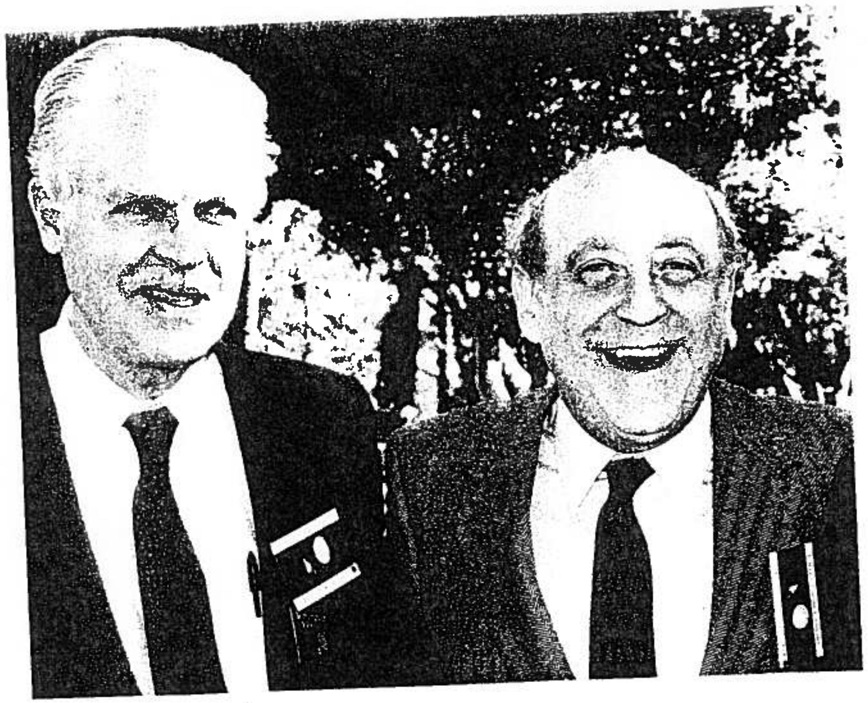

Irving S. Reed and Gustave Solomon

Reed-Solomon Codes and Their Applications

Edited by

Stephen B. Wicker
Georgia Institute of Technology

Vijay K. Bhargava
University of Victoria

IEEE PRESS

IEEE Communications Society and IEEE Information Theory Society, *Co-sponsors*

The Institute of Electrical and Electronics Engineers, Inc., New York

that at most four successive collisions can occur between two patterns, which alleviates the burden on the error control system as well. Further details of this construction can be found in [2].

2.10 Vajda's Construction

The use of a product code construction of hopping patterns has also been explored by Vajda [32] who took a cyclic product of two codes. The first code is obtained from $\mathcal{C}(N, t+1; 0)$ over GF(q), where N is a prime. As described in Section 2.5, q^t hopping patterns of period N can be obtained from this code. Let r denote the largest integer such that $N^{r-1} \leq q^t$. This code is a (nonlinear) cyclic code consisting of a set of N^{r-1} hopping patterns of period N and all their cyclic shifts. Note that the minimum distance of this nonlinear cyclic code is $N - t$. The other code is a coset of $\mathcal{C}(M, K-1; 2)$ over GF(N^r) that is a subcode of $\mathcal{C}(M, K+1; 0)$ over GF(N^r). Note that M is a divisor of $N^r - 1$. Thus, this code has $N^{r(K-1)}$ code words over an alphabet of size N^r, and since the code words belong to $\mathcal{C}(M, K+1; 0)$, the minimum distance between cyclic shifts of two code words is at least $M - K$. Vajda has proposed using the cyclic product of these codes instead of the direct product discussed in the previous subsection. Thus, each of the M N^r-valued symbols in a code word of the second code is replaced by a column vector of length N consisting of a code word of the first code. This creates an $N \times M$ matrix $\mathbf{Q} = Q_{i,j}$. Now, M and N are relatively prime, and hence the entries in $\mathbf{Q}$ can be read off in cyclic fashion to form a hopping pattern of length MN whose ith symbol is $Q_{i \bmod N,\, i \bmod M}$. Since the cyclic product of an (n_1, k_1, d_1) cyclic code with an (n_2, k_2, d_2) cyclic code is an $(n_1 n_2, k_1 k_2, d_1 d_2)$ cyclic code [13], this hopping pattern is actually a code word in an $[MN, (k+1)(K+1), (M-K)(N-t)]$ cyclic code over GF(q). There are $N^{r(K-1)}$ such hopping patterns, and it follows from (8) that, as shown in [32],

$$H_{\max} \leq MN - (M-K)(N-t) = Mt + KN - Kt.$$

As an example of this construction, let $q = 32$, $N = 31$, $t = 2$, $r = 3$, and $M = (31^3 - 1)/(31 - 1) = 993$. Let $K = 4$. Then, a set of $31^{3 \cdot 2} = 887,503,681$ hopping patterns of period $31 \cdot 993 = 30,783$ over GF(32) is obtained. The maximum Hamming correlation is 2102, so that there is, on the average, one hit every 14.64 symbols. In contrast, the Reed and Solomon sets of hopping patterns from $\mathcal{C}(31, 3; 0)$ over GF(32) provide 1024 hopping patterns of period 31 with a maximum Hamming correlation of 2, that is, one hit every 15.5 symbols, which is very slightly better.

2.11 Einarsson's Construction

Because of technological limitations on the frequency synthesizers used to produce the frequency-hopped signals, the hopping rate in a FH/SS system is limited to a few thousand dwells per second. In a fast FH/SS system, the transmission of a symbol occurs over several hops, and it is necessary to use M-ary signaling in order to achieve a reasonably large data rate. Einarsson [5] proposed a combined design of hopping patterns and M-ary modulation for use in such systems. In systems using this design, each transmitter is assigned a *collection* of M hopping patterns of length N and transmits one M-ary data symbol per N dwells by choosing and transmitting one of the hopping patterns. The data rate is thus $\log_2(M)/NT_h$ bits per second. Note, however, that the receiver is now more complicated since it must track all M possible hopping patterns in order to determine which one is being transmitted. Thus, M different frequency synthesizers might be needed in each receiver.

The Einarsson design uses all the nonzero code words in the Reed-Solomon code $\mathcal{C}(q-1, 2; 0)$. Each transmitter is assigned all the code words in a cyclic equivalence class. Thus, $M = N = q - 1$, and the hopping patterns assigned to jth transmitter are of the form

$$(\beta_j, \beta_j, \ldots, \beta_j) + \alpha^i (1, \alpha, \alpha^2, \ldots, \alpha^{q-2}), \ 0 \leq j \leq q-1.$$

Since all these sequences are from $\mathcal{C}(q-1, 2; 0)$, the number of hits between two patterns assigned to different transmitters is at most 1 regardless of the relative time delay between the two patterns. However, the number of hits per period can be guaranteed to be 1 only if the two transmitters are *frame-synchronous*. If the transmitters are only dwell-synchronous, then the tail end and the front end of *two possibly different* hopping patterns from an interfering transmitter can cause collisions,[3] and thus the number of hits per period can be two in some cases. There is also the question of the initial acquisition of synchronization in the receivers in such systems since the hopping patterns assigned to a transmitter are not cyclically inequivalent. In fact, the Hamming cross-correlation between two hopping patterns assigned to the same transmitter can have values as large as $N - 1$.

2.12 Other Constructions

There are several other constructions of frequency hopping patterns that are not directly related to Reed-Solomon codes except in certain special cases.

[3] A similar phenomenon in DS/SS systems gives rise to the *odd cross-correlation function* of binary sequences (cf. [23]).