Correction to "On normal and subnormal q-ary codes"

References

[1] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms*. Reading, MA: Addison-Wesley, 1974.
[2] E. Bach, "Realistic analysis of some randomized algorithms," in *Proc. Nineteenth Ann. ACM Symp. Theory of Comput.*, 1987, pp. 453–461. [Final version to appear, *J. Comput. Syst. Sci.*]
[3] P. Bachmann, *Niedere Zahlentheorie*, vol. 1. New York: Chelsea, 1968.
[4] E. R. Berlekamp, "Factoring polynomials over large finite fields," *Math. Comp.*, vol. 24, pp. 713–735, 1970.
[5] E. R. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Inform. Contr.*, vol. 10, pp. 553–564, 1967.
[6] G. Collins and R. Loos, "The Jacobi symbol algorithm," *SIGSAM Bull.*, vol. 16, pp. 12–16, 1982.
[7] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," in *Proc. Nineteenth Ann. ACM Symp. Theory of Computing*, 1987, pp. 1–6. [Final version to appear, *J. Symbol. Comp.*]
[8] F. E. Fich and M. Tompa, "The parallel complexity of exponentiating polynomials over finite fields," *J. ACM*, vol. 35, pp. 651–667, 1988.
[9] C. F. Gauss, "Neue Beweise und Erweiterungen des Fundamentalsatzes in der Lehre von den quadratischen Resten," in C. F. Gauss, *Untersuchen über Höhere Arithmetik*. New York: Chelsea, 1965, pp. 496–510.
[10] R. Hartshorne, *Algebraic Geometry*. Berlin: Springer-Verlag, 1977.
[11] T. Itoh and S. Tsujii, "An efficient algorithm for deciding quadratic residuosity in finite fields GF(p^m)," *Inform. Processing Lett.*, vol. 30, pp. 111–114, 1989.
[12] H. Kühne, "Eine Wechselbeziehung zwischen Functionen mehrer Unbestimmten, die zu Reciprocitätsgesetzen führt," *J. Reine Angew. Math.*, vol. 124, pp. 121–131, 1902.
[13] D. H. Lehmer, "Computer technology applied to the theory of numbers," in *Studies in Number Theory*, W. J. LeVeque, Ed. Washington, D.C.: MAA, 1969.
[14] R. Moenck, "Fast computation of GCD's," *Proc. Fifth Ann. ACM Symp. Theory of Computing*, 1973, pp. 142–151.
[15] R. Loos, "Generalized polynomial remainder sequences," in *Computer Algebra: Symbolic and Algebraic Computation*, 2nd ed., B. Buchberger, G. E. Collins, and R. Loos, Eds. Wien: Springer-Verlag, 1983, pp. 115–137.
[16] O. Ore, "Contributions to the theory of finite fields," *Trans. Amer. Math. Soc.*, vol. 36, pp. 243–274, 1934.
[17] R. Peralta, "A simple and fast probabilistic algorithm for computing square roots modulo a prime number," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 846–847, 1986.
[18] M. O. Rabin, "Probabilistic algorithms in finite fields," *SIAM J. Comput.*, vol. 9, pp. 273–280, 1980.
[19] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*. Berlin: Springer-Verlag, 1976.
[20] A. Schönhage, "Schnelle Berechnungen von Kettenbruchentwicklungen," *Acta Informatica*, vol. 1, pp. 139–144, 1971.
[21] D. Shanks, "Five number-theoretic algorithms," in *Proc. Second Manitoba Conf. Numerical Math.*, 1972, pp. 51–70.
[22] V. Shoup, "New algorithms for finding irreducible polynomials over finite fields," *Math. Comp.*, vol. 54, pp. 435–447, 1990.

Correction to "On Normal and Subnormal q-ary Codes"

ANTOINE C. LOBSTEIN AND GERHARD J. M. VAN WEE

In the above correspondence,[1] the following corrections are necessary.

When sets are defined, a vertical bar | is intended where a division bar / is used. The most important place where this might cause confusion is in the proof of Lemma 1. A rewritten version of part of that proof will follow.

The last two sentences of the Introduction should read: We include a table of lower and upper bounds on $K_3(n,R)$, the minimal number of codewords in any ternary code of length n and covering radius R, for $n \le 13$, $R \le 3$, known to us. We improved some of the known lower bounds by linear programming.

Section II, line 13: ..., and such a coordinate i is called *acceptable*.

Proof of Theorem 1, line 5: $\cdots + d((u,v), B_a^{(1)}) - \Delta_{a,u}\}$.

Theorem 2 should read: If C is a $(q,n,M)R$ subnormal code with an acceptable partition without the empty set, then for every natural number p there is a $(q,n+pq,M)R+(q-1)p$ code.

In the proof of Lemma 1, the first few lines should read:

Proof: The repetition code is $C_{\text{rep}} = \cup_{a \in F_q}\{J_a^n\}$, with J_a^n the all-a vector of length n. Let w be any vector in F_q^n, containing p_a times the symbol a. Let $p = \max\{p_a | a \in F_q\}$. Then $p \ge \lceil n/q \rceil$ and $d(w, C_{\text{rep}}) = n - p \le n - \lceil n/q \rceil$ and so C_{rep} has covering radius $R \le n - \lceil n/q \rceil$. Taking w with $p = \lceil n/q \rceil$ shows that $R = n - \lceil n/q \rceil$. Now, ...

Three lines before Theorem 3 should read: ... are nonempty for all $a \in F_q$.

The second sentence of the proof of Theorem 3 should read: For $t \in F_q$ let $\Delta_t = 0$ if $t = 0$, and $\Delta_t = 1$ otherwise.

Two lines before Lemma 3, the name should read: J. H. van Lint, Jr.

On page 1293, first column, line 4: $\cdots + \sum_{a \in F_q \setminus \{c_1\}} d(x, b^a)$.

The middle of line 2 of Theorem 5 should read: then $d \le (q/(q-1)) \cdot R + 1$.

The first sentence in the proof of Theorem 5 should end with: $d(c, \varnothing) = n \ge d$.

The second to last sentence of Section III should read: Theorem 5 and any choice of the parameters of the Hamming codes just mentioned can be used to disprove the q-ary generalization of this conjecture, even when we replace "normal" by "subnormal."

On page 1293, second column, line 2 should read: $|C| \ge 3^n/(1+2n)$.

Proof of Theorem 6, line 3: ...such that $d(c,c') \le 2$.

Page 1294, second column, line 8 the C should be uppercase.

In Section V, Open Problem 1) should read:

1) Find ternary, optimal or nonoptimal, normal or subnormal codes improving, by the amalgamated direct sum construction, on the upper bounds on $K_3(n,R)$ (cf. Section IV-A).

The following piece of text is missing at the end of the paper.

Notes Added in Proof

1) The result, mentioned in the Introduction, that binary linear codes with minimum distance $d_{\min} \le 5$ are normal, has not (yet) been established. X. Hou (Univ. of Chicago) has shown that the proof in [12] is incorrect.
2) For open problem No. 2, see: G. J. M. van Wee, "Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces," *J. Combin. Theory (A)*, to appear.

In [5], there are two authors, H. O. Hämäläinen and S. Rankinen. Reference [8] appeared in *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 1343–1344, Sept. 1988.

Manuscript received May 1990.

A. C. Lobstein is with the Centre National de la Recherche Scientifique, URA 251, Télécom Paris, Département Informatique, 46 rue Barrault, 75634 Paris Cedex 13, France.

G. J. M. van Wee is with the Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

IEEE Log Number 9037999.

[1] A. C. Lobstein and G. J. M. van Wee, *IEEE Trans. Inform. Theory*, vol. 35, no. 6, pp. 1291–1295, Nov. 1989.