.

[151] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Annals of Mathematics* 126 (1987), 649–673.

[152] K. Mahler, On a special functional equation, *J. London Math. Soc.* 15 (1940), 115–123.

[153] G. Maze, Existence of a limiting distribution for the binary GCD algorithm, *J. Discrete Algorithms* 5 (2007), 176–186.

[154] C. Mead and L. Conway, *Introduction to VLSI Systems*, Addison-Wesley, 1980, Sec. 5.5.

[155] G. L. Miller and J. H. Reif, Parallel tree contraction, Part I: Fundamentals, in *Randomness and Computation* (edited by S. Micali), JAI Press, 1988.

[156] G. L. Miller, V. Ramachandran and E. Kaltofen, Efficient parallel evaluation of straight-line code and arithmetic circuits, *SIAM J. Computing* 17, 1988, 687–695.

[157] G. F. Miller and S.-H. Teng, Dynamic parallel complexity of computational circuits, *Proc. 19th Annual ACM Symposium on Theory of Computing*, ACM, New York, 1987, 254–263.

[158] J. J. Moré and M. Y. Cosnard, Numerical solution of nonlinear equations, *ACM Transactions on Mathematical Software* 5 (1979), 64–85.

[159] I. D. Morris, A rigorous version of R. P. Brent's model for the binary Euclidean algorithm, *Advances in Mathematics*, to appear. Preprint: arXiv:1409.0729v1, 2 Sept 2014.

[160] D. E. Muller and F. P. Preparata, Restructuring of arithmetic expressions for parallel evaluation, *J. ACM* 23, 1976, 534–543.

[161] I. Munro and M. Paterson, Optimal algorithm for parallel polynomial evaluation, *Proc. IEEE Twelfth Annual Symp. on Switching and Automata Theory*, 1971, 132–139.

[162] T. R. Nicely, Enumeration to 10^{14} of the Twin Primes and Brun's Constant, *Virginia Journal of Science* 46, 1995, 195-204. Reviewed by R. P. Brent in *Mathematics of Computation* 66, 924–925.

[163] A. M. Odlyzko, On the distribution of spacings between zeros of the zeta function, *Math. Comp.* 48 (1987), 273–308.

[164] A. M. Odlyzko, An improved bound for the de Bruijn-Newman constant, *Numerical Algorithms* 25 (2000), 293–303.

[165] A. M. Odlyzko, *The* 10^{22}*-nd zero of the Riemann zeta function*, in *Dynamical, Spectral, and Arithmetic Zeta Functions*, M. van Frankenhuysen and M. L. Lapidus, eds., Amer. Math. Soc., Contemporary Math. series, no. 290, 2001, 139–144.

[166] A. M. Odlyzko and H. J. J. te Riele, Disproof of the Mertens conjecture, *J. Reine Angew. Mathematik* 357, 1985, 138–160.

[167] Yu. P. Ofman, On the algorithmic complexity of discrete functions, *Dokl. Akad. Nauk SSSR* 145 (1962), 48–51. English translation: *Sov. Phys. Dokl.* 7 (1968), 589–591.

[168] F. W. J. Olver, Error bounds for polynomial evaluation and complex arithmetic, *IMA J. Numer. Anal.* 6 (1986), 373–379.

[169] M. J. D. Powell, An efficient method for finding the minimum of a function of several variables without calculating derivatives, *Computer J.* 7 (1964), 155–162.

[170] F. P. Preparata, D. E. Muller and A. B. Barak, Reduction of depth of Boolean networks with a fan-in constraint, *IEEE Transactions on Computers* C-26, 1977, 474.

[171] I. S. Reed and G. Solomon, Polynomial codes over certain finite fields, *J. SIAM* 8, 1960, 300–304.

[172] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.

[173] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* 21, 1978, 120–126.

[174] E. Salamin, Computation of π using arithmetic-geometric mean, *Math. of Comp.* 30, 1976, 565–570.

[175] J. E. Savage, *The Complexity of Computing*, Wiley, New York, 1976, Chs. 2–3.

[176] P. Stevenhagen, On Aurifeuillian factorizations, *Nederl. Akad. Wetensch. Indag. Math.* 49, 1987, 451–468.

[177] M. Stewart and P. Van Dooren, Stability issues in the factorization of structured matrices, *SIAM J. Matrix Analysis and Applications* 18 (1997), 104–118.

[178] V. Strassen, Gaussian elimination is not optimal, *Numerische Mathematik* 13 (1969), 354–356.

[179] D. W. Sweeney, On the computation of Euler's constant, *Math. Comp.* 17, 1963, 170–178.

[180] D. R. Sweet, Fast Toeplitz orthogonalization, *Numerische Mathematik* 43 (1984), 1–21.

[181] J. F. Traub and H. Wozniakowski, *A General Theory of Optimal Algorithms*, Academic Press, New York, 1980.

[182] A. Tyagi, A reduced-area scheme for carry-select adders, *IEEE Trans. on Computers* 42 (1993), 1163–1170.

[183] J. D. Ullman, *Computational Aspects of VLSI*, Computer Science Press, Maryland, 1984.

[184] L. G. Valiant, S. Skyum, S. Berkowitz and C. Rackoff, Fast parallel computation of polynomials using few processors, *SIAM J. Computing* 12, 1983, 641–644.

[185] B. Vallée, Dynamics of the binary Euclidean algorithm: functional analysis and operators, *Algorithmica* 22 (1998), 660–685.

[186] M. Ward, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.* 35 (1933), 600–628.

[187] N. Weste and K. Eshraghian, *Principles of CMOS VLSI Design*, Addison Wesley, Reading, Mass., 1985, Sec. 8.2.6.

[188] S. Winograd, On the time required to perform addition, *J. ACM* 12 (1965), 277–285.

[189] S. Winograd, On the time required to perform multiplication, *J. ACM* 14, 1967, 793–802.

[190] S. Winograd, A new algorithm for inner product, *IEEE Transactions on Computers* C-17 (1968), 693–694.

[191] S. Winograd, On the parallel evaluation of certain arithmetic expressions, *J. ACM* 22, 1975, 477–492.

[192] As at September 2016, there are $14,519$ citations to Brent's publications on Google Scholar.

[193] In fact, the paper [1] was written by Brent's coauthor Mark Legg, and does not accurately describe the software designed and implemented by Brent.

[194] This was not pointed out in [2] since Level 3 BLAS had not been invented at the time.

[195] When stapling his handwritten solution together, Brent accidentally stapled his thumb, resulting in a blood-stain on the first page. The professor (Bob Floyd) commented "you must have sweated blood on this one".

[196] Valiant's processor bound was improved by Miller *et al* [156].

[197] The paper [9] did not allow division, and required $O(n^2)$ processors.

[198] Closely related to Von Neumann's *cellular automata*. See Kung [147] for an introduction to systolic architectures.

[199] The results for systolic arrays are also applicable to more general models of parallel computation.

[200] NC is the class of problems which can be solved in poly-log time using a polynomial number of processors. The basic arithmetic operations are in NC. See Cook [131] for an introduction.

[201] See [42, 47, 53] for GCDs, and [45, 48, 50] for the symmetric eigenvalue problem, the SVD and various generalisations.

[202] For example, reduction to tridiagonal or Hessenberg form followed by the QR algorithm, or the "divide and conquer" algorithm of Dongarra and Sorensen [136].

[203] R. P. Brent and R. B. Stanton (editors), *ANU/Fujitsu CAP Research Program Report 1996*, Department of Computer Science and Computer Sciences Laboratory, Australian National University, October 1996.

[204] For historical reasons this project was known as the "Area 4" project. For software developed during the project, see [78, 87].

[205] See, for example, Brent [3], Ofman [167], Savage [175], and Winograd [189].

[206] A similar result was obtained independently by Abelson and Andreae [117].

[207] As opposed to *discrete*. See, for example, Traub and Wozniakowski [181].

[208] The order is bounded by $d+1$ for iteration schemes *without memory*, e.g. Newton's method.

[209] In 2013, Fredrik Johansson [143] showed how to obtain a small constant factor improvement over the Brent-Kung algorithm for univariate reversion by avoiding the reduction to composition and Newton's iteration.

[210] The probabilistic assumptions of Brent's paper [23] were justified by Brigitte Vallée [185] (see also Knuth [145]). The existence and uniqueness of a limiting distribution (conjectured in [23]) was proved by Gérard Maze [153]. Further progress has been made recently by Ian Morris [159].

[211] Since the widespread acceptance of the IEEE floating-point standard it has become the conventional wisdom that base two is preferable to higher bases for floating-point arithmetic. However, in 1972 the subject was controversial enough to delay the publication of [11].

[212] Faster than an earlier algorithm of Brent [25], which in turn was faster than algorithms of Sweeney [179] and Knuth [144]. For an historical perspective, see [74].

[213] A gap in the error analysis of the most efficient version of the Brent-McMillan algorithm was filled by Brent and Johansson [109].

[214] The term *unrestricted* was used in this sense by Clenshaw and Olver [130].

[215] For example: Bailey [119], also in *GMP*, *Magma*, *MPFR* and (probably) in commercial packages such as *Mathematica*. (We say "probably" because the public documentation is incomplete.)

[216] For the GNU MPFR Library, see `http://www.mpfr.org/`.

[217] GIMPS stands for "Great Internet Mersenne Prime Search", see `http://www.mersenne.org/`.

[218] Nicely [162] extended Brent's computation of Brun's constant. He describes the computation which uncovered the notorious bug in the Intel Pentium floating-point divide operation. This was noticed when results of computations on the Pentium disagreed with the results computed on earlier 32-bit Intel processors (used by Nicely) and on a 36-bit Univac 1108 computer (used by Brent).

[219] The factorisation of F_9 was completed in 1990 by a world-wide collaboration (in which Brent was a participant) using the *Number Field Sieve* algorithm: see Lenstra *et al* [150].

[220] A positive integer is *perfect* if it is equal to the sum of its divisors (other than itself), e.g. $28 = 1 + 2 + 4 + 7 + 14$.

[221] For example, the $q^{5k/2}$ Theorem of [64].

[222] Specifically, the *elliptic curve method* (ECM) and the *multiple polynomial quadratic sieve* (MPQS).

[223] The algorithms can be generalised to other classes of low displacement-rank matrices, e.g. Hankel, block Toeplitz, etc.

[224] For historical references, see Bunch [128].

[225] R is upper triangular. For simplicity we assume that the matrix A is square.

[226] The algorithm computes the Cholesky factor R of A^TA stably, but the computed Q is not necessarily close to orthogonal, so it is best to solve for x using $R^TRx = A^Tb$, followed if necessary by iterative refinement.

[227] For generalisations of this result, see [129, 177].

[228] For rectangular matrices $A \in \mathbb{R}^{m\times n}$, $m \ge n > 0$, Hadamard's problem can be generalised by considering the determinant of the Gram matrix A^TA.

[229] A complete list of Brent's publications, many of which are available online, is at `http://maths-people.anu.edu.au/~brent/pub/pubsall.html`.