Errata and Addenda to Published Papers

Eric Bach
University of Wisconsin
2/20/2023

How to Generate Factored Random Numbers

The displayed equation on p. 182 should have $\left(1-\frac{Q}{P}\right)^{t-1}$.

Last displayed equation on p. 188 should have $\sum_{2\le\alpha\le d}$.

Intractable Problems in Number Theory (Proc. CRYPTO 88)

On p. 90 it is claimed that $\rho \le \lambda^{-\lambda}$ for $5 \le \lambda \le 10$; this is false.

Efficient Prediction of Marsaglia-Zaman Random Number Generators (IEEE-IT 1998)

Page 1254, line 18 should read $2^3 + 2^1 - 1 = 9$.

Regarding Theorem 3, work by Wang and Collins/Encarnacion should be mentioned.

Sieve Algorithms for Perfect Power Testing

An almost-linear time algorithm for power testing has been found by Dan Bernstein (Math. Comp. v. 67, 1998).

For an improved version of Lemma 4.3, see Balasubramanian and Nagaraj, Inform. Proc. Lett. v. 58, 1996.

Section 5: Change "large sieve" to "sieve." (If you remove one congruence class per prime, it's a small sieve.)

Realistic Analysis of Some Randomized Algorithms

The error estimate for the Miller-Rabin test has been sharpened by R. Peralta and V. Shoup, Computational Complexity v. 3, 1993. This also gives results for Solovay-Strassen.

Sums of Divisors, Perfect Numbers and Factoring (SICOMP 1986)

Adleman and Huang showed that PRIMES belongs to ZPP, and Agrawal, Kayal and Saxena showed that PRIMES is in P. This makes the BPP examples of less interest now.

Number-Theoretic Algorithms (Ann. Rev. Comp. Sci. v. 4)

Page 144, line 4, change to $O(n + \deg f + \log p)\log^2 f)$.

The comments on factoring are now out of date, due to progress with the general number field sieve.

Fast Algorithms Under the ERH: A Concrete Estimate

The main result of this paper was superseded by my thesis. What remains of possible interest are the explicit bounds for $\psi^1(x,\chi)$.

Factoring with Cyclotomic Polynomials

In the algorithm on p. 204, $D$ should get the value $\gcd_{0\le j<k}\{c_j - y_j\}$. In the paragraph following, use $t$ instead of $x$.

Last paragraph on p. 215, interchange "residue" and "nonresidue."

Text for example 3 should say 3 is a generator for $\mathbf{Z}_7^*$.

Algorithmic Number Theory (MIT Press 1996)

See the web site

`http://www.cs.uwaterloo.ca/~shallit/anterrata.html`

Moments in the Duration of Play

The variance for the duration of play was computed earlier by I.J. Good, Random Motion on a Finite Abelian Group, Proc. Cambridge Phil. Soc., v. 47, 1951, p. 761.

Comments on Search Procedures for Primitive Roots

Some additional data for Table 1:

| $p$ | $\hat{g}$ | ratio |
|---|---|---|
| 31552100581 | 367 | .840069 |
| 81651092041 | 383 | .823451 |
| 96736641541 | 461 | .980414 |
| 1867622877121 | 479 | .852547 |

The first 3 were found by Scott Lindhurst. Tomás Olivera e Silva has a web page

`http://www.ieeta.pt/~tos/p-roots.html`

containing the last, plus many other tables on small primitive roots.

It should be emphasized that the reduction from primitive root construction to discrete logarithms is only valid under ERH.

The Complexity of Number-Theoretic Constants

The interval two lines down from equation (9) should be (-1, 1).

Weil Bounds for Singular Curves

For complete intersections, Theorems 3.1–3.3 were given by Aubry and Perret ["A Weil Theorem for Singular Curves," in Arithmetic, Geometry, and Coding Theory

IV, N. de Gruyter, Berlin-New York 1995. See also Aubry's thesis, Variétés sur un Corps Fini et Codes Géometriques Algébriques, Univ. Aix-Marseille II, 1993.]

P. 293, first displayed equation should read $p_a(C) \le p_a(D)$.

Energy Arguments in the Theory of Algorithms

The spring analogy for the KMP algorithm is misleading, as Hooke's law has a quadratic potential. For a better model, write the machine vertically, so that state $i$ is at height $i$ from the ground.

Discrete Logarithms and Factoring

Equation (*) needs the hypothesis that $a, b$ are prime to $p$. The line after this should read $p^e \mid a^{p^{e-1}} - 1$.

The middle displayed equation on p. 5 should have $2^{e-2}$, not $p^{e-2}$.

DNA Models and Algorithms for NP-complete Problems

Page 175, first displayed equation, $\binom{n}{3}$ should be $\binom{n}{n/3}$.

Threshold Data Structures and Coding Theory

The method for solving $y^2 + y = \gamma$ in section 3 is incorrect, as it may direct one to invert a matrix that is not full rank. It should be modified as follows. Let

$$\begin{pmatrix} U & 0 \\ & \\ v & 0 \end{pmatrix} \begin{pmatrix} y_{m-1} \\ \vdots \\ y_0 \end{pmatrix} = \begin{pmatrix} \gamma'_{m-1} \\ \vdots \\ \gamma'_0 \end{pmatrix},$$

where $U$ is an invertible $(m-1) \times (m-1)$ matrix, and $\gamma'_0, \ldots, \gamma'_{m-1}$ are the $\gamma_i$'s in some order. (The linear operator taking $y$ to $y^2 + y$ has nullity 1, hence rank $m-1$. Therefore we will always be able to do this.) Let

$$\begin{pmatrix} y_{m-1} \\ \vdots \\ y_1 \end{pmatrix} = U^{-1} \begin{pmatrix} \gamma'_{m-1} \\ \vdots \\ \gamma'_1 \end{pmatrix}.$$

The equation is solvable iff

$$v \begin{pmatrix} y_{m-1} \\ \vdots \\ y_1 \end{pmatrix} = \gamma'_0,$$

and if so taking $y_0 = 0, 1$ gives two values for $y$.

On Testing for Zero Polynomials by a Set of Points with Bounded Precision

A formula equivalent to Theorem 5 (with the local factor expressed differently) appears in Manfred Schroeder, Number Theory in Science and Communication,

1986. He gave a heuristic argument for this but did not prove it. The case $n = 3$ was proved by Pieter Moree: Counting Carefree Couples, unpublished manuscript, 2000. (See `http://web.inter.nl.net/hcc/J.Moree`.)

Timing the Blind Watchmaker

It is falsely stated on p. 299 that a random walk on the hypercube converges to the invariant (uniform) distribution. This is not possible since the chain is periodic.

Text before (3) should read "summing over $k = 0, \ldots, n-1$."

Asymptotic Semi-smoothness Probabilities

In the proof of (2.7), use (5.4) (not (1.4)) and (5.3) of [3].

Theorem 3.1 should assume $x^\alpha \geq 2$.

In the third displayed equation (p. 1705), the $O$-estimate should have $\log x$, not $\log^2 x$.

Fifth displayed equation, p. 1705, is missing the factor $x$ in front of the integral.

Results and Estimates on Pseudopowers

Some of the conjectures in this paper were proved (conditionally, assuming GRH and more) by O. M. Fomenko, J. Math. Sci. (N.Y.) 122, 2004, no. 6, 3685-3698. See MathSciNet MR19377377 for citation of original Russian language article.

Computing Prime Harmonic Sums

On p. 17, "primes $\leq x^{1/2}$" should read "primes up to the square root of the upper bound in (8.1)."

Sums over Primes

Errors by the printer rendered several footnotes uninformative.

Sum in first displayed equation on p. 13 should be over $n \geq 1$, $n$ odd.

Section 5, characterization of $q$-special nodes with $x/m \in B_k$: ii) should read "smallest prime factor of $m'$ is $> q$.

In code following this, $q \leq p_a$.

Section 5, pgh beginning "The other ideas...": names of special and ordinary nodes were reversed.

Improved Asymptotic Formulas for Counting Correlation Immune Boolean Functions

First author of [9] is L. Hellerstein.

Statistical Evidence for Small Generating Sets

Table 1 has some errors. Here is what it should have been:

| $n$ | $G(n)$ | $a(n)$ | $a'(n)$ |
|---|---|---|---|
| 3 | 2 | 13.417211 | 1.000000 |
| 4 | 3 | 4.592292 | 1.000000 |
| 6 | 5 | 3.316650 | 1.666667 |
| 12 | 7 | 2.145161 | 1.400000 |
| 20 | 11 | 2.319711 | 1.571429 |
| 24 | 13 | 2.452159 | 1.857143 |
| 70 | 19 | 2.142920 | 1.461538 |
| 714 | 31 | 1.736978 | 1.347826 |
| 1364 | 37 | 1.797547 | 1.275862 |
| 2706 | 43 | 1.824282 | 1.387097 |
| 26220 | 47 | 1.380249 | 1.093023 |
| 53570 | 53 | 1.412988 | 1.127660 |
| 67044 | 59 | 1.528140 | 1.113208 |
| 164220 | 71 | 1.648685 | 1.203390 |
| 5053620 | 97 | 1.591658 | 1.227848 |
| 60369855 | 101 | 1.354115 | 1.041237 |
| 191895456 | 103 | 1.269674 | 1.000000 |
| 475528443 | 107 | 1.239532 | 1.000000 |
| 715236599 | 109 | 1.229120 | 1.000000 |

Thanks to Steven Finch for pointing this out.

Exploiting Product Distributions to Identify Relevant Variables of Correlation Immune Functions

To get Lemma 5 from Theorem 3 of Pinelis (1992), assume $||Z(i)-Z(i-1)|| \leq c_i$, and let $D = \sum c_i^2$. Then take $p = 2$, $f_n = (Z(n) - Z(0))/\sqrt{D}$, and $r = \lambda/\sqrt{D}$. Thomas Hayes (manuscript, 2005) also proves this, with the slightly larger factor $2e^2$.

The Hardness of Computing an Eigenform

Middle line of the displayed equation on p. 14 should begin with $q$, not 1.

Approximately Counting Semismooth Integers

The second author of [8] is C.-W. de Boor. The second editor of [17] is H. W. Lenstra, Jr.

Phase Transition of Multivariate Polynomial Systems

The caption for Figure 4 should have $z = 4/5$ (not 2/3). Thanks to James Davenport for informing me of this.

Iterative Root Approximation Methods in $p$-adic Numerical Analysis

Reference to Lang's Algebra on p. 515 should be to page 310, not 300. See also the same author's Algebraic Number Theory (1970), p. 42.