Coding Theory

Introduction

J. H. VAN LINT
ASSOCIATE EDITOR

There are fourteen papers on algebraic and combinatorial coding theory in this special issue. Their subject matter mix attests that there are at least two hot topics currently, namely, covering radius problems (four papers) and algebraic geometric codes (three papers); moreover, several other papers on these two areas are in the pipeline. Of course, there are also a few papers on decoding algorithms.

If a binary code \( C \) has covering radius \( R \), then the spheres of radius \( R \) around codewords cover the space \( F^n_2 \). By expressing this fact in terms of the group algebra \( GF^n_2 \), Calderbank and Sloane find linear inequalities involving the Lloyd polynomials via the Delgarte–MacWilliams inequalities. This leads to two new values of \( \ell(n, k) \), the smallest covering radius of any \( [n, k] \) code, namely, \( \ell(17, 10) = 3 \) and \( \ell(23, 15) = 5 \). MacWilliams’ equation also plays a role in the paper by Simonis, who shows that \( \ell(15, 6) = 4 \) using a combination of this equation and arguments from finite geometry. Previous upper bounds on \( K(n, R) \), the minimal cardinality of a binary code of length \( n \) and covering radius \( R \), are improved by a new family of normal nonlinear codes given by Honkala and Hämmäläinen. Their idea is first to construct the code consisting of all words with weights in a set \( W \) satisfying carefully chosen conditions, then to double the length by the rules \( 0 \rightarrow 00 \) and \( 1 \rightarrow 11 \) or \( 0 \rightarrow 10 \) and \( 1 \rightarrow 01 \), and finally to delete a coordinate. The paper by Pach and Spencer is in a different vein. Probabilistic and asymptotic methods are used to find a series of linear codes with both low covering radius and a rapid decoding algorithm. For a survey of results on covering radius problems that appeared either as a paper or as a preprint in 1986–1988, see [2].

Recently several papers have appeared extending Goppa’s construction of codes using algebraic curves. For an introduction to the subject, see [3]. Quebeman considers what he calls a “cyclotomic extension” \( E \) of the rational function field \( \mathbb{F}_{q}(X) \). He shows that \( E \) has small genus compared to its number of \( \mathbb{F}_{q} \)-rational points. This leads to a sequence of codes with a transitive automorphism group. Although the codes are not “good” in the usual asymptotic sense, they are not bad either. Wirtz found a gap in the original proof of Goppa on the parameters of subfield subcodes of generalized Goppa codes. This is repaired by an ingenious induction argument. Stichtenoth considers codes defined using Hermitian curves. The results extend those of Tiersma [5]. As was the case for Tiersma’s paper, this one is useful for those readers who are still gaining familiarity with this area, since it is not too deep and it explicitly finds generator matrices and results on weight distribution.

There are two papers related to Berlekamp–Massey decoding of BCH codes. Stevens decodes beyond the BCH bound by using not only the known values of power sums but also a number of them that can take on only a few (unknown) values. The method seems useful for parallel computing. The paper also contains several important tables. Shiozaki’s correspondence is essentially about decoding Reed–Solomon codes. By a slight variation on the standard method, involving an error-locator and error-evaluator, the final step (which is again a gcd calculation) produces the information polynomial directly instead of the error evaluator. The amount of computation seems to be the same as in Berlekamp–Massey decoding.

The paper by Boly and van Gils was inspired by the \((N, K)\) concept fault-tolerant computers (cf. [1]). The codes involve as symbols elements of \( \mathbb{F}_{m} \) represented as \( m \)-tuples over \( \mathbb{F}_{p} \). The codes are used to handle single symbol errors, multiple bit errors, and combinations of symbol erasures and bit errors. Extensive tables are given. Eitzen’s paper concerns two-dimensional generalizations of De Bruijn sequences, namely, \( r \times n \) doubly periodic arrays (where \( r = 2^m \)) with the so-called “\( n \times m \) window property,” i.e., each \( n \times m \) binary matrix appears exactly once in one period of the array. Some generalizations are also considered.

Weber, de Vroedt, and Boecke consider codes for the Z-channel, a binary channel where the \( 1 \rightarrow 0 \) error occurs with probability \( p \) and the \( 0 \rightarrow 1 \) error essentially does not occur. There have been several papers in the IT Transactions on this subject plus others by Delgarte and Piret, Kloue, Shiozaki, and Varshamov. In the present paper new upper bounds on the maximum number of codewords in a linear code of length \( n \) and asymmetric distance \( \Delta \) are given. Construction methods for such codes with small length are discussed and several tables are included.

In [4] McEliece applied some sophisticated methods from number theory to the study of cyclic codes. These ideas are used by Remijn and Tiersma to prove that the weight enumerators of two seemingly unrelated codes,
namely, a \([q^m + 1, 2m]\) irreducible cyclic code and a certain \([q^m - 1, 2m]\) cyclic code over \(F_q\), are connected by a simple formula. The case \(q = 2\) had been shown by Dillon and later by Dür. In the meantime an extension of these results has been submitted to the IT Transactions by Lachaud and Wolfmann.

Finally, the correspondence by Leon deserves special mention. A combined effort of several editors, referees, and of the author himself has resulted in a period of four and a half years between submission and publication! By means of a probabilistic algorithm, the minimum weight of very large codes is determined with a certain probability of error (usually very small). Similar ideas have been used recently by other authors when the codes were too difficult to handle completely.

I feel privileged to have served as the Associate Editor for Coding Theory, and on balance I enjoyed the experience. Among the benefits is that, even if I had not been editor, I would have intended to read at least ten of the above fourteen papers, but it is not certain that this would really have happened. Now, I have read all of them and hope that others will do the same.

REFERENCES