The cross correlation of a_v with an offset of itself is studied by considering the polynomial $\alpha(1-\omega^k)x + \beta(1-\omega^{tk})x^t + \gamma(1-\omega^{sk})x^s$. We want to be certain that the reduction of the trace of previous polynomial is not identically zero. There is a number of procedures for limiting the choices of (α, β, γ) in order to do so, while insuring at the same time that $a_v(\alpha, \beta, \gamma)$ and $a_v(\alpha', \beta', \gamma')$ have small cross correlation for different choices. If case n is not divisible by 4, we may pick (α, β, γ) so that α and β are never simultaneously zero, and choose the γ's from distinct (additive) cosets of $G_{n/2}$ in GF(2^n), giving $2^{n/2}$ possibilities for γ. Altogether, not counting phase shifts as distinct gives $(2^{2n}-1)/(2^n-1)2^{n/2}$ coding sequences. Our control over the degree of the reduced trace polynomial gives all cross correlations, including the nontrivial autocorrelations, lying between $-\left(2^{(n+2)/2}+1\right)$ and $2^{(n+2)/2}-1$.

If case n is divisible by 4, it suffices, since s and t are relatively prime, to avoid $\alpha = \beta = 0$ and choose γ from distinct cosets, not including the zero coset of $G_{n/2}$ in GF(2^n). This gives $((2^{2n-1})/(2^n-1))(2^{n/2}-1)$ coding sequences. (A more careful choice gives $(2^{2n}-1)/(2^n-1)2^{n/2}$ coding sequences.)

The description we have given above can actually be materially simplified in practice, as follows. We are considering sequences such as $\mathrm{tr}(\gamma\omega^{sv})$. ω^{sv} always belongs to GF($2^{n/2}$) which has its own trace map tr. We claim that for each $\gamma \in$ GF(2^n) there is a $c \in$ GF($2^{n/2}$) such that $\mathrm{tr}(\gamma\omega^{sv}) = \mathrm{tr}(c\omega^{sv})$. This is an easy consequence of the following trivial observation.

As c ranges through GF($2^{n/2}$), tr(cx) ranges through all linear functionals on GF($2^{n/2}$) over GF(2), since it has the right dimension and cardinality. Thus, tr(γx) must be of form tr cx.

What all of this means in practice is quite simple. With the choices of γ as described earlier (distinct cosets of $G_{n/2}$ in GF(2^n)), the sequences $\mathrm{tr}(\gamma\omega^{tv})$ just run through the various phases of a single maximal sequence of length $2^{n/2}-1$, (and through the all zeros sequence if we pick the coset $G_{n/2}$ itself).

The merit of the general theoretical discussion that we gave lies only in the uniformity of treatment.

Finally, it is clear how this procedure generalizes to choice of an additional power of ω, the best being ω^r with $r = 2^{(n+4)/2}+1$, for purpose of controlling rank and cross correlation. Relative primality becomes a (minor) issue here, easily overcome by judicious choice of coefficients. In the case at hand, the gcd of 2^n-1 and $2^{(n+4)/2}+1$ is 3 if n is even but not divisible by 4; it is 5 if n is divisible by 8, and one in all other cases.

Detailed choices are left to the reader.

REFERENCES

[1] R. Gold "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619–621, Oct. 1967.

[2] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd-order binary Reed–Muller Codes," *Inform. Contr.*, vol. 18, pp. 369–394, May 1971.

[3] V.M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Doklady*, vol. 12, pp. 197–201, 1971.

Perfect (d,k)-Codes Capable of Correcting Single Peak-Shifts

V. I. Levenshtein and A. J. Han Vinck

***Abstract*—Codes, consisting of sequences $0^{\alpha_1}10^{\alpha_2}1\cdots0^{\alpha_N}1$, where $d \le \alpha_i \le k$, and call them (d,k)-codes of reduced length N are considered. We introduce a definition of arbitrary (d,k)- and perfect (d,k)-codes capable of correcting single peak-shifts of given size t. For the construction of perfect codes, a general combinatorial method connected with finding "good" weight sequences in Abelian groups is used, and the concept of perfect t-shift N-designs is introduced. Explicit constructions of such designs for $t=1$, $t=2$, and $t=(p-1)/2$ are given, where p is a prime. This construction is not only effective, but also universal in the sense that it does not depend on the (d,k)-constraints. It also allows to correct automatically those peak-shifts that violate (d,k)-constraints. Furthermore, our construction is naturally extended to (d,k)-codes of fixed binary length and allows the determination of the beginning of the next codeword. The question whether the designed codes can be represented as systematic codes with minimal redundancy is considered as well. In particular, for any (d,k)-code with n q-ary $(q=k-d+1\ge 2)$ information digits, a method of finding r q-ary check digits is given such that the resulting systematic code is capable of correcting single peak-shifts of size 1, where r is determined uniquely by $q^{r-1}-2(r-1) < 2n+1 \le q^r-2r$. This code is perfect if $2n+1=q^r-2r$.**

***Index Terms*—Peak-shift correction, (d,k)-codes, perfect (d,k)-codes**

I. INTRODUCTION

In high-density magnetic recording systems, runlength-limited (RLL) sequences are used to increase density and control self clocking [1]. The read-out mechanism detects changes in magnetization and thus from the RLL sequence we can derive a so called (d,k)-sequence, where $d+1$ and $k+1$ correspond to the minimum and maximum length of the RLL substrings, respectively. A (d,k)-sequence is represented by consecutive zero-symbol runs of length i, $d \le i \le k$, between pairs of one symbols. Read-out circuitry imperfection and clock jittering may cause misdetection of magnetization transitions and is supposed to result in peak-shifts left or right in the (d,k)-sequence.

Shamai and Zehavi [2] give bounds on the capacity of the bit-shift magnetic recording channel. Kolesnik and Krachkovski [3] obtained asymptotic bounds on the achievable rates of bit-shift, error-correcting codes. Fredrickson and Wolf [4] introduced a class of single bit-shift detecting codes. Codes designed specifically to cope with a single bit shift and multibit shifts of a single position are discussed by Kuznetsov and Vinck and by Ytrehus in [5], [6], respectively. Ferreira and Lin [7] give several code constructions based on the representation of constrained sequences as integer compositions. Abdel-Ghaffar and Weber [8] extends the results given in [4], [6]. We discuss the design of encoding and decoding for the multibit peak-shift channel.

In Section II, we give a definition of a multibit peak-shift and a general definition of a code capable of correcting single peak-shifts of size t. We concentrate on codes C consisting of (d,k)-sequences, and call them (d,k)-codes. For (d,k)-codes with k-$d \ge 2t$, we introduce the concept of a perfect code capable of correcting single peak-shifts

Manuscript received December 4, 1991.

V. I. Levenshtein is with the Keldysh Institute for Applied Mathematics of the Russian Academy of Sciences, Miusskaya sq. 4, 125047, Moscow, Russia.

A. J. Han Vinck is with the Institute for Experimental Mathematics, University of Essen, Ellernstrasse 29, 4300 Essen 12, Germany.

IEEE Log Number 9203977.

of size t. We remark that the problem of constructing maximum (d,k)-codes is reduced to the same problem for (d,k)-codes with a fixed number N of substrings.

In Section III, we give a universal and effective construction of (d,k)-codes capable of correcting single peak-shifts of size t. The construction is universal in the sense that it does not depend on the (d,k)-constraints and, in particular, allows to correct single peak-shifts of size t that disturb these constraints. The main idea of the construction consists of using a finite Abelian group G of order m to partition any code C into m subcodes, each having the desired error correcting properties [9]. Since at least one of these subcodes has size at least $|C|/m$, this construction is efficient if the order of the group G is sufficiently small. In the framework of this construction, we reduce the problem of finding perfect (d,k)-codes of reduced length N capable of correcting single peak-shifts of size t to the problem of finding "good" weight sequences in Abelian groups and introduce the concept of perfect t-shift N-designs.

In Section IV, we give explicit constructions of perfect t-shift n-designs for $t = 1$ and any N and for $t = (p-1)/2$, where p is a prime, and $N = (p^n - 1)/(p-1)$. Moreover, we find the necessary and sufficient conditions for the existence of perfect 2-shift N-designs.

In Section V, we consider the problem of finding the minimum redundancy r of systematic codes that are contained in the constructed perfect (d,k)-codes of reduced length N capable of correcting single peak-shifts of size t. This problem is connected with the existence of a particular ordering of perfect t-shift N-designs. We show that the lower bound $r \geq \lceil \log_q(2tN+1) \rceil$ is attained in some cases, where $\lceil x \rceil$ is the smallest integer at least x and $q = k - d + 1$. Furthermore, for any (d,k)-code with n q-ary information digits we give a method of finding the minimum number of q-ary check digits such that the resulting systematic (d,k)-code is capable of correcting single peak-shifts of size 1.

II. Definition of Codes Capable of Correcting Single Peak–Shifts of Given Size

Following [5], [10], we consider codes consisting of binary sequences of the following sort

$$\alpha := 0^{\alpha_1} 1\, 0^{\alpha_2} 1 \cdots 0^{\alpha_i} 1\, 0^{\alpha_{i+1}} 1 \cdots 0^{\alpha_N} 1. \tag{1}$$

We call N (number of substrings) the *reduced length* of the binary sequence $\boldsymbol{\alpha}$. The length of the sequence $\boldsymbol{\alpha}$ in the terms of binary digits is $L = \sum_{i=1}^{N} \alpha_i + N$.

Let d and k be nonnegative integers $0 \leq d \leq k$. The sequence (1) is called *d-sequence* if $d \leq \alpha_i, i = 1, 2, \cdots, N$. *$(d,k)$-sequence* if $d \leq \alpha_i \leq k, i = 1, 2, \cdots, N$. There is a natural one-to-one correspondence φ_d between d-sequences $\boldsymbol{\alpha}$ in (1) of reduced length N and the words

$$\begin{aligned} \varphi_d(\boldsymbol{\alpha}) &= (\alpha_1 - d, \alpha_2 - d, \cdots, \alpha_N - d), \\ &= (\beta_1, \beta_2, \cdots, \beta_N) \end{aligned} \tag{2}$$

of length N over the alphabet of nonnegative integers. In particular for $d = 0$, $\boldsymbol{\alpha}$ is a 0-sequence and

$$\varphi_0(\boldsymbol{\alpha}) = (\alpha_1, \alpha_2, \cdots, \alpha_N). \tag{3}$$

Note that in case of (d,k)-sequences $\varphi_d(\boldsymbol{\alpha})$ is a word over the alphabet $\{0, 1, \cdots, q-1\}$, where $q = k - d + 1$.

We say that the words

$$0^{\alpha_1} 1\, 0^{\alpha_2} 1 \cdots 0^{\alpha_i + j} 1\, 0^{\alpha_{i+1} - j} 1 \cdots 0^{\alpha_N} 1, \quad \text{where } \alpha_{i+1} \geq j \quad \text{and} \quad i = 1, 2, \cdots, N-1.$$

$$0^{\alpha_1} 1\, 0^{\alpha_2} 1 \cdots 0^{\alpha_{i-1}} 1\, 0^{\alpha_i + j} 1, \quad \text{where } i = N.$$

are *obtained from (1) by a shift of the ith peak to the right in j digits,* and say that the words

$$0^{\alpha_1} 1\, 0^{\alpha_2} 1 \cdots 0^{\alpha_i - j} 1\, 0^{\alpha_{i+1} + j} 1 \cdots 0^{\alpha_N} 1, \quad \text{where } \alpha_i \geq j \quad \text{and} \quad i = 1, 2, \cdots, N-1.$$

$$0^{\alpha_1} 1\, 0^{\alpha_2} 1 \cdots 0^{\alpha_{i-1}} 1\, 0^{\alpha_i - j} 1, \quad \text{where } \alpha_i \geq j \quad \text{and} \quad i = N.$$

are *obtained from (1) by a shift of the ith peak to the left in j digits.*

The important consequence of the previous definition of a peak-shift is that for multibit peak-shifts phrases are *neither destroyed nor generated* by peak-shifts, and thus

1) the reduced length N does not change;
2) the overall binary length of a sequence $\boldsymbol{\alpha}$ given by $L = \sum_{i=1}^{N} \alpha_i + N$ changes only when the length of the Nth substring changes.

Definition: A code C consisting of sequences (1) of reduced length N (or/and binary length L) is called *a code capable of correcting single peak-shifts of size t,* if it is possible to determine uniquely a codeword from any word that can be obtained from it by a shift of a peak to the left or to the right in at most t digits.

Definition: A code C consisting of sequences (1) of reduced length N (or/and binary length L) and capable of correcting single peak-shifts of size t is called *maximum* if it contains the greatest number of words among codes with the same property.

We concentrate on codes C consisting of (d,k)-sequences, and call them *(d,k)-codes.* In the next section, we give a universal and effective construction of (d,k)-codes of reduced length N capable of correcting single peak-shifts of size t. The construction is universal in the sense that it does not depend on (d,k)-constraints and, in particular, allows to correct single peak-shifts of size t which disturb these constraints. On the other hand, the construction is effective to the extent that any (d,k)-sequence (1) transformed into another (d,k)-sequence by any single peak-shift of size t can be obtained from one (and only one) codeword by a single peak-shift of size at most t.

In this connection we introduce the following definition.

Definition: A (d,k)-code C of reduced length N capable of correcting single peak-shifts of size t is called *perfect* if $k-d \geq 2t$ and any $(d+t, k-t)$-sequence of reduced length N can be obtained from one (and only one) codeword by a single peak-shift of size at most t.

This definition is a natural analog of the classical definition for error-correcting codes although there are essential distinctions. In the classical case, any word of Hamming space can be obtained by permissible errors from one (and only one) word of a perfect code. In our case it is valid in general only for the subset of $(d+t, k-t)$-sequences of the set of (d,k)-sequences under consideration. However, it should be noted that any (d,k)-sequence that is not a $(d+t, k-t)$-sequence can already be obtained by permissible errors from a sequence that is not (d,k). The second distinction is connected with the definition of a maximum code. If in Hamming space every perfect code is maximum, in our case (as well as in case of perfect codes capable of correcting single deletions [11]) perfect codes can have different sizes. However, it will be shown later that among them always exist perfect codes whose sizes are very close to maximum.

Remark 1: From the previously stated definitions, it immediately follows that a (d,k)-code of binary length L capable of correcting single peak-shifts of size t is maximum, if and only if it is a union of similar maximum (d,k)-codes consisting of words (1) of binary length L and reduced length N for all N. $L/(k+1) \leq N \leq L/(d+1)$. However, the length L of transmitted codewords can be changed in virtue of a shift of the last peak, and a question arises whether the decoder can determine uniquely the position of this peak in the received message. Now, we verify that for some

natural assumptions it is possible without using merging digits. Considering (d,k)-codes, we can assume that the permissible size t of shifts does not exceed d and that any two neighbor peaks cannot shift simultaneously (really we use a stronger similar assumption concerning all peaks of a codeword). Then the decoder can determine the last peak of a transmitted codeword of length L as a peak that is closest to the Lth position. Indeed, if the last peak did not shift, it takes the Lth position in the received message. If the last peak shifted to the left or to the right in at most t positions, both neighbor peaks did not shift and are situated at distance at least $d+1>t$ from the Lth position of the received message. Thus, the decoder can determine the last peak of the transmitted codeword and hence its reduced length without using merging digits.

This remark allows us to concentrate on (d,k)-codes of a fixed reduced length N. However, in Table I we present the sizes and efficiencies of some (d,k)-codes of binary length L capable of correcting single peak-shifts constructed by our method.

III. A Combinatorial Problem Connected with the Correction of Single Peak-Shifts of Given Size

For constructing codes capable of correcting peak-shifts, we use a general combinatorial method that was suggested in [9]. The main idea of this construction consists of using a finite Abelian group G of order m to partition any code C into m subcodes, each having the desired error correcting properties. Since at least one of these subcodes has size at least $|C|/m$, this construction is efficient if the order m of the group G is sufficiently small.

Let G be a finite (additive) Abelian group of order $m=|G|$ and $W:=\{w_1,w_2,\cdots,w_N\}$ be a sequence of not necessarily different elements of G. We refer to W as *weight sequence*. For any code C, consisting of sequences $\boldsymbol{\alpha}$ in (1), and any element $g\epsilon G$ we define the subcode

$$C(W,g):=\Big\{\boldsymbol{\alpha}\epsilon C:\sum_{i=1}^{N}\alpha_i w_i=g,\quad \text{where } (\alpha_1,\alpha_2,\cdots,\alpha_N)=\varphi_0(\boldsymbol{\alpha})\Big\}. \tag{4}$$

Here, $\alpha_i w_i$ denotes the sum of α_i elements w_i of the Abelian group G. The problems are to find necessary and sufficient conditions on a sequence $W=\{w_1,w_2,\cdots,w_N\}$ for which every of $m=|G|$ subcodes $C(W,g)$ of a code C is capable of correcting single peak-shifs of given size t, and to find the minimal order m of the group G in which the suitable sequence W exists.

Notice that for a code C, consisting of d-sequences (1), we can determine (see (2)) subcodes

$$C_d(W,g)=\Big\{\boldsymbol{\alpha}\epsilon C,\sum_{i=1}^{N}\beta_i w_i=g,\quad \text{where } (\beta_1,\beta_2,\cdots,\beta_N)=\varphi_d(\boldsymbol{\alpha})\Big\}.$$

It is easy to see that this is the same class of subcodes as given in (4) since

$$C_d(W,g)=C\left(W,g+d\sum_{i=1}^{N}w_i\right).$$

The following definition and Theorem 1 are the basis for the codes to be designed.

Definition: A set $H:=\{h_1,h_2,\cdots,h_N\}\subset G$ is called a *t-shift N-design in G* if for any $j=1,\cdots,t$ and any $i=1,\cdots,N$ all $2Nt$ elements $\pm j h_i$ are different and not equal to zero.

The values $\pm j\,h_i$ are considered to be the syndromes that result after a peak-shift in a codeword.

We fix some weight sequence $W=\{w_1,w_2,\cdots,w_N\}$ of elements of G.

Theorem 1: For any code C, consisting of sequences $\boldsymbol{\alpha}$ in (1), any subcode $C(W,g)$ as defined in (4), is capable of correcting single peak-shifts of given size t, if and only if the set $H:=\{h_1,h_2,\cdots,h_N\}$ of G, where

$$h_i=w_i-w_{i+1},\qquad i=1,\cdots,N-1,\qquad h_N=w_N, \tag{5}$$

is a t-shift N-design in G.

Proof: Sufficiency follows from the fact that for a sequence $\gamma=0^{\gamma_1}10^{\gamma_2}1\cdots0^{\gamma_N}1$, obtained from a codeword $\boldsymbol{\alpha}$ by a shift of the ith peak to the right (or left) in j digits, the difference $\sum_{i=1}^{N}\gamma_i w_i-\sum_{i=1}^{N}\alpha_i w_i$ is equal to $\pm j(w_i-w_{i+1})$ if $i=1,2,\cdots,N-1$ or to $\pm j w_i$ if $i=N$. The $+$ sign corresponds to a right shift. On the other hand, if H is not a t-shift N-design in G, for any d-sequence $\boldsymbol{\alpha}$ in (1), where $d\geq t$, there exist two different single peak-shifts of size at most t giving rise to the same syndrome. Then these peak-shifts transform $\boldsymbol{\alpha}$ in two different sequences of reduced length N, which belong to the same subcode $C(W,g)$ and, hence, this subcode cannot be capable of correcting peak-shifts of size t

It is significant to note that (5) gives a one-to-one correspondence between $W=\{w_1,w_2,\cdots,w_N\}$ and $H=\{h_1,h_2,\cdots,h_N\}$. W is uniquely determined for any ordering of the t-shift N-design $H=\{h_1,h_2,\cdots,h_N\}$ by

$$w_i=\sum_{j=i}^{N}h_j,\qquad i=1,2,\cdots,N, \tag{6}$$

and will be denoted as $W(H)$. By Theorem 1, for any code C, consisting of sequences (1), any subcode $C(W(H),g)$, $g\epsilon G$, is capable of correcting single peak-shifts of size t. If we change the ordering of H, we change $W(H)$. In Section V, we use a special ordering of the t-shift N-design H in order to choose a particular weight sequence $W(H)$ and decrease the redundancy of (d,k)-codes capable of correcting single peak-shifts. □

Later, we will see that for any t and N there exists a t-shift N-design in an Abelian group of sufficient small order. Let $m(N,t)$ denote the minimum order of the Abelian group G in which there exists a t-shift N-design. According to the definition for such a design $m(N,t)\geq 2N+1$. Therefore, a t-shift N-design in G is called *minimum* if $|G|=m(N,t)$ and *perfect* if $|G|=2tN+1$. Using this, we have the following.

Corollary 1: For any code C consisting of sequences (1) of reduced length N there exists a subset of C which is a code capable of correcting single peak-shifts of given size t and has cardinality at least $|C|/m(N,t)$, where $|C|$ is the cardinality of the code C.

The cardinality $|C|$ of $C=C_{d,k}^{N}$ consisting of all (d,k)-sequences of reduced length N is $|C|=(k-d+1)^N$. The average length $\overline{L}$ per code symbol is $(k+d+2)/2$, and hence, the number of information bits represented by a codeword divided by $N\overline{L}$ is

$$\frac{\log_2|C|}{N\overline{L}}=\frac{2}{k+d+2}\log_2(k-d+1), \tag{7}$$

which is equal to the lower bound to the capacity $C(d,k)$ of (d,k)-sequences as given by Zehavi and Wolf [10]

$$(C(d,k)=\lim_{L\to\infty}\frac{\log A(d,k,L)}{L},$$

where $A(d,k,L)$ is the number of (d,k)-sequences (1) of binary length L). The maximum information rate $C(d,k)$ is given as the base-two logarithm of the largest real root of the equation

$$1+Z^{k+2}-Z^{k+1}-Z^{k+1-d}=0.$$

In general, an exact expression for the capacity is hard to give. However, in [10] it is shown that the capacity $C(d,k)$ is bounded by

$$\frac{2\log_2(k-d+1)}{(k+1)+(d+1)} \le C(d,k) \le \frac{\log_2(k-d+1)}{d+1}.$$

Theorem 2: Let the code $C = C_{d,k}^{N}$ consist of all (d,k)-sequences of reduced length N, let $k-d \ge 2t$, and let there exist a perfect t-shift N-design H. Then, any code $C(W(H),g)$, see (4), is a perfect (d,k)-code capable of correcting single peak-shifts of size t and at least one of them has size at least $q^N/(2Nt+1)$, where $q = k-d+1$.

Proof: Let $\boldsymbol{\alpha}$ be any $(d+t,k-t)$ sequence $\varphi_o(\boldsymbol{\alpha}) = (\alpha_1,\alpha_2,\cdots,\alpha_N)$. $H = \{h_1,h_2,\cdots,h_N\}$ and $W(H) = \{w_1,w_2,\cdots,w_N\}$. Since H is a perfect t-shift N-design then for any g, $\sum_{i=1}^{N}\alpha_i w_i - g$ is equal to 0 or to some element $\pm jh_i$, where $j = 1,\cdots,t$, $i = 1,2,\cdots,N$. Realizing in the word $\boldsymbol{\alpha}$ a corresponding shift in j digits to left or to right we obtain a (d,k)-sequence which belongs to the code $C(W(H),g)$.

Thus, the problem of constructing perfect (d,k)-codes of reduced length N capable of correcting single peak-shifts of size t is reduced in the framework of the method under consideration to the problem of finding perfect t-shift N-designs. □

IV. Construction of Perfect t-Shift N-Designs and Codes Capable of Correcting Single Peak-Shifts

In Section III, we reduced the problem of constructing codes or reduced length N capable of correcting single peak-shifts of given size t to the combinatorial problem of finding t-shift N-designs H in an Abelian group G. Corollary 1 and Theorem 2 shows that the construction is the most efficient when H is a perfect t-shift N-design, that is G has order $2tN+1$. In this section, we give constructions for perfect t-shift N-designs for $t = 1$, $t = 2$, and $t = (p-1)/2$, where p is prime.

Let G_m be the group of integers modulo m and F_p^r be (the additive group of) the r-dimensional vector space over $GF(p)$, where p is a prime.

First, notice that any nonzero element g of an Abelian group G of odd order differs from its opposite element $-g$. Hence, the set of all nonzero elements of the Abelian group of order $2N+1$, is partitioned into N pairs of opposite elements $\{+g,-g\}$. Choosing any element from each such pair we obtain a perfect 1-shift N-design, that gives the following.

Theorem 3: A perfect 1-shift N-design exists in any Abelian group of order $2N+1$, and hence, $m(N,1) = 2N+1$.

In particular, the set of integers $H = \{1,2,\cdots,N\}$ forms a perfect 1-shift N-design in G_{2N+1}. The corresponding weight sequence $W(H)$ is defined by (6).

Example: For $N = 7$, $W(H) = \{w_1,w_2,w_3,w_4,w_5,w_6,w_7\} = \{13,12,10,7,3,13,7\}$. The values $\pm i$, $i = 1,2,\cdots,N$ of changes determine the position of the erroneous peak and the direction of the shift.

We show how it is possible to use Remark 1 and Theorem 3 for constructing effective (d,k)-codes of binary length L capable of correcting single peak-shifts (of size 1). For any fixed N, $L/(k+1) \le N \le L/(d+1)$, we consider the code C consisting of all (d,k)-sequences of binary length L and reduced length N and use the perfect 1-shift N-design H of Theorem 3 to choose by Theorem 1 the largest subcode $C(W(H),g)$. By Corollary 1, it contains at least $1/(2N+1)$ of all words of C. A union of these codes of all given above lengths N gives rise (see Remark 1) to a code consisting of some number $V(d,k,L)$ of (d,k)-sequences with binary length L and being capable of correcting single peak-shifts. In Table I, for $L = 16$ and $L = 24$, we present sizes $V(d,k,L)$ and efficiencies

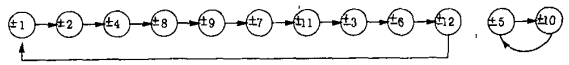
$$R(d,k,L) = \frac{\log V(d,k,L)}{L}$$

of obtainable codes in comparison with analogue values for the set of all (d,k)-sequences of binary length L.

TABLE I
Efficiencies for Several (d,k)-Codes of Fixed Binary Length $L = 16$ and 24

(d,k)	(1,3)	(1,5)	(1,7)	(2,5)	(3,7)
$A(d,k,16)$	165	431	551	41	17
$A(d,k,24)$	3505	15911	23830	557	157
$C(d,k)$	0.55	0.65	0.68	0.46	0.40
$V(d,k,16)$	11	39	52	4	3
$R(d,k,16)$	0.22	0.33	0.37	0.13	0.10
$V(d,k,24)$	185	976	1561	44	15
$R(d,k,24)$	0.31	0.41	0.43	0.23	0.16

In the case $t = 2$, for any Abelian group G of order $4N+1$, we consider the directed graph $\Gamma(G)$ with as vertices the $2N$ pairs of opposite elements $\{+g,-g\}$. From vertex $\{+g,-g\}$ there exists a directed edge to vertex $\{+h,-h\}$, if and only if $h = 2g$ or $h = -2g$. For any element h in an Abelian group G of odd order there exists a unique element $g \epsilon G$ such that $h = 2g$. Therefore, in $\Gamma(G)$, only one edge begins at each vertex and only one edge leads to each vertex. Hence, the graph $\Gamma(G)$ is partitioned into directed cycles. From the construction of $\Gamma(G)$, it follows that a perfect 2-shift N-design in G exists, if and only if we can choose N pairwise nonadjacent vertices among the $2N$ vertices of $\Gamma(G)$. It follows that a perfect 2-shift N-design in G exists, if and only if the graph $\Gamma(G)$ consists of only even cycles. As an example for groups G of order 25, the graph $\Gamma(G_{25})$ has only two cycles



consisting of 10 and 2 vertices, and the set $\{1,4,9,11,6,5\}$ forms a 2-shift 6-design in G_{25}. In the same way, the graph $\Gamma(F_5^2)$ is partitioned into 6 cycles of length 2. We now show that the condition that the graph $\Gamma(G)$ is partitioned into only even directed cycles is equivalent to the following arithmetical condition:

$$\left(2^{4\ell+2}-1,4N+1\right) = 1. \qquad \text{for any } \ell = 0,1,\cdots,N-1. \quad (8)$$

Let the vertex $\{g,-g\}$ of $\Gamma(G)$ belong to a cycle of length $2\ell+1$, $\ell = 0,1,\cdots,N-1$. Then $\left(2^{2\ell+1}+1\right)g = 0$ or $\left(2^{2\ell+1}-1\right)g = 0$ and $\ell \ne 0$, and thus the order of g is a common divisor of $2^{4\ell+2}-1$ and $4N+1$. On the other hand, if ℓ is the minimum number for which (8) is not fulfilled and a prime p is a common divisor of $2^{4\ell+1}-1$ and $4N+1$ then in G there exists an element g of order p and hence $\left(2^{2\ell+1}+1\right)g = 0$ of $\left(2^{2\ell+1}-1\right)g = 0$. Using the minimality of the number ℓ, it is easy to show that the length of a cycle that goes through vertex $\{+g,-g\}$ is equal to $2\ell+1$. As a consequence we have the following.

Theorem 4: A perfect 2-shift N-design in an Abelian group G of order $4N+1$ exists, if an only if the graph $\Gamma(G)$ consists of only even cycles or equivalently, if and only if (8) is fulfilled.

The first criterion of existence of a perfect 2-shift N-design is a convenient check for the computer and for explicit constructions in case a perfect 2-shift N-design exists. The second criterion shows that the question of existence of a perfect 2-shift N-design depends only on the number theoretical nature of the order of the group,

but not its structure. Using that $2^{p-1} - 1 \equiv 0 \pmod{p}$ note that for any $p = 4n + 3$, $2^{p-1} - 1 = 4^{2n+1} - 1 \equiv 0 (\text{mod } p)$, 4 has an odd (multiplicative) order (mod p), and if $p = 4n + 3$ is a divisor of $4N + 1$, then (8) is not satisfied. If $p = 4n + 1$ is a divisor of $4N + 1$ and 4 has some odd order $2\ell + 1$ (mod p), then $2^{4n} - 1 = 4^{2n} - 1 \equiv 0 \pmod{p}$, $2\ell + 1 \leq n \leq N$, and the condition (8) is not satisfied as well. On the other hand, if (8) is not satisfied and a prime p is a common divisor of $2^{4\ell+2} - 1$ and $4N + 1$ for some $\ell = 0, 1, \cdots, N - 1$, then $4^{2\ell+1} - 1 \equiv 0 \pmod{p}$, and hence, 4 has an odd order (mod p). Therefore, we have the following.

Corollary 2: A perfect 2-shift N-design in any Abelian group G exists, if and only if the factorization of $4N + 1$ contains only primes p (of the type $4n + 1$) such that 4 has an even order (mod p).

The corollary allows us to quickly check the condition whether a perfect 2-shift N-design exists or not. The following numbers $4N + 1$, $1 \leq N \leq 25$, satisfy the condition of Theorem 4 and corollary 2: 5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 85, 97, 101. On the other hand, it is interesting to mention that for $n \leq 250$, the only primes of the type $4n + 1$, such that 4 has an odd order (mod p), are 73, 89, 233, 281, 337, 601, 617, 881, and 937.

If a perfect 2-shift N-designs does not exist we suggest another construction of 2-shift N-designs that are minimum.

Theorem 5: The set of integers $H := \{h_i = 2i-1, i = 1, \cdots, N\}$ forms a 2-shift N-design in G_{4N+2}.

Proof: It is sufficient to check that the congruences $h_i - h_j \equiv 0, 2(h_j - h_j) \equiv 0 \text{ mod}(4N + 2)$ hold only for $i = j$ and the congruences $h_i + h_j \equiv 0, 2(h_i + h_j) \equiv 0$, $h_i + 2h_j \equiv 0$, $h_i - 2h_j \equiv 0 \text{ mod}(4N + 2)$ do not hold for any i and j, $1 \leq i, j \leq N$. □

Corollary 3: $4N + 1 \leq m(N, 2) \leq 4N + 2$.

We now give a general construction for the specific case where $t = (p - 1)/2$, and p is a prime. It is known that in the r-dimensional vector space F_p^r there exist $(p^r - 1)/(p - 1)$ one-dimensional subspaces and $(p^r - 1)/(p - 1)$ projective vectors the first nonzero coordinates of which are equal to 1 which generate these one-dimensional subspaces. We denote the set of these vectors by H_p^r.

Theorem 6: Let $t = (p - 1)/2$, where p is a prime, and $N = (p^r - 1)/(p - 1)$, then H_p^r forms a perfect t-shift N-design in F_p^r and hence, $m(N, t) = 2tN + 1$.

Proof: First remark that $2tN + 1 = p^r$. The proof follows from the fact that the numbers $^{\pm}t, t \leq (p - 1)/2$ give different elements from GF(p) and thus different scalar products with any vector from H_p^r. Furthermore, one-dimensional subspaces, generated by any two vectors from H_p^r have only zero vector as intersection. □

Note that for the conditions of Theorem 6, a perfect t-shift N-design exists in G_{p^r} as well. It can be obtained if every projective vector $(c_1, c_2, \cdots, c_r) \epsilon H_p^r$ is replaced by the number $c_1 + c_2 p + \cdots + c_r p^{r-1}$ (but not the number $c_1 p^{r-1} + c_2 p^{r-2} + \cdots + c_r$).

Example: Let $t = 3$, $p = 7$, $r = 2$ and $N = 8$. The perfect 3-shift 8-design H_7^2 in F_p^2 consists of eight vectors: (1,0), (1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (0,1) and the weight sequence

$$W(H_7^2) = \{(0,1), (6,1), (5,0), (4,5), (3,2), (2,5), (1,0), (0,1)\}.$$

The corresponding set $H = \{1, 8, 15, 22, 29, 36, 43, 7\}$ forms a perfect 3-shift 8-design in G_{49}.

Notice that if $t \leq (p - 1)/2$, p is a prime and $(p^{r-1} - 1)/(p - 1) < N \leq (p^r - 1)/(p - 1)$, then any N vectors of H_p^r form a t-shift N-design in F_p^r. Since $|F_p^r| = p^r$ and $p^{r-1} \leq N(p - 1)$ then $m(N, t) \leq p(p - 1)N$. By the Chebyshev inequality, there exists a prime p such that $2t + 1 \leq p < 4t$. It follows that in any case the value $m(N, t)$ does not exceed $16t^2N$.

This perfect t-shift N-designs H can be used in Theorem 2 to construct perfect (d, k)-codes $C(W(H), g)$ capable of correcting single peak-shifts of size t. At this point we want to consider other properties of the weight sequence $W = \{w_1, w_2, \cdots, w_N\}$ connected with correction of errors of different sorts. Following [9], we say that W has property A_s, B_s, C_s if under the conditions a) k_i and ℓ_i are $-1, 0, +1$ such that $\sum_{i=1}^N |k_i| \leq s, \sum_{i=1}^N |\ell_i| \leq s$, b) k_i and ℓ_i are 0 or 1 such that $\sum_{i=1}^N k_i \leq s \sum_{i=1}^N \ell_i \leq s$,c) k_i and ℓ_i are nonnegative integers such that $\sum_{i=1}^N k_i \leq s, \sum_{i=1}^N \ell_i \leq s$, respectively, the equality $\sum_{i=1}^N k_i w_i = \sum_{i=1}^N \ell_i w_i$ holds in G only if $k_i = \ell_i$ (modulo 2, in the case A_s), $i = 1, \cdots, N$. It is easy to show that for any binary code C of length N and any sequence W with property A_s or B_s, all subcodes $C(W, g)$ are capable of correcting at most s usual ($0 \to 1$ and $1 \to 0$) or asymmetrical ($0 \to 1$) errors, respectively. Furthermore, for any code C consisting of sequences (1), and for any sequence W, having the property C_s, all subcodes $C(W, g)$ are capable of correcting at most s deletions of zeros. The order of a group G in which there exists a sequence W with property A_s, B_s, C_s is at least $\sum_{i=0}^S C_N^i, \sum_{i=0}^S C_N^i$, and $\sum_{i=0}^S C_{i+N-1}^i$, respectively; if this order is attained, we call the corresponding W perfect. In the first case it is possible only if any element g has order 2 and hence $G = F_2^r$ and $\sum_{i=0}^S C_N^i = 2^r$. For $s = 1$, all nonzero elements of G form a perfect W that gives the perfect single-error-correcting Hamming codes, the single asymmetric-error correcting Varshamov–Tenengolz codes [12] and the perfect single asymmetric-deletion correcting codes, constructed in [9]. It is known that there does not exist another perfect W, having property A_s except for $s = 3, N = 23, r = 11$ (Golay code) and the trivial cases $2s+1 = N$, $r = N-1$. There is a natural generalization of the properties A_s and B_s for the q-ary case. Notice also that any q-ary code of length N, with t-shift N-designs as weight sequences, is nothing else than a code capable of correcting a single usual error of size $^{\pm}i, i \leq t$.

These examples and the examples of weight sequences $W(H)$ from the perfect t-shift N-designs show that the general combinatorial approach under consideration is universal and fruitful.

V. Minimum Redundancy of (d, k)-Codes Capable of Correcting Single Peak-Shifts of Given Size

We can use the constructions of perfect t-shifts N-designs H and Theorem 2 in order to partition any (d, k)-code C of reduced length N into $2tN + 1$ codes $C(W(H), g)$, each capable of correcting single peak-shifts of size t. In this section, we consider the problem of dividing N q-ary symbols of (d, k)-codes $C(W(H), g)$ into information and check symbols, where $q = k - d + 1$.

A code C of length N over the alphabet $\{0, 1, \cdots, q - 1\}$ is called *systematic* if it is possible to partition all its digits into two parts of n ($n \geq 1$) and r ($N = n + r$) digits such that for any filling of the n digits (called *information digits*), there exists a unique filling of the remaining r digits (called *check digits*) leading to a valid codeword. It is evident that a systematic code contains exactly q^n words. The number r is called the *redundancy* of the code C of length N.

Next, we consider the problem of finding the minimum redundancy r such that for any code $C(W(H), g)$, where $C = C_{d,k}^N$ is a code from all q^N (d, k)-sequences of reduced length N and H is a perfect t-shift N-design, there exists a systematic subcode of redundancy r. Since the size of such a subcode is equal to q^{N-r} and the number of these disjoint subcodes is equal to $2tN + 1$, then $(2tN + 1)q^{N-r} \leq q^N$ and hence

$$r \geq \lceil \log_q (2tN + 1) \rceil,$$

where $\lceil x \rceil$ is the smallest integer at least x. To prove that this bound is attained, it is sufficient to show that, if

$$q^{r-1} < 2tN + 1 \leq q^r, \tag{9}$$

there exists a particular ordering of a perfect t-shift N-design in the group G_{2tN+1} such that the weight sequence $W(H)$ contains the weights $1, q, \cdots, q^{r-1}$. We find such an ordering for $t = 1$ and any $q \geq 2$.

Theorem 7: Let $C = C_{d,k}^N$ be the code consisting of all (d, k)-sequences of reduced length N, $q = k - d + 1$ and $N \geq 3$ of $q \geq 3$, $N \geq 5$ if $q \geq 2$. Then, there exists a perfect 1-shift N-design H in G_{2N+1} such that any (d, k)-code $C(W(H), g)$, $g \epsilon G_{2N+1}$ (by Theorem 1 capable of correcting peak-shifts of size 1) contains a systematic subcode of redundancy

$$r = \lceil \log_q (2N + 1) \rceil. \tag{10}$$

Moreover, if $\log_q (2N + 1)$ is an integer, every code $C(W(H), g)$ is a perfect systematic code capable of correcting peak-shifts of size 1 and has redundancy $r = \log_q (2N + 1)$.

Proof: Define the number r from the inequalities (9) and consider the sequence of r numbers

$$q^{r-2}(q-1), q^{r-3}(q-1), \cdots, q(q-1), q-1, 1. \tag{11}$$

For $q \geq 3$, these numbers decrease and, hence, are different in G_{2N+1}. For $0 \leq i \leq r-2$ and $r \geq 2$ any number $q^i(q-1)$ is not opposite to 1 since $q^i(q-1) + 1 \leq q^{r-1}$, and for $0 \leq i < j \leq r-2$ and $r \geq 3$, any pair of numbers $q^i(q-1)$ and $q^j(q-1)$ are not opposite to each other, since $q^i(q-1) + q^j(q-1) \leq (q^{r-2} + q^{r-3})(q-1) < q^{r-1}$. Hence, for $q \geq 3$, the sequence (11) consists of different elements of G_{2N+1}, not opposite to each other. From (9), we know that $r < N$ for $N \geq 3$ and $q \geq 3$ and thus we can add $N - r$ elements of G_{2N+1} to construct an ordered perfect 1-shift N-design H, in which the last elements form the sequence (11). The corresponding weight sequence $W(H)$ ends with the weights $q^{r-1}, q^{r-2}, \cdots, q, 1$, and the Theorem is proved for $q \geq 3$. For $q = 2$ and the condition that $N \geq 5$, it follows that $r \geq 4$. In this case, we consider the sequence of r numbers

$$2^{r-2}, 2^{r-2}, \cdots, 2^2, 3, -1, 2. \tag{12}$$

By analogy, it is easy to show that the sequence (12) consists of different elements of G_{2N+1}, any two of them are not opposite to each other, and construct a perfect 1-shift N-design H. The corresponding weight sequence $W(H)$ ends with the weights $2^{r-1}, 2^{r-2}, \cdots, 2^2, 1, 2$, which proves the Theorem for $q = 2$. □

Example: Let $d = 1, k = 3, t = 1, N = 10$. Then, $q = 3$ and $2N + 1 = q^r - 2r$ for $r = 3$. Using (11), we find the perfect 1-shift 10-design $H = \{3, 4, 5, 7, 8, 9, 10, 6, 2, 1\}$ and the weight sequence $W(H) = \{13, 10, 6, 1, 15, 7, 19, 9, 3, 1\}$. For $C = C_{1,3}^{10}$ any (1,3)-code $C(W(H), g)$ $g \epsilon G_{21}$, is a perfect systematic code of reduced length 10 and of redundancy 3 capable of correcting peak-shifts of size 1.

The ordering of a perfect 1-shift N-design in G_{2N+1} given in Theorem 7 allows us to give a solution to the following problem. What is the minimum amount of q-ary check digits needed to add to a code $C_{d,k}^n$ of reduced length n such that the resulting (d, k)-code is capable of correcting single peak-shifts of size1? From Theorem 7, it follows that it is sufficient to add r digits, where r is the minimum number such that

$$2(n + r) + 1 \leq q^r. \tag{13}$$

TABLE II
MINIMUM REDUNDANCY r OF SYSTEMATIC (d, k)-CODES WITH n INFORMATION q-ARY DIGITS CAPABLE OF CORRECTING PEAK-SHIFTS OF SIZE 1 $(q = k - d + 1)$

n	$q =$	2	3	4	5	6	7
2		4	2*	2	2	2	1*
3		4	3	2	2	2	2
4–5		5	3	2	2	2	2
6–9		5	3	3	2	2	2
10		5	3*	3	2*	2	2
11–15		6	4	3	3	2	2
16–21		6	4	3	3	3	2
22		6	4	3	3	3	2*
23–25		6	4	3	3	3	3

TABLE III
A PARTICULAR ORDERING OF THE PERFECT 2-SHIFT N-DESIGN H IN G_{4N+1} AND $W(H)$ FOR $q = 5$

m	N	H	W
13	3	{3,4,1}	{8, 5, 1}
17	4	{5,3,4,1}	{$\cdots$, 5, 1}
25	6	{5,6,9,11,4,1}	{$\cdots$, 5, 1}
29	7	{6,7,5,16,20,4,1}	{$\cdots$, 25, 5, 1}
37	9	{5,22,16,24,14,6,20,4,1}	{$\cdots$, 25, 5, 1}
41	10	{7,12,28,3,16,18,31,30,4,1}	{$\cdots$, 25, 35, 5, 1}

Since (13) does not hold if we replace r by $r-1$, then $2(n + r - 1) + 1 > q^{r-1}$ and hence,

$$q^{r-1} - 2(r-1) < 2n + 1 \leq q^r - 2r. \tag{14}$$

The number r is uniquely determined by (14) because the function $q^r - 2r$ is increasing for $r \geq 1$ if $q \geq 3$, and for $r \geq 2$ if $q \geq 2$. For $2n + 1 = q^r - 2r$, the resulting (d, k)-code is a perfect systematic code capable of correcting single peak-shifts of size 1.

In Table II, we give the minimum value of r according to (14) for $n \leq 25$ and $q \leq 7$. The cases which give rise to perfect systematic codes are marked with a star.

We assume that if there exists a perfect 2-shift N-design H (see Theorem 4 and Corollary 2) and for some q and r the inequalities (9) are fulfilled then there exists a particular ordering of H such that the weight sequence $W(H)$ contains the numbers $1, q, \cdots, q^{r-1}$. In this case, any (d, k)-code $C(W(H), g)$, $g \epsilon G_{4N+1}$, contains a systematic subcode of redundancy $r = \lceil \log_q (4N + 1) \rceil$ and if $\log_q (4N + 1)$ is an integer, every code $C(W(H), g)$ is a perfect systematic code capable of correcting peak-shifts of size 2 and has redundancy $r = \log_q (4N + 1)$. We checked that this assumption is true for small N and q. As an example, Table III gives the desirable H and $W(H)$ for the initial values of $m = 4N + 1 = 13, 17, \cdots, 41$ and $q = 5$. The check symbols are underlined. It should be noted that for $N = 10$ the check positions can not be located at the end of $W(H)$ and for $N = 6$ the corresponding codes are perfect systematic codes capable of correcting single peak-shifts of size 2.

Note that if there exists a prime p such that $t = (p - 1)/2$, and $q = k - d + 1 = p$, we can determine for a code $C = C_{d,k}^N$ consisting of all (d, k)-sequences of reduced length $N (N \geq 3)$, the number r from the inequalities

$$p^{r-1} < 2tN + 1 \leq p^r,$$

and taking into account that $N > r$ we construct an ordered t-shift N-design H in F_p^r for which the last r elements are the projective vectors $(1, p-1, 0, \cdots, 0)$, $(0, 1, p-1, 0, \cdots, 0), \cdots$.

$(0,\cdots,0,1,p-1),(0,0,\cdots,0,1)$. The corresponding weight sequence $W(H)$ ends by r unit vectors. Therefore, if $t=(p-1)/2$, $C=C_{k,d}^{N}$ and $q=k-d+1=p$ any of p^r subcodes $C(W(H),g)$, $g\epsilon F_p^r$, contains a systematic code with redundancy $r=\lceil\log_p(2tN+1)\rceil$; moreover, if $2tN+1=p^r$, then the code C is partitioned into p^r perfect codes $C(W(H),g)$ capable of correcting single peak-shifts of size t, each of which is a systematic code with redundancy $r=\log_p(2tN+1)$.

Example: Let $t=1$, $p=3$, $q=k-d+1=3$, and $N=13$. Then, $2tN+1=p^3$ and, thus, $r=3$.
Then,

$$H=\begin{matrix}1&1&1&1&1&1&1&1&0&0&1&0&0\\ \{0&1&0&0&1&1&2&2&1&1&2&1&0\}\\ 0&0&1&2&1&2&1&2&0&1&0&2&1\end{matrix}$$

and

$$W(H)=\begin{matrix}0&2&1&0&2&1&0&2&1&1&1&0&0\\ \{0&0&2&2&2&1&0&1&2&1&0&1&0\}\\ 1&1&1&0&1&0&1&0&1&1&0&0&1\end{matrix}$$

give rise to systematic (d,k)-codes of reduced length 13 and of redundancy 3, which are perfect codes capable of correcting single peak-shifts of size 1 for any d and k such that $k-d=2$.

VI. Conclusion

We introduce a definition of arbitrary (d,k)- and perfect (d,k)-codes capable correcting single peak-shifts of given size t. For the construction of perfect codes we use a general combinatorial method connected with finding "good" weight sequences in Abelian groups and introduce the concept of perfect t-shift N-designs. We give explicit constructions of such designs for $t=1$, $t=2$, and $t=(p-1)/2$, where p is a prime. Our construction is not only effective, but also universal in the sense that it does not depend on the (d,k)-constraints. It also allows to correct automatically those peak-shifts that violate (d,k)-constraints and to determine the beginning of the next codeword.

For an ideal multibit peak-shift channel, decoding errors that do not occur in the Nth substring do not propagate to subsequent blocks, as the length of the codeword does not change. However, if a decoding error occurs in the Nth substring, the first symbol of the next block is in error. If $^{\pm}tw_1$ is a valid syndrome, we make a decoding error in this block. Only if again in the Nth substring a decoding error occurs, we may speak of error propagation. By appropriate choice of w_1 we may avoid this phenomenon.

Catastrophic error propagation occurs whenever random errors are involved. These errors completely ruin the structure of the codewords. They insert new phrases or delete existing phrases in a codeword and thus synchronization regarding the beginning of the first symbol of a codeword is completely lost. One way to solve this problem is to fix the length of the codeword to a certain value. We can construct codes with a fixed binary length L by considering the union of all codewords of binary length L belonging to the (d,k)-codes of reduced length N, $L/(k+1)\le N\le L/(d+1)$. The codewords of fixed binary length start with d zeros and end with a symbol equal to 1. These codewords can be stored without merging digits.

References

[1] K. A. S. Immink, *Coding Techniques for Digital Recording.* Englewood Cliffs, NJ: Prentice Hall, 1990.

[2] S. Shamai and E. Zehavi, "Bounds on the capacity of the bit-shift magnetic recording channel," *IEEE Trans. Inform Theory,* vol. 37, pp. 863–872, May 1991.

[3] V. K. Kolesnik and V. Yu. Krachkovsky, "Generating function and lower bounds on rates for limited error-correcting codes," *IEEE Trans. Inform. Theory,* vol. 37, pp. 778–788, May 1991.

[4] L. J. Fredrickson and J. K. Wolf, "Error detecting multiple block (d,k) codes," *IEEE Trans. Magn.,* vol. MAG-25, pp. 4096–4098, Sept. 1989.

[5] A. Kuznetsov and A. J. Vinck, "Single peak-shift correction in (d,k)-sequences," in *IEEE Int. Symp. Inform. Theory,* Budapest, Hungary, June 24–28, 1991, p. 256.

[6] Ø. Ytrehus, "On (d,k) constrained error-controlling block codes," to be published. (See also *Abstracts of Papers, Int. Symp. Inform. Theory,* San Diego, CA, Jan. 1990, p. 124.)

[7] H. C. Ferreira and S. Lin, "Error and erasure control (d,k) block codes," *IEEE Trans. Inform. Theory,* vol. 37, pp. 1399–1408, Sept. 1991.

[8] K. A. S. Abdel-Ghaffar and J. H. Weber, "Bounds and constructions for runlength-limited error-control block codes," *IEEE Trans. Inform. Theory,* vol. 37 pt. II, pp. 789–800, May 1991.

[9] V. I. Levenshtein, "Binary codes correcting spurious insertions and deletions of ones," *Probl. Peredachi Inform.,* vol. 1, pp. 12–25, 1965.

[10] E. Zehavi and J. K. Wolf, "On runlength codes," *IEEE Trans. Inform. Theory,* vol. 34, pp. 45–54, Jan. 1988.

[11] V. I. Levenshtein, "On perfect codes in deletion and insertion metric," (in Russian) Discrete Math., vol. 3, no. 1, p. 3, 1991, English translation: *Discrete Math. Applica.,* vol. 2, no. 3, 1992).

[12] R. R. Varshamov and G. M. Tenengolz, "One asymmetrical error-correcting codes," (in Russian) *Avtomatika i Telemehanika,* vol. 26, no. 2, pp. 288–292, 1965.

An Updated Table of Minimum-Distance Bounds for Binary Linear Codes

A. E. Brouwer and Tom Verhoeff

***Abstract*—Tables with lower and upper bounds for $d_{\max}(n,k)$, the maximum possible minimum distance of a binary linear code with word length n and dimension k are shown.**

***Index Terms*—Binary linear codes, lower and upper bounds on minimum distance**

I. New Table of Bounds

We present some corrections and a further update on [64]. The update consists of new Tables I (Bounds), II (Index), and V (Statistics), and new lists of Labels and References. We also add one more condition to the list of Formal Invariance Conditions (see below). We adhere to the terminology used in [64], but here the references that appear in the table of bounds will be called *labels* (to avoid confusion with regular references).

The following corrections have been incorporated. The [69, 12, 29] code (labeled MS) from [40] has been withdrawn since it is not linear [67]. The [73, 49, 9] code (labeled V) from [35] has been withdrawn since it was in fact a [73, 46, 9] code (cf. [44]). Part of the damage done to the table by this withdrawal is repaired using a [64, 40, 9] Goppa code and a [68, 42, 10] code found by Shearer. It is quite

Manuscript received April 9, 1992; revised June 12, 1992.

The authors are with the Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

IEEE Log Number 9204103.