and deg $(e_2(x)) \geq m_0$. If $f \leq m_0$, then $x^i e_1(x) \not\equiv e_2(x) \bmod g_1(x^b)g_2(x)$. Therefore the shortened cyclic code generated by $g(x) = g_1(x^b)g_2(x)$ is capable of correcting all single-burst errors of length min $\{m_0, bt\}$ or less.

Earlier we presented a class of shortened cyclic codes for a compound channel [4]. A code in this class was generated by the polynomial $g(x) = (x^d + 1)g'(x)$ where $g'(x)$ generates a t-error-correcting cyclic code of length N. A comparison shows that for the same number of check digits, the shortened cyclic codes presented here have a better rate of transmission, but the earlier shortened cyclic codes have a better guaranteed burst-error correction capability.

Acknowledgment

The author is very grateful to Prof. J. L. Massey for helping with the preparation of this correspondence.

References

[1] J. J. Stone, "Multiple-burst error correction with the Chinese remainder theorem," *J. Soc. Ind. Appl. Math.*, vol. 11, pp. 74–81, Mar. 1963.
[2] D. Mandelbaum, "A method of coding for multiple errors," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-14, pp. 518–521, May 1968.
[3] H. T. Hsu, T. Kasami, and R. T. Chien, "Error-correcting codes for a compound channel," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 135–139, Jan. 1968.
[4] H. T. Hsu, "A class of binary shortened cyclic codes for a compound channel," *Inform. Contr.*, vol. 18, pp. 126–139, Mar. 1971.
[5] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd ed. Cambridge, Mass.: M.I.T. Press, 1970.
[6] T. Kasami, "Optimum shortened cyclic codes for burst-error correction," *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 105–109, Apr. 1963.

On the Fractional Weight of Distinct Binary n-Tuples

JAMES L. MASSEY

***Abstract*—It is shown that the fraction p of ones in the Mn positions of M distinct binary n-tuples satisfies the inequality**

$$h(p) \geq (1/n) \log_2 M$$

where $h(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$ is the binary entropy function. This inequality, which simplifies the derivation of the distance property of the Justesen codes, is proved using an elegant information-theoretic argument due to Kriz.

Let p be the fraction of the Mn positions in M distinct binary n-tuples which contain ones, and let p_i be the fraction of these n-tuples whose ith component is a one; then

$$p = \frac{p_1 + p_2 + \cdots + p_n}{n}.$$

We now derive an inequality relating p and n using an information-theoretic argument employed by Kriz [1] for a closely related problem.

Let $[x_1, x_2, \cdots, x_n]$ be a random n-tuple, which takes on each of the M given distinct n-tuple values with probability $1/M$. Then the uncertainty of this random n-tuple is

$$H(X_1 X_2 \cdots X_n) = \log_2 M.$$

As always the joint uncertainty of n letters is overbounded by the sum of their individual uncertainties, i.e.,

$$H(X_1 X_2 \cdots X_n) \leq H(X_1) + H(X_2) + \cdots + H(X_n)$$

and because of our probabilistic assignment

$$H(X_i) = h(p_i), \qquad 1 \leq i \leq n$$

where $h(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$. Combining these expressions, we have

$$h(p_1) + h(p_2) + \cdots + h(p_n) \geq \log_2 M$$

and also

$$h(p_1) + \cdots + h(p_n) = n\left[\frac{1}{n} h(p_1) + \cdots + \frac{1}{n} h(p_n)\right]$$
$$\leq nh\left(\frac{p_1 + p_2 + \cdots + p_n}{n}\right) = nh(p)$$

where we have exploited the convexity of h. We have thus proved the following theorem.

Theorem: The fraction p of ones in the Mn positions of M distinct binary n-tuples satisfies

$$h(p) \geq \frac{1}{n} \log_2 M.$$

It is interesting to note that the bound of this theorem is tight for a) $M = 1$, since $h(p) \geq 0$ implies $0 \leq p \leq 1$ and the values $p = 0$ and $p = 1$ are achievable, and for b) $M = 2^n$, since $h(p) \geq 1$ implies the unique solution $p = \frac{1}{2}$. Moreover, the bound is surprisingly tight in general. For instance, with $n = 20$ and $M = 2^{10} = 1024$, the bound gives $h(p) \geq \frac{1}{2}$, which implies $0.110 \leq p \leq 0.890$. The actual minimum and maximum achievable values of p for this case are 0.139 and 0.861, respectively.

The reader will recognize the theorem as a strengthening and simplification of the lemma of Justesen [2], which was the key inequality used in the derivation of the asymptotic distance bound for the Justesen codes.

References

[1] T. A. Kriz, "Some binary output sequence properties of deterministic autonomous finite-state machines," in *Proc. 6th Princeton Conf. Information Science and Systems*, Mar. 23–24, 1972, p. 442.
[2] J. Justesen, "A class of constructive asymptotically good algebraic codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 652–656, Sept. 1972.

Manuscript received March 16, 1973; revised July 5, 1973. This work was supported by NASA under Grant NGL-15-004-026 at the University of Notre Dame, Notre Dame, Ind., in liaison with the Communication and Navigation Division of the Goddard Space Flight Center.
The author is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, Ind. 46556.

On Binary Majority-Logic Decodable Codes

S. G. S. SHIVA AND S. E. TAVARES

***Abstract*—Let V' be a binary (n,k) majority-logic decodable code with $g'(X)$ as its generator polynomial and odd minimum distance d. Let V be the $(n, k - 1)$ subset code generated by $g'(X)(1 + X)$. This correspondence shows that V is majority-logic decodable with $d + 1$ orthogonal estimates. This fact is useful in the simultaneous correction of random errors and erasures.**

Manuscript received February 20, 1973; revised June 15, 1973.
S. G. S. Shiva is with the Electrical Engineering Department, University of Ottawa, Ottawa, Ont., Canada.
S. E. Tavares is with the Electrical Engineering Department, Queen's University, Kingston, Ont., Canada.