is very well written and is impressive in the breadth and depth of its coverage of the field. A major strength of the book is that it typically gives an excellent intuitive explanation of an algorithm or data structure before providing implementation details. The lower-bound proofs are given in the unified framework of Ben-Or's theorem; including this theorem was a particularly good decison by the authors. As a reference, the book is a must for the researcher in algorithm design and data structures, and for any programmer writing software that deals with geometric objects. As a textbook, the book is ideal for a graduate-level course taken by students who have already taken an algorithms course, or as a supplementary textbook for a senior or graduate-level course on algorithm design and analysis; in either case, the book's list of suggested exercises will be most valuable to the instructor.

MIKHAIL J. ATALLAH

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

49[11T06].—HAROLD FREDRICKSEN & ROBERT WARD, *A Table of Irreducible Binary Pentanomials of Degrees* 4 *Through* 100, 4 pp. of introductory text, 1 fig., and 273 pp. of tables, deposited in the UMT file.

An irreducible binary pentanomial of degree n takes the form $f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + 1$. The c_i are 0's and 1's with exactly three c_i nonzero. $f(x)$ is irreducible means there are no polynomials $g(x)$ and $h(x)$, both of degrees less than n over the field of 2 numbers, for which $f(x) = g(x)h(x)$.

In the tables, all irreducible pentanomials over the field of 2 elements are given for each degree from $n = 4$ through $n = 100$. Each polynomial which appears is listed as a, b, c, where these are the exponents of x for which the coefficients of f are nonzero. If $x^n + x^c + x^b + x^a + 1$ is irreducible with $a < b < c$, then its reverse polynomial $x^n + x^{n-a} + x^{n-b} + x^{n-c} + 1$ is also irreducible. We do not list both of these polynomials in the interest of economy. For each degree we also list the total number of irreducible pentanomials of that degree. Here, of course, we count both a polynomial and its reverse polynomial.

There have not been extensive tables of irreducible binary pentanomials published. However, there have been a number of tables of irreducible binary trinomials published [1]–[2]. When one examines these tables of trinomials, it is clear that there are several degrees for which there are no irreducible trinomials of these degrees. In fact, for degree $8t$ there are no irreducible trinomials for any t and for degrees $8t \pm 3$ there are very few irreducible trinomials of those degrees. It has been conjectured that there is no degree above $n = 4$ which does not possess an irreducible pentanomial of that degree. Our table lends evidence to support that conjecture.

The number N_n, of pentanomials of degree n, is also plotted with our tables. At (n, N_n) we have plotted the value of n (mod 8). One of the main suggestions of our work is clear from this figure, that is, there is a distinct modulo 8 character to the number of irreducible pentanomials. This compares to the similar modulo 8 character of irreducible trinomials indicated in Swan [3] and Fredricksen et al. [4].

Curves drawn through the points with $n \equiv c \pmod 8$ and with $c \equiv 4$ and $\pm 1 \pmod 8$ are approximately the same curves and lie above the others. Next come the curves for $c \equiv \pm 2 \pmod 8$, then those for $c \equiv \pm 3 \pmod 8$ and finally that for $c \equiv 0 \pmod 8$. These curves reflect the distribution for the similar sums of irreducible trinomials of the same congruences. If $1/n$ of all pentanomials of degree n are irreducible then the curves should be roughly quadratic in growth rate, as there are $\binom{n-1}{3}$ pentanomials of degree n. The curves appear to fit parabolas quite well.

The factoring algorithm. The irreducible pentanomials were found by subjecting all pentanomials of degree n to the following algorithm. Only one of the pentanomials $P_{n,c,b,a}$ and $P_{n,n-a,n-b,n-c}$ need be tested as they are both either reducible or irreducible together. If $P_{n,a,b,c}$ passes a test it is subjected to the next test. Survivors of Test 5 are irreducible.

Test 1. Check that not all of n, a, b, c are even, for if all are even, $P_{n,c,b,a}$ is a square and hence reducible.

Test 2. $P_{n,c,b,a}$ is divisible by the polynomial $f(x)$ of the following table if any three of (n, a, b, c) are congruent to y and the other is congruent to z (modulo m) of the table.

m	$f(x)$	(y, z)
3	$x^2 + x + 1$	(2, 1)
7	$x^3 + x + 1$	(3, 1)(5, 4)(6, 2)
7	$x^3 + x^2 + 1$	(3, 2)(5, 1)(6, 4)
15	$x^4 + x + 1$	(4, 1)(8, 2)(9, 7)(10, 5)(12, 11)(13, 6)(14, 3)
15	$x^4 + x^3 + 1$	(4, 3)(8, 6)(9, 2)(10, 5)(12, 1)(13, 7)(14, 11)

Test 3. The GCD of $P_{n,a,b,c}$ and $x^{2^d} + x$ for $d = 5, 6, \ldots, 10$ is computed. A nontrivial GCD of $P_{n,a,b,c}$ and $x^{2^d} + x$ will identify $P_{n,a,b,c}$ as having an irreducible factor of degree d.

Test 4. Calculate $x^{2^n} \pmod{P_{n,a,b,c}}$. When $P_{n,a,b,c}$ is irreducible, it is necessary that $x^{2^n} \equiv x \pmod{P_{n,a,b,c}}$. Some pentanomials $P_{n,a,b,c}$ will pass this test but not be irreducible. The final test is required.

Test 5. The remaining pentanomials $P_{n,a,b,c}$ have $x^{2^n} \equiv x \pmod{P_{n,a,b,c}}$, so any irreducible factor $g(x)$ of $P_{n,a,b,c}$ will have degree m which divides n. If m is not equal to n, then $m = n/p$ for some prime p. The $g(x)$ divides $x^{2^{n/p}} + x$ and the GCD of $P_{n,a,b,c}$ and $x^{2^{n/p}} + x$ is not equal to 1. Thus, calculate the GCD of $P_{n,a,b,c}$ and $x^{2^{n/p}} + x$ for each prime factor p of n. If all these GCD's are 1, then $P_{n,a,b,c}$ is irreducible.

Conjectures. We gather together here the observations we have about the tables we present.

Conjecture 1. There is an irreducible binary pentanomial of each degree $d \geqslant 4$.

Conjecture 2. There is a distinct modulo 8 character to the number of irreducible binary pentanomials.

Conjecture 3. The congruence classes of degrees of irreducible binary pentanomials are ordered with classes $c \equiv \pm 1, 4$ being largest, then $c \equiv \pm 2$, followed by $c \equiv \pm 3$ and finally $c \equiv 0$ (modulo 8).

Conjecture 4. The congruence classes of degrees of irreducible binary pentanomials are quadratically generated so that approximately $1/n$ of all binary pentanomials are irreducible.

AUTHOR'S SUMMARY

Department of Mathematics
Naval Postgraduate School
Monterey, California 93943

Department of Defense
Fort George G. Mead, Maryland

1. N. ZIERLER & J. BRILLHART, "On primitive trinomials (mod 2)," *Inform. and Control*, v. 13, 1968, pp. 541–554.

2. N. ZIERLER & J. BRILLHART, "On primitive trinomials (mod 2). II," *Inform. and Control*, v. 14, 1969, pp. 566–569.

3. R. G. SWAN, "Factorization of polynomials over finite fields," *Pacific J. Math.*, v. 12, 1962, pp. 1099–1106.

4. H. M. FREDRICKSEN, A. W. HALES, & M. M. SWEET, "A generalization of Swan's theorem," *Math. Comp.*, v. 46, 1986, pp. 321–331.