correction of the received digit must be done before the decoder is shifted to decode the next digit. Fig. 1 shows a decoder for the (11,6) shortened code derived from the (15,10) 2-step decodable code. The 2-flat polynomials listed in the figure are in the null space of the (15,10) code.

The salient differences between the full-length decoder and the shortened decoder are the following.

1) 1-step decoding is always possible, resulting in large hardware savings.

2) Error correction of the information digit currently being decoded is required before cyclically shifting the received codeword to decode the next digit.

The code may also be decoded by calculation of the syndromes and forming error estimates from the check sums expressed in terms of the syndromes [1, pp. 312 ff.] with the additional constraint that the effect of each error must be removed from the syndrome before the next digit is decoded.

Conclusions

A new class of 1-step majority logic decodable codes has been exhibited by shortening full-length multistep decodable geometric codes. The decoding is much simpler due to the 1-step property. An interesting problem is the analytic determination of the minimum-degree polynomials associated with r-flats.

References

[1] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd ed. Cambridge, Mass.: M.I.T. Press, 1972.

[2] R. L. Townsend and E. J. Weldon, Jr., "Self-orthogonal quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 183–195, Apr. 1967.

Comment on "A Class of Codes for Asymmetric Channels and a Problem from the Additive Theory of Numbers"

ROBERT J. McELIECE

In the above paper,[1] Varshamov considers discrete channels with q inputs and q outputs, q being an arbitrary integer. The inputs and outputs are labeled with the integers $\{0,1,\cdots,q-1\}$, and if the symbol i is transmitted, only the symbols $\{i, i+1,\cdots, q-1\}$ can be received. Thus if $x = (x_1,x_2,\cdots,x_n)$ is transmitted the received vector is of the form $(x_1+e_1,\cdots,x_n+e_n)$, where "+" denotes real addition, and $x_i + e_i \le q-1$ for all i. In this case Varshamov says that t errors have occurred, where

$$t = \sum_{i=1}^{n} e_i.$$

Notice that this definition differs from the usual Hamming error definition, if $q > 2$.

Varshamov then presents several constructions for t-error correcting codes for these channels. Since any code that corrects t Hamming errors will also correct t Varshamov errors, and since Varshamov did not provide estimates for the size of his codes, we thought it would be worthwhile to show that his codes really are superior to, for example, BCH codes.

Here is Varshamov's idea. Let (a_{ij}) be an $n \times m$ matrix of integers, and let $M_1,M_2,\cdots,M_m$ be positive integers. For each of the q^n vectors $x = (x_1,x_2,\cdots,x_n)$ of input symbols, define $V(x) = (V_1(x),V_2(x),\cdots,V_m(x))$, where $0 \le V_j(x) \le M_j - 1$ and

$$V_j(x) \equiv \sum_{i=1}^{n} x_i a_{ij} (\text{mod } M_j).$$

Then if x is transmitted and $y = x + e = (x_1+e_1,\cdots,x_n+e_n)$ is received, $V(y) = V(x) + V(e)$. Thus if it happens that distinct error patterns e with $\sum e_i \le t$ yield distinct vectors $V(e)$ (and of course this must be verified for the particular (a_{ij}) and M_j), *any* of the $M_1M_2\cdots M_m$ subsets of input vectors on which V is constant can be used as a code which correct t Varshamov errors. Now since there are q^n choices for x, at least one such code will contain at least $q^n/M_1M_2\cdots M_m$ codewords. Table I lists 4 constructions of this type given by Varshamov.

Now a t-error correcting BCH code of length $n = q^m - 1$ over $GF(q)$ has about $q^n/(n+1)^{t'}$ codewords, where $t' = \lceil 2t(q-1)/q \rceil$, and so we see that for fixed q and t, for large n, Varshamov's codes are superior to BCH codes if $q \ge 3$. For $q = 2$ his code 1 is superior to any possible single-symmetric error-correcting code, except when $n = 2^m - 1$ (when $n = 2^m - 1$ his construction yields exactly $2^n/(n+1)$ codewords) and for $q = 2$, $t = 2$, his code 2 is superior to the $t = 2$ BCH code, but is possibly inferior to the Preparata codes that have $2^{n+1}/(n+1)^2$ codewords.

We will conclude by sketching a proof that Varshamov's construction 4 really works. From the earlier remarks it will be sufficient to show that if $e = (e_1,e_2,\cdots,e_{p-1})$ is a vector of integers with $0 \le e_i \le p-1$ and $\sum e_i \le t$, that the e_i can be recovered from the sums

$$s_j = \sum_{i=1}^{p-1} e_i i^j, \qquad j = 1,2,\cdots,t.$$

The sums s_j, however, are merely the power-sum symmetric functions of the roots of

$$f(x) = \prod_{i=1}^{p-1} (x-i)^{e_i},$$

and so Newton's identities can be used to recover $f(x)$ and so also the e_i. A similar proof can be given for construction 3.

TABLE I

Code	t	n	m	a_{ij}	M_j	Lower Bound on Number of Codewords
1	1	arbitrary	1	i	$n+1$	$q^n/(n+1)$
2	2	prime-power	1	$b_i - b_0$ where $\{b_0,b_1,\cdots,b_n\} =$ $(n^2+n+1, n+1, 1)$ difference set	n^2+n+1	$q^n/(n^2+n+1)$
3	≥ 2	$p-2$, p prime	t	$a_{i1} = i$ $a_{ij} = g^{ij} - 1, j > 1$ $g =$ prim. root mod p	$M_1 = n+1$ $M_j = n+2, j > 1$	$q^n/(n+1)(n+2)^{t-1}$
4	arbitrary	$p-1$, p prime	t	i^j	$n+1$	$q^n/(n+1)^t$

Manuscript received July 27, 1972.
The author is with the Jet Propulsion Laboratory, Pasadena, Calif.

[1] R. R. Varshamov, "A class of codes for asymmetric channels and a problem from the additive theory of numbers," *IEEE Trans. Inform. Theory*, this issue, pp. 92–95.