[10] D. Blackwell, "Infinite codes for memoryless channels," *Ann. Math. Stat.*, vol. 30, pp. 1242–1244; December, 1960.

[11] D. Blackwell, "Exponential error bounds for finite-state channels," *Proc. 4th Berkeley Symp. on Math. Statistics and Probability*, University of California Press, Berkeley, vol. 1, pp. 57–63; 1961.

[12] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacity of a class of channels," *Ann. Math. Stat.*, vol. 30, pp. 1229–1241; December, 1959.

[13] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Stat.*, vol. 31, pp. 558–567; September, 1960.

[14] L. Breiman, Correction to "The individual ergodic theorem of information theory," *Ann. Math. Stat.*, vol. 31, pp. 809–810; September, 1960.

[15] L. Breiman, "On achieving channel capacity in finite-memory channels," *Illinois J. Math.*, vol. 4, pp. 246–252; June, 1960.

[16] L. Breiman, "Finite-state channels," *Trans. 2nd Prague Conf. on Information Theory, Statistical Decision Functions, Random Processes*, Academic Press, Inc., New York, N. Y., pp. 49–60; 1960.

[17] J. W. Carlyle, "Equivalent stochastic sequential machines," to appear in *J. Math. Anal. Appl.*

[18] K. L. Chung, "A note on the ergodic theorem of information theory," *Ann. Math. Stat.*, vol. 32, pp. 612–614; June, 1961.

[19] R. L. Dobrushin, "Mathematical problems in the Shannon theory of optimal coding of information," *Proc. 4th Berkeley Symp. on Math. Statistics and Probability*, University of California Press, Berkeley, vol. 1, pp. 211–252; 1961.

[20] R. L. Dobrushin and B. S. Tsybakov, "Information transmission with additional noise," IRE Trans. on Information Theory, vol. IT-8, pp. 293–304; September, 1962.

[21] R. M. Fano, "Transmission of Information," Technology Press of M.I.T., Cambridge, Mass., and Wiley, New York, N. Y.; 1961.

[22] R. Fortet, "Hypothesis testing and estimation of Laplacian functions," *Proc. 4th Berkeley Symp. on Mathematical Statistics and Probability*, University of California Press, Berkeley, vol. 1, pp. 289–305; 1961.

[23] E. J. Gilbert, "On the identifiability problem for functions of finite Markov chains," *Ann. Math. Stat.*, vol. 30, pp. 688–697; September, 1959.

[24] P. R. Halmos, "Recent progress in ergodic theory," *Bull. Am. Math. Soc.*, vol. 67, pp. 70–80; January, 1961.

[25] R. Y. Huang and R. A. Johnson, "Information capacity of time-continuous channels," IRE Trans. on Information Theory, vol. IT-8, pp. 191–198; September, 1962.

[26] H. Kesten, "Some remarks on the capacity of compound channels in the semicontinuous case," *Information and Control*, vol. 4, pp. 169–184; September, 1961.

[27] J. Kieffer and J. Wolfowitz, "Channels with arbitrarily varying channel probability functions," *Information and Control*, vol. 5, pp. 44–54; March, 1962.

[28] S. Kotz, "Exponential bounds on the probability of error for a discrete memoryless channel," *Ann. Math. Stat.*, vol. 32, pp. 577–582; June, 1961.

[29] S. C. Moy, "A note on generalizations of Shannon-McMillan theorem," *Pacific J. Math.*, vol. 11, pp. 1459–1465; Winter, 1961.

[30] K. R. Parthasarathy, "On the integral representation of the rate of transmission of a stationary channel," *Illinois J. Math.*, vol. 5, pp. 299–305; June, 1961.

[31] F. M. Reza, "An Introduction to Information Theory," McGraw-Hill Book Company, Inc., New York, N. Y.; 1961.

[32] W. L. Root, "Communications through unspecified additive noise," *Information and Control*, vol. 4, pp. 15–29; March, 1961.

[33] C. E. Shannon, "Coding theorems for a discrete source with a fidelity criterion," in "Information and Decision Processes," R. E. Machol, Ed., McGraw-Hill Book Company, Inc., New York, N. Y., pp. 93–126; 1960. (Also in 1959 IRE National Convention Record, pp. 142–163.)

[34] C. E. Shannon, "Two-way communication channels," *Proc. 4th Berkeley Symp. on Math. Statistics and Probability*, University of California Press, Berkeley, vol. 1, pp. 611–644; 1961.

[35] D. Slepian, "The threshold effect in modulation systems that expand bandwidth," IRE Trans. on Information Theory, vol. IT-8, pp. 122–127; September, 1962.

[36] A. J. Thomasian, "An elementary proof of the AEP of information theory," *Ann. Math. Stat.*, vol. 31, pp. 452–456; June, 1960.

[37] A. J. Thomasian, "The metric structure of codes for the binary symmetric channel," *Proc. 4th Berkeley Symp. on Math. Statistics and Probability*, University of California Press, Berkeley, vol. 1, pp. 669–679; 1961.

[38] A. J. Thomasian, "Error bounds for continuous channels," *Proc. 4th London Symp. on Information Theory*, C. Cherry, Ed., Butterworths, Washington, D. C., pp. 46–60; 1961.

[39] A. J. Thomasian, "A finite criterion for indecomposable channels," to appear in *Ann. Math. Stat.*, vol. 34, pp. 337-338; March, 1963.

[40] L. Weiss, "On the strong converse of the coding theorem for symmetric channels without memory," *Quart. Appl. Math.*, vol. 18, pp. 209–214; 1960.

[41] J. Wolfowitz, "Simultaneous channels," *Arch. Rational Mech. Anal.*, vol. 4, pp. 371–386; 1960.

[42] J. Wolfowitz, "A channel with infinite memory," *Proc. 4th Berkeley Symp. on Math. Statistics and Probability*, University of California Press, Berkeley, vol. 1, pp. 763–767; 1961.

[43] J. Wolfowitz, "Coding theorems of Information Theory," Springer-Verlag, Berlin, Germany, and Prentice-Hall, Englewood Cliffs, New Jersey; 1961.

CODING THEORY

W. W. PETERSON,* MEMBER, IEEE, AND J. MASSEY†

Algebraic Coding Theory

The class of error-correcting codes studied most during the past several years is the class of cyclic codes. A cyclic code is a parity-check code which has the property that every cyclic permutation of a code word is also a code word. This class includes the Hamming codes, the well-known Golay perfect (23, 12) code, the "maximal length sequence" codes. It also includes the important class of codes discovered independently by Bose and Ray-Chaudhuri [15] and Hocquenghem [61], and the class of double-adjacent error-correcting codes found by Abramson [1]. These latter papers are to a large measure responsible for interest in cyclic codes for random-error and burst-error correction respectively.

A large class of burst-error-correcting cyclic codes with small redundancy has been found by Fire [38] and a number of workers have found codes with minimum or near-minimum redundancy for correcting short bursts [2], [3], [33], [41], [55], [56], [95]. Some of the work includes nonbinary codes [32], [90]. Furthermore, very simple and efficient encoding and error-correcting equipment can be built for any burst-error-correcting cyclic code [79]–[82], [90].

Progress in the study of cyclic codes for random-error correction has been spurred by the interest and efforts of a number of algebraists. Reed and Solomon [93] discovered a new class of codes closely related to the Bose-Chaudhuri-Hocquenghem codes. Then Solomon and Mattson [104] found that the ideas behind the Reed-Solomon codes could be used as the basis for a new way of treating the generalized Bose-Chaudhuri codes, and they were able to determine specific properties of certain cyclic codes with their methods. H. B. Mann [76]

* Department of Electrical Engineering, University of Florida, Gainesville, Fla.

† Department of Electrical Engineering, University of Notre Dame, Notre Dame, Ind.

has derived expressions for the number of information symbols in a Bose-Chaudhuri-Hocquenghem code. Interest is still high [10], [20], [51], and new results along these lines can be expected.

Some of the algebraically oriented coding theory of the past three years applies to parity-check codes in general [9], [18], [34], [59], [67], [97], [99]. Slepian [103] has published new work relating to group-code equivalence and to sums and products of codes. MacWilliams [75] has found a formula for determining the weight distribution of a code from the weight distribution of its null space. From this, Pless [91] has derived a formula for the sum of the rth powers of the weights of all code words in a code, for any integer r. Independently, Assmus and Mattson [6], [118], have derived an interesting theorem which gives as a corollary a formula for the sum of the squares of the weights of code words. Solomon [105] also has an interesting weight formula. Many of these results have been helpful in determining properties of specific cyclic codes [7], [78], [83], [106].

Some very simple decoding methods and equipment have been designed for cyclic random-error-correcting codes. The general method of Meggitt [79]–[82] applies, but refinements are necessary for practical implementation. Prange [92] has described an idea involving the choice of information sets which leads to simple decoding of short cyclic codes. Massey [77] has found very simple implementations for several cyclic and recurrent codes. Rudolph [98] (and Kasami in Japan) have found very simple and practical decoding algorithms for some short cyclic codes. At least two corporations in the United States, General Electric Company and Codex Corporation, plan to build and market simple cyclic or recurrent error-correcting encoders and decoders.

A decoder for a 127-bit 5-error-correcting Bose-Chaudhuri-Hocquenghem code has been constructed by Bartee [11]. This machine is roughly the size of a file-cabinet drawer. It is made from 1-μsec transistor and diode logic, and can process roughly 4000 bits per second. A similar machine design was done by Moss [85].

A variety of coding schemes suited to special types of errors have been reported recently. Wolf and Elspas [114] have introduced the concept of error-location codes. Stone [109] has discussed the problem of correcting multiple bursts, and Reed and Solomon [93] have pointed out the applicability of certain nonbinary codes to this situation. Calingaert [19] has described a code for correcting a "spot" of errors in a two-dimensional array. A method for correcting for a bit loss or gain was devised by Sellers [100], and Gallager [45] has pointed out that sequential decoding can be adapted to correct for this type of error.

A type of coding based on ordinary arithmetic has been studied by Brown [16], Henderson [60], Bernstein and Kim [14], and Chien [25]. The coded form of the number n is of the form $An + B$. The error-correction capabilities are dependent on the value chosen for A and the limits on the range of n. Since the encoding operation is linear, these codes can be used to check an adder. In that case, they can detect or correct carry errors as well as the more commonly considered digit errors. Since encoding and decoding can be done by ordinary arithmetic, these codes could be used conveniently in communication between computers.

Freiman [42] and Berger [12], [13] have found codes well adapted to an assymetric channel. One particularly interesting coding scheme uses as check symbols a count, possibly weighted, of the "ones" in the information. The count is expressed as the complement of the conventional binary number. Then an error pattern which changes only ones to zeros, or vice versa, is always detected.

More refined bounds on the error-correcting capabilities of codes have been found [8], [53], [54]. Both upper and lower bounds are known for burst-correcting codes [21], [90]. Perhaps the most interesting new work, reported by Johnson [65], [66] and Gramenopoulos [52] are two different upper bounds on minimum distance which are assymptotically lower than the Hamming or Plotkin bounds.

Some interesting binary and nonbinary sequences with good autocorrelation properties have been found recently [48], [50], [62], [64], [88]. These sequences, which can be used as error-correcting codes, also have applications in spectroscopy and radar and communication signal design.

The work traditionally designated coding theory and that called signal design differ only in that the former deals with discrete spaces and the latter deals with continuous spaces. Otherwise they are the same, and in fact Shannon [101] considers both to be special cases of transformations of signals or information, and uses the term coding for both. J. L. Kelly [71] has published a random-coding-type theorem that applies to continuous channels and for which the codes bear some resemblance to group codes. Harmuth [57] and Franco and Lachs [44] have found methods of constructing continuous codes (*i.e.*, signal design) based on discrete error-correcting codes. Recent work by Frank, Zadoff, and Heimiller [43], [58], Viterbi [112] and Stutt [111] is at least related very closely to conventional coding theory. Other work in the area of signal design is summarized in another section.

Present Status of Algebraic Coding Theory

Shannon's fundamental theorem for the noisy channel [101], which sets limits on the amount of information which can be transmitted reliably through a noisy channel, was the initial motivation and goal for work on error-correcting codes. Shannon [102] and Elias [31] later sharpened that goal by deriving bounds which show the relationship between code length and error probability for the best code for certain channels.

The simplest and best-understood noisy channel is the binary symmetric channel in which the error probability is the same for both symbols and independent from symbol to symbol. For this channel, the Bose-Chaudhuri-Hocquenghem codes are far the best codes known at the present, and in many instances such codes can be very effectively used to control errors. For example, if the channel error probability is 0.01, the 20-error-correcting Bose-Chaudhuri-Hocquenghem code of length 511 symbols, results in a probability for erroneous decoding of approximately 8×10^{-8}. Bounds of the type derived by Shannon and Elias show that the best parity-check code with 340 information and 171 check symbols has an error probability lying between 3.7×10^{-16} and 2.6×10^{-17}. These same bounds show that the shortest code in which one-third of the symbols are parity-check symbols, and which has error probability less than 8×10^{-8} must have its length between 171 and 213. Thus the best codes which we know fall far short of what is possible.

The figure 3.7×10^{-16} is an upper bound on the average error probability for all codes with 340 information and 171 check symbols. Thus the Bose-Chaudhuri codes fall far short of average! Yet, they are the best codes for which the construction and correction procedure can be given explicitly now. There are two possible explanations: the correction procedure for correcting any combination of 20 or fewer errors is not optimum, because there are many combinations of more than 20 errors which this code certainly could correct. No effective method for correcting these error patterns is known, and it is not even known how much lower the error probability would be if optimum decoding were possible. Thus these codes might be near optimum although it has not been proved, or alternatively they might indeed be nonoptimum and even worse-than-average codes!

This state of affairs has challenged coding theorists and the modest but important and rather steady progress in this area in the past several years has spurred them on, and has paid off both in producing useful codes and in some practical equipment designs. It has also motivated the study of systems based on randomly chosen codes as an alternative to the so-far unsuccessful search for near-optimum codes of algebraic structure.

Progress in Random Coding

The term "random coding" is commonly applied to the process of computing average properties of an ensemble of codes in which all codes are assigned equal probability. The first proof of the noisy coding theorem by Shannon [101] was based on random coding and most of the recent progress in random coding has been made by the workers gathered about Shannon at M.I.T. The tightness of the bounds on average probability of error, $P(e)$, for a random code ensemble has been greatly enhanced by the introduction of the technique of Chernoff [24]. Fano [35] has recently extended the earlier work of Feinstein [37] and Elias [31] to the general discrete memoryless channel (DMC) and has shown that for rates (R) between some critical rate and channel capacity (C) the exponent $nE(R)$, where n is the code length, in the expression for $P(e)$ obtained by random coding is equal to the exponent in the lower bound for the probability of error with any code. A random code ensemble with this property is called optimum.

One interesting question is the size of the ensemble necessary for the proof of optimality. Elias [31] had shown earlier that the ensemble of sliding parity check codes with only 2^n member codes is optimum on the binary symmetric channel (BSC). Wozencraft [77] recently discovered an optimum ensemble for the BSC with 2^N member codes where $N = \max (Rn, n - Rn)$. It might be expected that as the size of the ensemble is reduced the decoding effort should also be reduced because of the increased structure of the ensemble, but there have been no efficient decoding methods proposed for the sliding parity check ensemble or for the Wozencraft ensemble. The link between code structure and decoding effort is largely unexplored.

It is in the area of bounding decoding effort for specific ensembles that the most significant progress in random coding has been made in the past three years. Most of this work has been based on the earlier results obtained by Wozencraft [116], [117]. Wozencraft considered ensembles of tree codes such as the convolutional codes proposed by Elias [31]. The encoding and decoding of successive digits can be done in the same manner for such codes. The delay in digits between receipt of a digit and the attempt to decode it is called the constraint length, n_t, and is analogous to code length in a block code. Using a technique called sequential decoding, Wozencraft showed that the average number of computations in discarding the incorrect subset grew as only a small power of n_t for R less than some computational rate (R_{comp}) less than C, while at the same time $P(e)$ decreased exponentially with n_t. The incorrect subset is that part of the coding tree, diverging from the node corresponding to the digit being decoded, which branches out from the erroneous values of that digit. Sequential decoding utilizes successive searches of the coding tree until a good match to the received sequence is obtained, the criterion for rejecting sequences from consideration being made less stringent on each search.

Much effort has gone toward broadening and refining the results of Wozencraft. An important step was taken by Gallager [94] who suggested a method whereby the average computation in the entire decoding process could be bounded. Reiffen [94] showed that this gave a bound which grew as $n_t^{2(1+R/R_{\text{comp}})}$ for $R < R_{\text{comp}}$, thereby removing one of the major objections to sequential decoding.

It was soon realized that sequential decoding, because of its highly probabilistic structure, was applicable to a broad class of channels and many recent results are concerned with this extension. Reiffen [94] extended most of the major aspects of the theory to the DMC and the semicontinuous channel. For the DMC symmetric from its output, he was able to show that the average number of computations in discarding the incorrect subset is bounded by a quantity proportional to $n_t^{R/R_{\text{comp}}}$

for $R < R_{\text{comp}}$ and that $P(e)$ decreased with the same exponent as for an optimum ensemble. Reiffen showed further that R_{comp} was equal to $E(0)$ for such symmetric channels and was bounded above by $E(0)$ for the assymetric DMC.

Ziv [119] has recently made further extensions in several directions. First, he showed that R_{comp} was bounded below by $\frac{1}{2}E(0)$ for the assymetric DMC, and that the bound on average number of computations in discarding the incorrect subset grew as n_t^2. Second, Ziv introduced an entirely new concept into sequential decoding. Rather than using reject criteria, Ziv's decoder computes the *a posteriori* probability of paths in the tree and makes a decoding decision whenever this probability exceeds a fixed predetermined threshold. The scheme was analytically attractive and allowed Ziv to compute a bound on the average number of decoding computations which grows as $n_t^{1+R/R_{\text{comp}}}$ for $R < R_{\text{comp}}$ for the DMC. R_{comp} was found to be $\frac{1}{2}E(0)$ for this scheme, the same as the lower bound on R_{comp} for sequential decoding on assymetric channels.

Very recently, Fano [36] announced a major new result in sequential decoding. By employing a probability criterion in a novel manner that is both operationally simple and mathematically tractable, Fano succeeded in bounding the average number of decoding computations by a constant independent of n_t for the symmetric DMC. The full impact of this result can be expected in the near future and should serve to enlarge the interest of workers in random coding. Theoretical research is already underway in some quarters to apply random coding techniques to channels with simple kinds of memory and results can be expected in the near future.

In addition to the theoretical progress described above, there has been concurrent effort to bring sequential decoding to the hardware stage. One phase of this work was the construction of SECO (SEquential deCOder) under the direction of Perry [89] at the M.I.T. Lincoln Laboratory. SECO was completed in late 1962 and is now in operation. Essentially it is a special-purpose digital computer programmed to instrument the Wozencraft decoding alogorithm. It is capable of operation at rates up to 50 kilobits per second with constraint lengths up to 60 information bits for a wide range of information rates. SECO was intended primarily as a tool for proving the feasibility of sequential decoding on real channels. Impressive results have been obtained [120].

In addition to sequential decoding, a second promising random coding technique was discovered recently by Gallager [46]. Gallager has termed his method "low-density parity check" coding since it is a decoding method for the ensemble of nonsystematic binary parity check codes constrained to have a small fixed number of bits in each parity set. Gallager showed that the average minimum distance of the codes in this ensemble increases linearly with block length but the ratio is less than optimum. The important feature of Gallager's work is the operationally simple decoding alogorithm for which the average number of decoding operations per digit is independent of block length for rates sufficiently less than C. For the BSC, Gallager could establish only that $P(e)$ decreased exponentially as a root of the block length, but a reasonable conjecture would imply that the actual decrease was exponential with the block length. A computer simulation of the decoding process was made and the results support this conjecture. Low-density parity check decoding, like sequential decoding, can employ *a posteriori* information about the received digits. It can thus be expected to generalize to a broader class of channels.

The progress in random coding methods has been quite remarkable during the past three years. Moreover the momentum of the movement appears to be on the increase. We can expect that the report three years from now will not lack for fundamental coding theorems that owe their proofs to random coding methods, and that commercial use will then be being made of hardware based on random coding principles.

Real Channels

Understanding of real channels, like that of the binary symmetric channel, has progressed immensely in the past few years, yet leaving many problems unanswered. For example, only a few years ago it was presumed that the important noise in typical channels was Gaussian and that consequently for ordinary modulation schemes the binary symmetric channel was a fairly accurate model. Experience soon showed that errors usually occur in "bursts," and consequently interest arose in burst-error-correcting codes. This also instigated some thorough studies of error statistics with conventional modulation schemes and it was found that bursts come in bursts, that generally there will be long periods with few or no errors, and then relatively short periods of many errors [4], [17], [39]. The cause of the errors has been found to be impulse noise, typically caused by lightning, switching transients, power line transients, and similar problems. With these conventional modulation schemes, error-correcting codes without feedback seem to be of little help [40]. On the other hand error-detecting codes with request for retransmission have been used with extremely low probabilities of undetected errors.

Work with real channels has brought into focus two problems on which we can expect serious efforts in the near future. First is the consideration of the entire system—binary coding and modulation and signal design—together. Wozencraft and Perry and their associates are doing some experiments of this type with SECO and a real channel [89]. Work of this type has been done at N.Y.U. The other problem is, what is the best way to use feedback? On this problem also, pioneering work has been done at N.Y.U. by Chang [22], [23] and Metzner and Morgan [84]. Various aspects of the problem of error-detection and retransmission have been studied by Cowell [29], [30], Jacobs [63], and Wozencraft and Horstein [115].

Other Work

Weiss [113] has found that linear codes for information compression are closely related to parity-check error-correcting codes. Karp [68] has generalized Huffman's coding procedure to give minimum-cost encoding when the symbols have unequal costs. Cohn and Gorman [26] have shown an interesting address encoding. Karush [69] has given a new, greatly simplified proof of McMillan's inequality. Other work in this area has been concerned largely with the important problem of gaining synchronization and detecting synchronization errors [72], [107], [108], [45], [100]. Neumann's work [87] is particularly interesting, in that it relates the synchronization problem to the theory of sequential machines, thus applying concepts new to this problem. At the same time he can specify machines for detecting synchronization errors.

Armstrong [5] and Cowan and Winograd [28] have independently found a way to design a redundant digital machine using error-correcting codes. This is a very natural generalization of their use in communication systems. However, there are two problems here which are not so serious in the communication problem. First, while the number of redundant units may be very modest, there is no assurance that these units will be of the same size as the ones to be checked. On the contrary, it would appear that in the usual case, the redundant units are much larger. Secondly, an error-correction unit for the error-correcting code is needed, and there is no easy way to make it more reliable than the available components permit. While at first glance the results look favorable, in fact they seem to add more weight to previous results which indicate that there is very likely no general way of detecting or correcting errors in computers which is simpler than duplication or triplication. In certain special cases an improvement is possible. The load-sharing switching matrix, discovered independently by Takahashi and Goto [110] and Constantine [27], is a case in point [87]. A very useful summary of practical techniques for improving reliablity in digital equipment has been compiled by Kautz [70].

Bibliography

[1] N. M. Abramson, "A class of systematic codes for non-independent errors," IRE Trans. on Information Theory, vol. IT-5, pp. 150–157; December, 1959.

[2] N. M. Abramson, "Error correcting codes from linear sequential networks," *Proc. 4th London Symp. on Information Theory*, C. Cherry, Ed., Butterworths, Washington, D. C.; 1961.

[3] N. M. Abramson, "A note on single error correcting binary codes," IRE Trans. on Information Theory, vol. IT-6, pp. 502–503; September, 1960.

[4] A. A. Alexander, R. N. Gryb, and D. W. Nast, "Capabilities of the telephone network for data transmission," *Bell Sys. Tech. J.*, vol. 39, pp. 431–476; May, 1960.

[5] D. B. Armstrong, "A general method of applying error correction to synchronous digital systems," *Bell Sys. Tech. J.*, vol. 40, pp. 577–594; March, 1961.

[6] E. F. Assmus and H. F. Mattson, "Error-Correcting Codes, Axiomatic Approach," Sylvania Electronic Systems, Waltham, Mass., Arm No. 269.

[7] E. F. Assmus and H. F. Mattson, "On Determining the Weight-Distribution in Cyclic Codes of Prime Block Length," Appl. Res. Lab., Sylvania Electric Products, Inc., Engrg. Note No. 253.

[8] R. P. Bambah, D. D. Joshi, and I. S. Luthar, "Some lower bounds on the number of code points in a minimum distance binary code," *Information and Control*, vol. 4, pp. 313–325; December, 1961.

[9] R. B. Banerji, "On constructing group codes," *Information and Control*, vol. 4, pp. 1–14; March, 1961.

[10] R. B. Banerji, "A decoding procedure for double-error-correcting Bose-Ray-Chaudhuri codes," Proc. IRE, vol. 49, p. 1585; October, 1961.

[11] T. C. Bartee and D. I. Schneider, "An electronic decoder for Bose-Chaudhuri-Hocquenghem codes," IRE Trans. on Information Theory, vol. IT-8, pp. 17–24; September, 1962.

[12] J. M. Berger, "A note on error-detection codes for asymmetric channels," *Information and Control*, vol. 4, pp. 68–73; March, 1961.

[13] J. M. Berger, "A note on burst error detecting sum codes," *Information and Control*, vol. 4, pp. 297–299; September, 1961.

[14] A. J. Bernstein and W. H. Kim, "Linear codes for single error correction in symmetric and asymmetric computational processes," IRE Trans. on Information Theory, vol. IT-8, pp. 29–34; January, 1962.

[15] R. C. Bose and D. K. Ray-Chaudhuri, "A class of error-correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79; March, 1960.

[16] D. T. Brown, "Error detecting and correcting binary codes for arithmetic operations," IRE Trans. on Electronic Computers, vol. EC-9, pp. 333–337; September, 1960.

[17] E. W. Brown, A. W. Hatch, and P. A. Portman, "Analysis of Binary Error Statistics Obtained on VHF Scatter Communications Systems," presented at URSI-IRE Meeting, Washington, D. C., April 30–May 3, 1962.

[18] L. Calabi, "A note on rank and nullity in coding theory," *Information and Control*, vol. 4, pp. 359–363; December, 1961.

[19] P. Calingaert, "Two dimensional parity checking," *J. ACM*, vol. 8, pp. 186–200; April, 1961.

[20] C. N. Campopiano, "Construction of relatively maximal, systematic codes for specified minimum distance from linear recurring sequences of maximal period," IRE Trans. on Information Theory, vol. IT-6, pp. 523–528; December, 1960.

[21] C. N. Campopiano, "Bounds on burst-error-correcting codes," IRE Trans. on Information Theory, vol. IT-8, pp. 257–259; April, 1962.

[22] S. L. Chang, "Theory of information feedback systems," IRE Trans. on Information Theory, vol. IT-2, pp. 29–40; September, 1956.

[23] S. S. L. Chang, "Improvement of two-way communication by means of feedback," 1961 IRE International Convention Record, pt. 4, pp. 88–104.

[24] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on a sum of observations," *Ann. Math. Stat.*, vol. 23, pp. 493-507; December, 1952.

[25] R. T. Chien, "Linear Codes for Burst-Error-Correction in Binary Arithmetic and Transmission," Internat'l Business Machine Corp., Yorktown Heights, N. Y., IBM Res. Rept. RC-817; 1962.

[26] D. L. Cohn and J. M. Gorman, "A code separation property," IRE Trans. on Information Theory, vol. IT-8, pp. 382–383; October, 1962.

[27] G. Constantine, "A load-sharing matrix switch," *IBM J. Res. & Dev.*, vol. 2, pp. 204-211; July, 1958.

[28] J. D. Cowan, W. S. McCulloch, and S. Winograd, "Redundant Computation in Anastomotic Nets of Formal Neurons," in "Redundancy Techniques for Computer Systems," R. H. Wilcox and W. C. Mann, Eds. Spartan Books, Washington, D. C., 1962.

[29] W. R. Cowell, "The use of group codes in error detection and message retransmission," IRE Trans. on Information Theory, vol. IT-7, pp. 168–171; July, 1961.

[30] W. R. Cowell and H. O. Burton, "Computer simulation of the use of group codes with retransmission on a Gilbert burst channel," *Trans. AIEE*, vol. 81 (*Commun. and Electronics*), pp. 577–585; January, 1962.

[31] P. Elias, "Coding for noisy channels," 1955 IRE Convention Record, pt. 4, pp. 37–46.

[32] B. Elspas, "A note on p-nary adjacent-error correcting codes," IRE Trans. on Information Theory, vol. IT-6, pp. 13–15; March, 1960.

[33] B. Elspas and R. A. Short, "A note on optimum burst-error correcting codes," IRE Trans. on Information Theory, vol. IT-8, pp. 39–42; January, 1962.

[34] C. Engelman, "On close-packed double error-correcting codes on P symbols," IRE Trans. on Information Theory, vol. IT-7, pp. 51–52; January, 1961.

[35] R. M. Fano, "Transmission of Information," M.I.T. Technology Press, Cambridge, Mass., and Wiley, New York, N. Y.; 1961.

[36] R. M. Fano, "A heuristic discussion of probabilistic decoding," IEEE Trans. on Information Theory, vol. IT-9, pp. 64–74; April, 1963.

[37] A. Feinstein, "A new basic theorem of information theory," IRE Trans. on Information Theory, vol. IT-4, pp. 2–22; September, 1954.

[38] P. Fire, "A Class of Multiple-Error-Correcting Binary Codes for Non-Independent Errors," Sylvania Electric Products, Inc., Mt. View, Calif., Rept. RSL-E-2; March, 1959.

[39] A. B. Fontaine, "Applicability of Coding to Radio Teletype Channels," M.I.T. Lincoln Laboratory, Lexington, Mass., 25G-3; October 27, 1961.

[40] A. B. Fontaine and R. G. Gallager, "Error statistics and coding for binary transmission over telephone circuits," Proc. IRE, vol. 49, pp. 1059–1065; June, 1961. See also M.I.T. Lincoln Laboratory, Lexington, Mass.; Rept. No. 25G0023.

[41] C. R. Foulk, "Some Properties of Maximally-Efficient Cyclic Burst-Correcting Codes and Results of a Computer Search for Such Codes," Digital Computer Lab., Univ. of Illinois, Urbana, File No. 375; June 12, 1961.

[42] C. V. Freiman, "Optimal error detection codes for completely asymmetric channels," *Information and Control*, vol. 5, pp. 72–86; March, 1962.

[43] R. L. Frank, S. A. Zadoff, and R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," IRE Trans. on Information Theory, vol. IT-8, pp. 381–382; October, 1962.

[44] G. A. Franco and G. Lachs, "An orthogonal coding technique for communications," 1961 IRE International Convention Record, pt. 8, pp. 126–133.

[45] R. G. Gallager, "Sequential decoding for binary channels with noise and synchronization errors," M.I.T. Lincoln Lab., Lexington, Mass., 25G-2; October 27, 1961.

[46] R. G. Gallager, "Low density parity check codes," IRE Trans. on Information Theory, vol. IT-8, pp. 21–28; January, 1962.

[47] E. N. Gilbert, "Synchronization of binary messages," IRE Trans. on Information Theory, vol. IT-6, pp. 470–477; September, 1960.

[48] A. Gill, "A theorem concerning compact and cyclic sequences," IRE Trans. on Information Theory, vol. IT-8, pp. 225–255; April, 1962.

[49] F. M. Goetz, "Self-Correcting Codes for Errors in Synchronization," M.S. thesis, Dept. of Math., New York Univ., N. Y.; March, 1960.

[50] M. J. E. Golay, "Complementary series," IRE Trans. on Information Theory, vol. IT-7, pp. 82–87; April, 1961.

[51] D. Gorenstein, W. W. Peterson and N. Zierler, "Two-error correcting Bose-Chaudhuri codes are quasi-perfect," *Information and Control*, vol. 3, pp. 291-294; September, 1960.

[52] N. Gramenopoulos, "An Upper Bound for Error-Correcting Codes," M.S. thesis, Mass. Inst. Tech., Cambridge; 1963.

[53] L. D. Grey, "Some bounds for error-correcting codes," IRE Trans. on Information Theory, vol. IT-8, pp. 200–203; April, 1962.

[54] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res. & Dev.*, vol. 4, pp. 532–542; July, 1960.

[55] A. J. Gross, "Binary group codes which correct in bursts of three or less for odd redundancy," IRE Trans. on Information Theory, vol. IT-8, pp. 356–359; October, 1962.

[56] A. J. Gross, "A note on some binary group codes which correct errors in bursts of four or less," IRE Trans. on Information Theory, vol. IT-8, p. 384; October, 1962.

[57] H. F. Harmuth, "Orthogonal Codes," Inst. of Elec. Engrg. (British) Monograph No. 369E; March, 1960.

[58] R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," IRE Trans. on Information Theory, vol. IT-7, pp. 254–257; October, 1961.

[59] C. W. Helstrom, "Maximum-weight group codes for the balanced *M*-ary channel," IRE Trans. on Information Theory, vol. IT-6, pp. 550–554; December, 1960.

[60] D. S. Henderson, "Residue class error checking codes," Ph.D. dissertation, Harvard University, Cambridge, Mass.; 1961.

[61] A. Hocquenghem, "Codes Correcteurs Derreurs," *Chiffres 2*, pp. 147–156; September, 1959.

[62] D. A. Huffman, "The generation of impulse-equivalent pulse trains," IRE Trans. on Information Theory, vol. IT-8, pp. 10–16; September, 1962.

[63] I. Jacobs, "Optimal error-detection codes for noiseless decision feedback," IRE Trans. on Information Theory, vol. IT-8, pp. 359–371; October, 1962.

[64] S. Jauregui, Jr., "Complementary sequences of length 26," IRE Trans. on Information Theory, vol. IT-8, p. 323; July, 1962.

[65] S. M. Johnson, "A New Upper Bound For Error-Correcting Codes," Math. Dept., The RAND Corporation, Santa Monica, Calif., P-2294-1; May 8, 1961.

[66] S. Johnson, "On Perfect Error-Correcting Codes," Memo. RM 3403-PR; December, 1962.

[67] D. M. Jones and J. J. Bussgang, "Tree-like structure of block-codes," IRE Trans. on Information Theory, vol. IT-8, pp. 384–385; October, 1962.

[68] R. M. Karp, "Minimum-redundancy coding for the discrete noiseless channel," IRE Trans. on Information Theory, vol. IT-7, pp. 27–38; January, 1961.

[69] J. Karush, "A simple proof of an inequality of McMillan," IRE Trans. on Information Theory, vol. IT-7, p. 118; April, 1961.

[70] W. Kautz, "Codes and Coding Circuitry for Automatic Error-Correction Within Digital Systems," in "Redundancy Techniques for Computing Systems," R. H. Wilcox and W. C. Mann, Eds. Spartan Books, Washington, D. C.; 1962.

[71] J. L. Kelly, "A class of codes for signaling on a noisy continuous channel," IRE Trans. on Information Theory, vol. IT-6, pp. 22–24; March, 1960.

[72] W. B. Kendall and I. S. Reed, "Path-Invariant Comma-Free Codes," The RAND Corporation, Santa Monica, Calif., P-23771-1; July, 1961 (revised September, 1961).

[73] W. Kilmer, "Linear-recurrent binary error-correcting codes for memoryless channels," IRE Trans. on Information Theory, vol. IT-7, pp. 7–12; January 1961.

[74] J. MacWilliams, "Error-correcting codes for multiple level transmission," *Bell Sys. Tech. J.*, vol. 40, pp. 281–308; January, 1961.

[75] J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Sys. Tech. J.*, vol. 42, pp. 79–94; January, 1963.

[76] H. B. Mann, "On the Number of Information Symbols in Bose-Chaudhuri Codes," Math. Res. Center, Univ. of Wisconsin, Madison, MRC Tech. Summary Rept. No. 249; August, 1961.

[77] J. L. Massey, "Threshold Decoding," The M. I. T. Press, Cambridge, Mass.

[78] H. F. Mattson, "On the (41, 21) Cyclic Code Over GF(2)," Applied Res. Lab., Sylvania Electronic Systems; April, 1962.

[79] J. E. Meggitt, "Error-correcting codes for correcting bursts of errors," *IBM J. Res. & Dev.*, vol. 4, pp. 329–334; July, 1960.

[80] J. E. Meggitt, "Error-correcting codes for correcting bursts of errors," *Trans. AIEE*, vol. 80 (*Commun. and Electronics*), pp. 708–711; January, 1961.

[81] J. E. Meggitt, "Error-correcting codes and their implementation for data transmission systems," IRE Trans. on Information Theory, vol. IT-7, pp. 234–244; October, 1961.

[82] C. M. Melas, "Reliable data communication through noisy media," *Trans. AIEE*, vol. 80 (*Commun. and Electronics*), pp. 501–504; November, 1961.

[83] C. M. Melas, "A cyclic code for double error correction," *IBM J. Res. & Dev.*, vol. 4, pp. 364–366; July, 1960.

[84] J. J. Metzner and K. C. Morgan, "Coded feedback communication systems," *Trans. AIEE*, vol. 81 (*Commun. and Electronics*), pp. 643–647; January, 1962.

[85] M. J. Moss, "Implementation of the Bose-Chaudhuri Error-Correcting Codes," M.S. thesis, Dept. of Elec. Engrg., Univ. of Fla., Gainesville; June, 1961.

[86] P. G. Neumann, "Efficient error-limiting variable-length codes," IRE Trans. on Information Theory, vol. IT-8, Pt. I, pp. 292–304, July, 1962; Pt. II, pp. S260–S266, September, 1962.

[87] P. G. Neumann, "On the logical design of noiseless load-sharing matrix switches," IRE Trans. on Electronic Computers, vol. EC-11, pp. 1–6; June, 1962.

[88] P. G. Neumann, "A note on cyclic permutation error-correcting codes," *Information and Control*, vol. 5, pp. 72–86; March, 1962.

[89] K. M. Perry and J. M. Wozencraft, "SECO: a self-regulating error-correcting coder-decoder," IRE Trans. on Information Theory, vol. IT-8, pp. 128–135; September, 1962.

[90] W. W. Peterson, "Error Correcting Codes," M.I.T. Technology Press, Cambridge, Mass., and Wiley, New York, N. Y.; 1961.

[91] V. Pless, "Power moment identities on weight distributions in error-correcting codes," to appear in *Information and Control.*

[92] E. Prange, "The use of information sets in decoding cyclic codes," IRE Trans. on Information Theory, vol. IT-8, pp. 5–9; September, 1962.

[93] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. SIAM*, vol. 8, pp. 16–21; July, 1960.

[94] B. Reiffen, "Sequential decoding for discrete input memoryless channels," IRE Trans. on Information Theory, vol. IT-8, pp. 208-220; April, 1962.

[95] S. H. Reiger, "Codes for the Correction of Clustered Errors," IRE Trans. on Information Theory, vol. IT-6, pp. 16–21; March, 1960.

[96] F. M. Reza, "An Introduction to Information Theory," McGraw-Hill Book Company, Inc., New York, N. Y.; 1961.
[97] M. Rubinoff, "*N*-dimensional codes for detecting and correcting multiple errors," *Comm. ACM*, vol. 4, pp. 545–551; December, 1961.
[98] L. Rudolph, "Easily Implemented Error Correction Encoding-Decoding," General Electric Company, Oklahoma City, Okla., Rept. 62MCD2; 1962.
[99] A. A. Sardinas, "Bounds on Minimum Distance for Product Codes with Parity Check Constraints," Ph.D. dissertation, Univ. of Pennsylvania, Philadelphia; 1962.
[100] F. F. Sellers, "Bit loss and gain correction code," IRE Trans. on Information Theory, vol. IT-8, pp. 35–38; January, 1962.
[101] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. J.*, vol. 27, July, pp. 379–423, October, pp. 623–656; 1948.
[102] C. E. Shannon, "Certain results in coding theory for noisy channels," *Information and Control*, vol. 1, pp. 6–25; September, 1957.
[103] D. Slepian, "Some further theory of group codes," *Bell Sys. Tech. J.*, vol. 39, pp. 1219–1252; September, 1960.
[104] G. Solomon and H. F. Mattson, "A new treatment of Bose-Chaudhuri codes," *J. SIAM*, vol. 9, pp. 654–669; December, 1961.
[105] G. Solomon, "A weight formula for group codes," IRE Trans. on Information Theory, vol. IT-8, pp. 1–4; September, 1962.
[106] G. Solomon, "A note on a new class of codes," *Information and Control*, vol. 4, pp. 364–370; December, 1961.
[107] J. J. Stiffler, "Self Synchronizing Codes for the Continuous Channel," presented at the URSI-IRE Meeting, Washington, D. C., April 30–May 3; 1962.
[108] J. J. Stiffler, "Synchronization methods for block codes," IRE Trans. on Information Theory, vol. IT-8, pp. 25–34; September, 1962.
[109] J. J. Stone, "Multiple burst error correction," *Information and Control*, vol. 4, pp. 324–331; December, 1961.
[110] H. Takahasi and E. Goto, "Application of error-correcting codes to multi-way switching," *Proc. Internat'l Conf. on Information Processing*, Paris; June, 1959.
[111] C. A. Stutt, "Information rate in a continuous channel for regular-simplex codes," IRE Trans. on Information Theory, vol. IT-6, pp. 516–522; December, 1960.
[112] A. J. Viterbi, "On coded phase-coherent communications," IRE Trans. on Space Electronics and Telemetry, vol. SET-7, pp. 3–14; March, 1961.
[113] E. Weiss, "Compression and coding," IRE Trans. on Information Theory, vol. IT-8, pp. 256–57; April, 1962.
[114] J. K. Wolf and B. Elspas, "Error-locating codes—a new concept in error control," IEEE Trans. on Information Theory, vol. IT-9, pp. 113–117; April, 1963.
[115] J. M. Wozencraft and M. Horstein, "Coding for two-way channels," *Proc. 4th London Symp. on Information Theory*, C. Cherry, Ed., Butterworths, Washington, D. C.; 1961.
[116] J. M. Wozencraft, "Sequential Decoding for Reliable Communication," M.I.T. Res. Lab. of Electronics, Cambridge, Mass., RLE Tech. Rept. 325; August, 1957.
[117] J. M. Wozencraft and B. Reiffen, "Sequential Decoding," Technology Press of M.I.T., Cambridge, Mass., and Wiley, New York, N. Y.; 1961.
[118] N. Zierler, "A note on mean square weight for group codes," *Information and Control*, vol. 5, pp. 87–89; March, 1962.
[119] J. Ziv, "Coding and decoding for time-discrete amplitude-continuous memoryless channels," IRE Trans. on Information Theory, vol. IT-8, pp. S199–S205; September, 1962.
[120] I. Lebow, *et. al.*, "Application of sequential decoding to high-rate data communication on a telephone line," IRE Trans. on Information Theory, vol. IT-9, pp. 124-126; April, 1963.

CONTRIBUTIONS TO SIGNAL AND NOISE THEORY

DAVID SLEPIAN*, Fellow, IEEE

A. Signal Theory

Refs. [1]–[17] indicate some of the activity in signal theory during the period under consideration. A number of the researches were concerned with the design of signals to achieve specific aims: the design of radar pulses to obtain good resolution in range and velocity, as treated by Klauder in [8] and by Sussman [17]; the attainment of prescribed correlation properties, Frank and Zadoff [3], Heimiller [5], Huffman [7], and Max [14]; or the elimination of intersymbol interference, Gerst and Diamond [4]. Others, Bedrosian [1], dealt with general representation problems of the signals commonly met in communication systems.

Interest in band-limited signals and their special properties continued to run high. The sampling theorem was extended by Linden and Abramson [13], and the error introduced in truncated sampling series was investigated by Helms and Thomas [6]. Several surprising facts about strictly band-limited signals came to light. Such signals can have much of their energy in semi-infinite regions where their Nyquist samples vanish, Pollak [15]. They are peculiarly robust as evidenced by the following, Landau [9], Landau and Miranker [10]. Let a band-limited signal $x(t)$ be distorted by an instantaneous device to produce a signal $y(t) = F[x(t)]$, no longer, in general, band-limited. Let y be restricted to the band of x by passage through an ideal filter to yield a signal $z(t)$. With certain weak restrictions on the nature of F, x can be reconstructed from z.

The extent to which a signal can be simultaneously concentrated in both the time and frequency domains was examined in detail in a series of three papers, [16], [11], [12] by Landau, Pollak and Slepian. In the last of these, Landau and Pollak prove a solid mathematically meaningful version of the long-standing ill-defined folk theorem that proclaims that signals of bandwidth W and duration T have $2WT$ degrees of freedom. Prolate spheroidal wave functions were shown to play a natural important role in the solution of many problems concerning the concentration of signals.

B. Noise Theory

Noise researches pertaining primarily to detection, estimation, filtering, prediction, and specific communication systems are treated elsewhere in this report. Even excluding these specific subjects, work in noise theory was most extensive. The listing made here must then necessarily be representative, rather than exhaustive.

The subject matter of noise theory has no well-defined borders, but instead shades off continuously into physics in one direction and into probability theory, statistics and pure mathematics in another direction. For this survey arbitrary boundaries have been drawn. We proceed from near the frontier with Physica and wander towards Mathematica.

Many papers appeared during the period that discussed the noise properties of new devices—tunnel diodes, transistors, masers, etc., and new circuit arrangements. Noise figure calculations and equivalent circuit configurations play a key role here. A few representative titles are given [18]–[30].

* Bell Telephone Laboratories, Inc., Murray Hill, N. J.