Richard Peirce BRENT

Research interests

Analysis of algorithms, combinatorics, computational complexity, number theory, numerical analysis, parallel computing, randomised algorithms, random number generators.

Education and degrees

1968 BSc Monash Honours 1 in Mathematics
1970 MSc Stanford in Computer Science
1971 PhD Stanford in Computer Science
1981 DSc Monash in Computer Science
1998 MA Oxon (by special resolution)

Awards and distinctions

1963 BHP Prize, Victoria
1982 Fellow, Australian Academy of Science
1984 Australian Mathematical Society Medal
1990 Forsythe Memorial Lecturer, Stanford University
1991 Fellow, Institute of Electrical and Electronics Engineers, USA (Life Fellow, 2011)
1993 Fellow, Institution of Engineers, Australia (resigned 1998)
1994 Fellow, Association for Computing Machinery, USA (resigned 2013)
1997 Fellow, Australian Mathematical Society
2000 IEEE Millennium Medal
2002 Fellow, British Computer Society (resigned 2008)
2003 Fellow, Institute for Mathematics and its Applications, UK
2005 Hannan Medal of the Australian Academy of Science
2009 Fellow, Society for Industrial and Applied Mathematics, USA
2009 Foreign Fellow, Bangladesh Academy of Science
2014 Moyal Lecturer and Medallist, Macquarie University
2015 Golub Memorial Lecturer, Hong Kong Baptist University

Employment

1968 Teaching Fellow, Computer Centre, Monash University
1971 Research Employee, IBM Research Center, Yorktown Heights, USA
1972 Research Fellow, Computer Centre, ANU
1973 Fellow, Computer Centre, ANU
1976 Senior Fellow, Computer Centre/Computing Research Group, ANU
1978 Foundation Professor and Head of Computer Science, Faculty of Science, ANU
1983 Professor, Centre for Mathematical Analysis, ANU
1985 Professor and Head, Computer Sciences Laboratory, RSPhysS/RSPhysSE/RSISE, ANU
1998 Statutory Professor of Computing Science and Fellow of St Hugh's College, Oxford, UK
2005 ARC Federation Fellow, MSI & RSISE, Australian National University
2010 Distinguished Professor, MSI & CECS, Australian National University
2011 Emeritus Professor, Australian National University

Visiting positions

1975 Visiting Assistant Professor, Computer Science, Stanford University (3 months)
1978 Visiting Professor, EECS, University of California, Berkeley (3 months)
1989 Visiting Professor, Computer Science, Carnegie-Mellon University (2 months)
1997 Visiting Professor, Mathematics, Harvard University (2 months)
2005–2011 Visiting Professor, University of Oxford, UK (short visits)
2014–2017 Vice-Chancellor's Visiting Fellow, University of Newcastle, NSW
2011–2020 Conjoint Professor, Mathematics, University of Newcastle, NSW

Teaching

Taught many undergraduate and graduate courses in both Computer Science (Stanford, Oxford, ANU) and Mathematics (Harvard, ANU, Newcastle), 1975–2013; for example:

- *Advanced Algorithms* (comp4600, 2010 and 2011) with B. McKay *et al*, ANU;
- *Number Theory and Cryptography* (math3301, 2010) with S. Montarani, ANU;
- *Parallel Systems* (comp4300/6430, 2011) with A. Rendell, ANU;
- *Differential Equations* (math2800, 2013) with B. Lamichhane, Newcastle.

Professional activities

- Editor/associate editor of journals: *Journal of the ACM* (1976–79), *Numerische Mathematik* (1981–87), *Advances in Computer Science* (Prentice-Hall Book Series, 1987–95), *SIAM J. on Matrix Analysis and Applications* (1987–89), *Parallel Processing Letters* (1990–93), *Internat. J. of High Speed Computing* (1990–2005), *Asian J. of Mathematics* (1997–2006), *Mathematics of Computation* (1998–2007), *Internat. J. High Performance Computing and Networks* (2004–), *Contributions to Discrete Mathematics* (2005–).
- Reviewer for numerous journals and granting bodies.
- Program/organising committee member for numerous national and international conferences, e.g. ACCMCC 2010, CATS 2008, PDCAT 2004–07, ICCSA 2004–05, ANTS 2004, FOCM 1999–2002, PDCS 2001, ISAAC 2001, ARITH15 2001.
- Member, IFIP Working Group 2.5 on Numerical Software, 1978–86.
- Member, National Committee for Mathematics, 1979–81, 1983–86, 1995–98.
- Foundation member and Secretary, Association of Australian Professors of Computer Science (now "CORE"), 1981–1985.
- Member, Council of the Australian Mathematical Society, 1983–1986.
- Member, ARC Engineering I Panel, 1994–96.
- Chair, Australian Academy of Science Sectional Committee 1, 2012–2014.
- Supervised 20 PhD students (plus 1 current) and numerous MSc and Honours students.
- Consultant and software architect for Quintessence Labs (2nd-generation quantum cryptography).

Research grants (since 2005)

- ARC Federation Fellowship *Exploring the Frontiers of Feasible Computation*, 2005–2010.
- CI in ARC Centre of Excellence *Mathematics and Statistics of Complex Systems* (MASCOS) with A. Guttmann (Melbourne) *et al*, 2005–2010.
- Australian leader in INRIA Associate Team program *Algorithms, Numbers, Computation* with P. Zimmermann (INRIA, France), 2008–2010.
- CI in ARC Discovery grant *Integral Lattices and their Theta Series* with J. Cannon (Sydney), 2008–2010.
- CI in ARC Discovery grant *An Integrative and Interactive Approach for Co-estimation of Multiple Sequence Alignment and Phylogeny Reconstruction* with B. Zhou (Sydney), 2009–2011.
- CI in ARC Linkage grant *Robust Numerical Solution of Partial Differential Equations on Petascale Computer Systems with Applications to Tsunami Modelling and Plasma Physics* with M. Hegland, A. Rendell, S. Roberts, P. Strazdins (ANU), R. Nobes (Fujitsu Laboratories Europe), 2011–2014.
- CI in ARC Discovery grant *Exploratory Experimentation and Computation in the Mathematical Sciences* with J. Borwein (Newcastle) and D. Bailey (USA), 2014–2017.

Research contributions

Brent's work is well-known and widely quoted in several areas of Computer Science and Mathematics, including algorithms for structured linear systems, analysis of algorithms, area-time bounds, computational complexity, computational number theory, high-precision computations, optimisation, parallel algorithms, random number generation, and solution of nonlinear algebraic systems.

Selected publications

Brent is the author of two books and over 270 papers. His publications have more than 16,400 citations with H-index 51 on Google Scholar (as at 6 May 2018). Only selected publications are listed here. A full list is available online.

1. R. P. Brent, *Algorithms for matrix multiplication*, Report TR-CS-70-157, DCS, Stanford (March 1970), 52 *pp.* [93 citations]

2. R. P. Brent, On the addition of binary numbers, *IEEE Transactions on Computers* C-19 (1970), 758–759. [58 citations]

3. R. P. Brent, Error analysis of algorithms for matrix multiplication and triangular decomposition using Winograd's identity, *Numerische Mathematik* 16 (1970), 145–156. [41 citations]

4. R. P. Brent, An algorithm with guaranteed convergence for finding a zero of a function, *Computer J.* 14 (1971), 422–425. [317 citations]

5. R. P. Brent, *Algorithms for Minimization without Derivatives*, Prentice-Hall, Englewood Cliffs, New Jersey, 1973, 195 *pp.* Reprinted by Dover Publications, Mineola, New York, 2002. [3892 citations]

6. R. P. Brent, Reducing the retrieval time of scatter storage techniques, *Communications of the ACM* 16 (1973), 105–109. [116 citations]

7. R. P. Brent, Some efficient algorithms for solving systems of nonlinear equations, *SIAM J. Numerical Analysis* 10 (1973), 327–344 (George E. Forsythe memorial issue). [214 citations]

8. R. P. Brent, The parallel evaluation of general arithmetic expressions, *J. ACM* **21** (1974), 201–206. [948 citations]

9. R. P. Brent, Algorithm 488: A Gaussian pseudo-random number generator, *Communications of the ACM* 17 (1974), 704–706. [125 citations]

10. R. P. Brent, Irregularities in the distribution of primes and twin primes, *Mathematics of Computation* **29** (1975), 43–56 (Derrick H. Lehmer special issue). [84 citations]

11. 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. [170 citations]

12. R. P. Brent, Fast multiple-precision evaluation of elementary functions, *J. ACM* **23** (1976), 242–251. [454 citations]

13. A. H. Sameh and R. P. Brent, Solving triangular systems on a parallel computer, *SIAM J. Numerical Analysis* 14 (1977), 1101–1113. [124 citations]

14. R. P. Brent, A Fortran multiple-precision arithmetic package, *ACM Transactions on Mathematical Software* 4 (1978), 57–70. [306 citations]

15. R. P. Brent and H. T. Kung, Fast algorithms for manipulating formal power series, *J. ACM* **25** (1978), 581–595. [301 citations]

16. R. P. Brent, On the zeros of the Riemann zeta function in the critical strip, *Mathematics of Computation* **33** (1979), 1361–1372. [98 citations]

17. R. P. Brent, An improved Monte Carlo factorization algorithm, *BIT* 20 (1980), 176–184. [279 citations]

18. R. P. Brent and H. T. Kung, The chip complexity of binary arithmetic, *Proc. Twelfth Annual ACM Symposium on the Theory of Computing*, ACM, New York, 1980, 190–200. [152 citations]

19. R. P. Brent and H. T. Kung, On the area of binary tree layouts, *Information Processing Letters* 11 (1980), 46–48. [110 citations]

20. 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. [504 citations]

21. R. P. Brent and H. T. Kung, The area-time complexity of binary multiplication, *J. ACM* 28 (1981), 521–534. [241 citations]

22. R. P. Brent and J. M. Pollard, Factorization of the eighth Fermat number, *Mathematics of Computation* **36** (1981), 627–630. [154 citations]

23. R. P. Brent and H. T. Kung, A regular layout for parallel adders, *IEEE Transactions on Computers* **C-31** (1982), 260–264. [1294 citations]

24. 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. [94 citations]

25. A. W. Bojanczyk, R. P. Brent and H. T. Kung, Numerically stable solution of dense systems of linear equations using mesh-connected processors, *SIAM J. Scientific and Statistical Computing* 5 (1984), 95–104. [151 citations]

26. R. P. Brent and H. T. Kung, Systolic VLSI arrays for polynomial GCD computation, *IEEE Transactions on Computers* C-33 (1984), 731–736. [154 citations]

27. 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 (1985), 242–270. [311 citations]

28. 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. [412 citations]

29. A. W. Bojanczyk, R. P. Brent and F. R. de Hoog, QR factorization of Toeplitz matrices, *Numerische Mathematik* 49 (1986), 81–94. [106 citations]

30. R. P. Brent, Some integer factorization algorithms using elliptic curves, *Proceedings of the Ninth Australian Computer Science Conference*, special issue of *Australian Computer Science Communications* 8 (1986), 149–163. Also arXiv:1004.3366v1 [139 citations]

31. A. W. Bojanczyk, R. P. Brent, P. Van Dooren and F. R. de Hoog, A note on downdating the Cholesky factorization, *SIAM J. Sci. Statist. Computing* 8 (1987), 210–221. [117 citations]

32. R. P. Brent and B. D. McKay, On determinants of random symmetric matrices over $\mathbf{Z}_m$, *Ars Combinatoria* **26A** (1988), 57–64.

33. 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. [118 citations]

34. R. P. Brent, Fast training algorithms for multi-layer neural nets, *IEEE Transactions on Neural Networks* 2, 3 (May 1991), 346–354. [213 citations]

35. R. P. Brent, On computing factors of cyclotomic polynomials, *Mathematics of Computation* **61** (1993), 131–149 (Derrick H. Lehmer memorial issue). [42 citations]

36. R. P. Brent, On the periods of generalized Fibonacci recurrences, *Mathematics of Computation* **63** (1994), 389–401. [88 citations]

37. On the stability of the Bareiss and related Toeplitz factorization algorithms, *SIAM J. Matrix Analysis and Applications* 16 (1995), 40–57. [84 citations]

38. R. P. Brent, Factorization of the tenth Fermat number, *Mathematics of Computation* **68** (1999), 429–451. [57 citations]

39. R. P. Brent, Recent progress and prospects for integer factorisation algorithms (keynote address), *Computing and Combinatorics*, *Lecture Notes in Computer Science*, Vol. 1858, Springer-Verlag, Berlin, 2000, 3–22. [109 citations]

40. 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, Oxford University Computing Laboratory, 31 December 2000, vii+502 *pp.*

41. R. P. Brent, Shuhong Gao and Alan G. B. Lauder, Random Krylov spaces over finite fields, *SIAM J. on Discrete Mathematics* **16** (2003), 276–287.

42. R. P. Brent and P. Zimmermann, A multi-level blocking distinct-degree factorization algorithm, *Contemporary Mathematics* **461** (2008), 47–58.

43. R. P. Brent and P. Zimmermann, Ten new primitive binary trinomials, *Mathematics of Computation* **78** (2009), 1197–1199.

44. R. P. Brent and P. Zimmermann, *Modern Computer Arithmetic*, Cambridge University Press, Nov. 2010, 236 *pp.* [226 citations]

45. R. P. Brent and P. Zimmermann, An $O(M(n) \log n)$ algorithm for the Jacobi symbol, *Lecture Notes in Computer Science* 6197, Springer-Verlag, 2010, 83–95.

46. R. P. Brent and P. Zimmermann, The great trinomial hunt, *Notices of the American Mathematical Society* **58**, 2 (2011), 233–239.

47. 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.

48. R. P. Brent and J. van de Lune, A note on Pólya's observation concerning Liouville's function, *Herman J. J. te Riele Liber Amicorum*, CWI, Amsterdam, Dec. 2011, 92–97.

49. 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* 7203 (2012), 609–618.

50. R. P. Brent and D. Harvey, Fast computation of Bernoulli, tangent and secant numbers, *Springer Proceedings in Mathematics and Statistics*, Vol. 50, 2013, Ch. 8, 127–142.

51. R. P. Brent, Finding D-optimal designs by randomised decomposition and switching, *Australasian Journal of Combinatorics*, 55 (2013), 15–30.

52. 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)*, Springer Proceedings in Mathematics and Statistics Vol. 43, Springer, New York, 2013, 75–97.

53. 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.

54. R. P. Brent and J. H. Osborn, Bounds on minors of binary matrices, *Bull. Austral. Math. Soc.* 88 (2013), 280–285.

55. R. P. Brent and J. H. Osborn, On minors of maximal-determinant matrices, *Journal of Integer Sequences* 16 (2013), Article 13.4.2, 30 pp.

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

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

58. 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.

59. R. P. Brent, Generalising Tuenter's binomial sums, *Journal of Integer Sequences* 18 (2015), article 15.3.2, 9 pp.

60. R. P. Brent, H. Ohtsuka, J. H. Osborn, and H. Prodinger, Some binomial sums involving absolute values, *Journal of Integer Sequences* 19 (2016), article 16.3.7, 14 pp.

61. 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.

62. R. P. Brent, J. H. Osborn and W. D. Smith, Probabilistic lower bounds on maximal determinants of binary matrices, *Australasian Journal of Combinatorics* 66 (2016), 350–364.

63. R. P. Brent, C. Krattenthaler and [S.] O. Warnaar, Discrete analogues of Mehta-type integrals, *J. Combin. Theory Ser. A* 144 (2016), 88–138.

64. R. P. Brent, A. Kruppa and P. Zimmermann, FFT extension for algebraic-group factorization algorithms, chapter in *Topics in Computational Number Theory inspired by Peter L. Montgomery*, J. Bos and A. Lenstra (editors), Cambridge University Press, 189–205, 2017.

65. David H. Bailey, Jonathan M. Borwein, Richard Brent, and Mohsen Reisi Ardali, Reproducibility in computational science: a case study: randomness of the digits of π, *Experimental Mathematics* 26 (2017), 298–305.

66. R. P. Brent, The Borwein brothers, π and the AGM, *Proceedings of the Jonathan Borwein Commemorative Converence*, to appear. Also arXiv:1802.07558, 8 Aug. 2018, 24 pp.

67. R. P. Brent and A. B. Yedidia, Computation of maximal determinants of binary circulant matrices, *Journal of Integer Sequences* **21** (2018), article 18.5.6. Also arXiv:1801.00399v4, 6 June 2018, 22 pp.

Publications accepted/submitted

1. R. P. Brent, On asymptotic approximations to the log-Gamma and Riemann-Siegel theta functions, submitted to *J. AustMS (Borwein memorial issue)*. Also arXiv:1609.03682, 6 Oct. 2016, 23 pp.