Kernels of q-ary 1-perfect codes *

K.T.Phelps † J.Rifà M.Villanueva ‡

1 Introduction

Let $\mathbb{F}_q^n$ be a vector space of dimension n over a Galois Field $\mathbb{F}_q = GF(q)$, where $q = p^r$, p prime. The *Hamming distance* between vectors u, $v \in \mathbb{F}_q^n$, denoted $d(u, v)$, is the number of coordinates in which u and v differ. A *q-ary code*, C, of length n is simply a subset of $\mathbb{F}_q^n$. The elements of C are called *codewords* and C is called *linear* if it is a linear space over $\mathbb{F}_q$. We will call p-linear a code C which is a linear space over the prime field $\mathbb{F}_p$. The *minimum distance* of a code is the smallest distance between a pair of codewords.

A q-ary code C of length n is *perfect* if for some integer $r \geq 0$ every $x \in \mathbb{F}_q^n$ is within distance r from exactly one codeword of C. In [8] it is shown that the only parameters for nontrivial perfect codes are the two Golay codes and the q-ary 1-perfect codes where q is a prime or prime power. The q-ary 1-perfect codes have length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 2$, and $r = 1$. They have q^{n-m} codewords and minimum distance 3. The linear 1-perfect codes are unique up to equivalence, they are the well-known *Hamming codes* and exist for all $m \geq 2$. Nonlinear q-ary 1-perfect codes also exist for $q = 2, m \geq 4$, $q \geq 3, m \geq 3$, and for q a prime power, $q \neq 4$ or 8, $m \geq 2$, [17], [16], [10].

Two structural properties of nonlinear codes are the rank and kernel.

The *rank* of a q-ary code C, $r(C)$, is simply the dimension of the subspace over $\mathbb{F}_q$ spanned by C. If $q = p^r$, $r > 1$, we define the *p-rank* of C as the dimension of the subspace over $\mathbb{F}_p$ spanned by C. By the dual of the nonlinear code C, denoted by $C^{\perp}$, we mean the dual of the subspace spanned by C having dimension $n - r(C)$. Etzion and Vardy [6] established the existence of binary 1-perfect codes of length $n = 2^m - 1$, $m \geq 4$, and rank $r(C) = n - m + s$ for each $s \in \{0, 1, \ldots, m\}$. In [13], the generalization to the q-ary case, that is, the existence of q-ary 1-perfect codes of length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 4$ and rank $r(C) = n - m + s$ for each $s \in \{0, 1, \ldots, m\}$ was established.

The *kernel* of a binary code C is defined as $K_C = \{x \in \mathbb{F}_2^n \ : \ x + C = C\}$. If the zero word is in C, then K_C is a linear subspace of C. In general, C can be written as the union of cosets of K_C and K_C is the largest such linear code for which this is true [4]. We will denote the dimension of the kernel of C by $k(C)$. Phelps and LeVan [11] established that for each such $m \geq 4$, there exists a nonlinear binary 1-perfect code of length $n = 2^m - 1$, with a kernel of dimension $k(C) = k$ for each $k \in \{1, 2, \ldots, n - m - 2\}$. The rank and kernel of binary 1-perfect codes are related, it is known that $k(C) + r(C) \geq n + 1$, since $C^{\perp} \subset K_C$ and the all

*Research partially supported by CICYT Grant TIC2000-0739-c04-01.
†Discrete & Statistical Sciences, Auburn University, Auburn, Al 36849-5307
‡Dep. d'Informàtica, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

ones codeword is always in the kernel, [4]. In [14], the exact upper and lower bounds on the kernel dimension for a fixed rank, $r(C) < n$, were established. In [3], binary 1-perfect codes of length n for all possible $k(C)$ and $r(C) < n$ are constructed.

In this paper, we will focus on the kernels of q-ary 1-perfect codes when $q \geq 3$. A previous approach, only over the field $\mathbb{F}_q$, was showed in [15]. Here, we will present definitions and properties of kernels for q-ary codes as well as p-ary subfield codes. We will construct q-ary 1-perfect codes of length n with different kernel dimensions, using switching constructions. We also give a simple and more general construction of nonlinear q-ary 1-perfect codes which were first constructed in [10]. Finally, we consider bounds on the dimension of the kernel.

2 Definitions and properties of the kernel

First of all, we will give different generalizations of the kernel for q-ary codes, C, over a Galois Field $\mathbb{F}_q = GF(q)$, where $q = p^r$, p prime. We will show some of their properties and when they are equivalent.

Definition 2.1 *The kernel and p-kernel of a q-ary code C over $\mathbb{F}_q$, where $q = p^r$, p prime, is respectively*

$$K_q(C) = \{x \in \mathbb{F}_q^n \;:\; \lambda x + C = C \quad \forall \lambda \in \mathbb{F}_q\}$$
$$K_p(C) = \{x \in \mathbb{F}_q^n \;:\; x + C = C\}.$$

It is easy to see that if the zero word is in C, then $K_q(C)$ is a linear sub-code of C and $K_p(C)$ is a p-linear sub-code of C. We will denote the dimension of the kernel and p-kernel of C by $k_q(C)$ and $k_p(C)$ respectively.

Proposition 2.1 *Let $K_q(C)$ ($K_p(C)$) be the kernel (p-kernel) of a q-ary code C. The code C is a union of cosets of $K_q(C)$ ($K_p(C)$), and $K_q(C)$ ($K_p(C)$) is the maximal linear subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$ ($\mathbb{F}_p$) with this property.*

It is easy to see that $K_q(C) \subseteq K_p(C)$ and also note that if $q = p$ prime, the kernel and p-kernel are exactly the same. The kernel of a binary code, C, is also the intersection of all maximal linear sub-codes of C, [9]. Next, we will show that, in general for q-ary codes, this is not necessarily true.

Proposition 2.2 *Let C be a q-ary code over $\mathbb{F}_q$, where $q = p^r$, p prime, and let $D = \{x \in C \;:\; \lambda x \in C \quad \forall \lambda \in \mathbb{F}_p\}$. Then, the intersection of all maximal linear sub-codes of C over $\mathbb{F}_p$ is $M(C) = \{x \in \mathbb{F}_q^n \;:\; x + D = D\}$.*

Proposition 2.3 *Let $M(C) = \{x \in \mathbb{F}_q^n \;:\; x + D = D\}$, where $D = \{x \in C \;:\; \lambda x \in C \quad \forall \lambda \in \mathbb{F}_p\}$. Then, D is a union of cosets of $M(C)$, and $M(C)$ is the maximal p-linear subspace of $\mathbb{F}_q^n$ with this property.*

It is easy to see that $K_p(C) \subseteq M(C)$, but, in general, $K_p(C) \neq M(C)$. For example, the code $C = \{0000, 1100, 2200, 0011\}$ over $\mathbb{Z}_3$ has kernel $K_3(C) = \{0000\}$ and $M(C) = \{0000, 1100, 2200\}$.

3 Subspaces T_i and T_i^p

In this section we consider two subspaces which play a key role in the switching construction. These are also important in determining the kernel and p-kernel of the resulting codes.

Definition 3.1 *T_i is the subspace over $\mathbb{F}_q$, $q = p^r$, generated by the codewords of weight 3 (triples) in the Hamming code, H_m, having a 1 in the i^{th} coordinate. T_i^p is the subspace over the sub-field $\mathbb{F}_p$ generated by these codewords.*

Proposition 3.1 *[13] Given a q-ary Hamming code H_m of length $n = \frac{q^m-1}{q-1}$, the dimension of T_i over $\mathbb{F}_q$ is $q^{m-1} - 1$, $\forall i \in \{1, \ldots, n\}$.*

Let H_m denote the Hamming code of length $n = \frac{q^m-1}{q-1}$. The columns of the parity check matrix of H_m are linearly independent and as such are representatives of all 1-dimensional subspaces in $\mathbb{F}_q^m$. The columns can be identified with the points of projective space of dimension $m-1$ over $\mathbb{F}_q$. In this way there is an obvious and natural correspondence between the coordinates of the codewords in H_m and points in the projective space $PG(m-1, q)$. We refer to certain coordinates as *independent* if the corresponding points in $PG(m-1, q)$ are independent or equivalently if the corresponding columns of the parity check matrix are independent (see [5]).

Proposition 3.2 *Given a q-ary Hamming code H_m with $\{1, 2, \ldots, m\}$ as a set of its independent coordinates, the dimension of $\cap_{i=1}^s T_i$ over $\mathbb{F}_q$ is $(q-1)^{s-1} q^{m-s}$, $\forall s \in \{2, \ldots, m\}$.*

Proposition 3.3 *Given a q-ary Hamming code H_m of length n, when $q = p^r$, $r \geq 2$, the dimension of T_i^p over the sub-field $\mathbb{F}_p$ is $\dfrac{q^{m-1}-1}{q-1}(r(q-2)+1)$, $\forall i \in \{1, \ldots, n\}$.*

The sub-code T_i^p is not a linear subspace over $\mathbb{F}_q$. In particular, we can ask what the kernel $K_q(T_i^p)$ is.

Corollary 3.4 *Given a q-ary Hamming code H_m of length n, when $q = p^r$, $r \geq 2$, the dimension of $K_q(T_i^p)$ is $\dfrac{q^{m-1}-1}{q-1}(q-2)$, $\forall i \in \{1, \ldots, n\}$.*

Corollary 3.5 *Given a q-ary Hamming code H_m of length n, when $q = p^r$, $r \geq 2$, if $\alpha\beta^{-1} \notin \mathbb{F}_p$, then $T = \alpha T_i^p \cap \beta T_i^p = \cap_{\gamma \in \mathbb{F}_q \setminus \{0\}} \gamma T_i^p$ and T is a subspace over $\mathbb{F}_q$ of dimension $\dfrac{q^{m-1}-1}{q-1}(q-2)$, $\forall \alpha, \beta \in \mathbb{F}_q$, $\forall i \in \{1, \ldots, n\}$.*

Proposition 3.6 *Given a q-ary Hamming code H_m with $\{1, 2, \ldots, m\}$ as a set of its independent coordinates, when $q = p^r$, $r \geq 2$, the dimension of $\cap_{i=1}^s T_i^p$ over $\mathbb{F}_p$ is $(r(q-1) - s(r-1))(q-1)^{s-2} q^{m-s}$, $\forall s \in \{2, \ldots, m\}$.*

Corollary 3.7 *Given a q-ary Hamming code H_m with $\{1, 2, \ldots, m\}$ as a set of its independent coordinates, when $q = p^r$, $r \geq 2$, the dimension of the kernel $K_q(\cap_{i=1}^s T_i^p)$ (over $\mathbb{F}_q$) is $(q-s-1)(q-1)^{s-2} q^{m-s}$, $\forall s \in \{2, \ldots, m\}$.*

4 Switching constructions

The most intuitive approach to constructing nonlinear 1-perfect codes consists of starting with the Hamming code H_m, and *switching* out one specially selected set of codewords $S \subset H_m$ for another set of words S' such that the resulting code $C = (H_m \backslash S) \cup S'$ would still be a 1-perfect code. This idea has been developed from different approaches to construct binary 1-perfect codes, see [1], [2], [6] and [12]. In [7], one generalization of this technique was used to construct q-ary 1-perfect codes. In [13], the approach developed in [11] was generalized to construct q-ary 1-perfect codes with different ranks. In this article, we will use switches to construct q-ary 1-perfect codes with kernels of different sizes.

Obviously, if sub-codes S, S' are switched we must have $|S| = |S'|$ and for all $x \in S', y \in H_m \setminus S$ we must have their distance $d(x,y) \geq 3$. If we consider the bipartite graph on the codewords in $H_m \cup H_m + w$ with an edge connecting codewords x, y if and only if $d(x,y) \leq 2$, then $S \subset H_m$, $S' \subset H_m + w$ will be a switch if and only if $S \cup S'$ is the union of components in the bipartite graph. If there is only one component, the switch is said to be minimal. Let $\mathbb{F}_q = \{0, \alpha^0, \alpha, \ldots, \alpha^{q-2}\}$, where α is a primitive element. Let e_i denote the vector of length n having all coordinates equal to zero, except the i^{th}, which contains a one.

Proposition 4.1 *$S \subset H_m$, $S' \subset H_m + \lambda e_i$ will be a minimal switch if and only if $S = \lambda T_i^p + y$ (and $S' = S + \lambda e_i$), where $y \in H_m$, $\forall i \in \{1, \ldots, n\}$ and $\forall \lambda \in \mathbb{F}_q \backslash \{0\}$.*

Corollary 4.2 *[13] Given a q-ary Hamming code H_m of length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 3$, $q \geq 3$ and $x_i \in H_m \backslash T_i$. Then,*

$$C' = (H_m \backslash (T_i + x_i)) \cup (T_i + x_i + \alpha^j e_i) \tag{1}$$

is a nonlinear q-ary 1-perfect code, $\forall i \in \{1, \ldots, n\}$ and $\forall j \in \{0, 1, \ldots, q-2\}$.

Lindström [10] gave a construction of nonlinear q-ary perfect codes for $m = 2$ ($n = q+1$) if q is a prime power, $q \neq 4$ or 8, which in effect relied on the existence of translation planes. We are able to give a simple construction of perfect codes with these parameters and in addition, a nonlinear code for $m = 2$ and $q = 8$.

Corollary 4.3 *Given a q-ary Hamming code H_m of length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 2$, $q = p^r$, $r > 1$ (except $m = 2$, $q = 4$) and $x_i \in H_m \backslash \alpha^j T_i^p$. Then,*

$$C' = (H_m \backslash (\alpha^j T_i^p + x_i)) \cup (\alpha^j T_i^p + x_i + \alpha^j e_i) \tag{2}$$

is a nonlinear q-ary 1-perfect code, $\forall i \in \{1, \ldots, n\}$ and $\forall j \in \{0, 1, \ldots, q-2\}$.

Proposition 4.4 *Let H_m be a q-ary Hamming code of length $n = \dfrac{q^m - 1}{q - 1}$, $m \geq 3$, $q \geq 3$ and let K be a subspace of H_m such that $T_i \subseteq K \subset H_m$ and $dim K \leq n - m - 1$. Then*

$$C' = (H_m \backslash (K + y)) \cup (K + y + \alpha^j e_i)$$

is a nonlinear q-ary 1-perfect code with rank $r(C') = n - m + 1$ and kernel $K_q(C') = K$, $\forall i \in \{1, \ldots, n\}$, $\forall j \in \{0, 1, \ldots, q-2\}$ and $\forall y \in H_m \backslash K$.

Corollary 4.5 *Let H_m be a q-ary Hamming code of length $n = \frac{q^m-1}{q-1}$, $m \geq 2$, $q = p^r$, $r > 1$, (except $m = 2$, $q = 4$) and let K be a p-linear subspace of H_m such that $\alpha^j T_i^p \subseteq K \subset H_m$ and $dim K \leq r(n-m)-1$ if $p > 2$ and $dim K \leq r(n-m)-2$ if $p = 2$. Then*

$$C' = (H_m \backslash (K+y)) \cup (K + y + \alpha^j e_i)$$

is a nonlinear q-ary 1-perfect code with p-rank $r(n-m)+1$ and p-kernel $K_p(C') = K$, $\forall i \in \{1, \ldots, n\}$, $\forall j \in \{0, 1, \ldots, q-2\}$ and $\forall y \in H_m \backslash K$.

By Proposition 4.2, once we have made one switch we have another q-ary 1-perfect code. Actually, it is proved [13] that for all $m \geq 4$, there exist $x_1, x_2, \ldots, x_m$ such that it is possible to make a series of switches. In this case, if $\{1, 2, \ldots, m\}$ is a set of independent points of H_m, we can switch $T_i + x_i$ with $T_i + x_i + \alpha^{j_1} e_i$, $\forall j_i \in \{0, \ldots, q-2\}$ $\forall i \in \{1, \ldots, m\}$, since $T_i + x_i$ and $T_k + x_k$ are always disjoint for all $k \neq i$.

Proposition 4.6 *Given a q-ary Hamming code H_m of length $n = \frac{q^m-1}{q-1}$, $m \geq 4$, with $\{1, 2, \ldots, m\}$ as a set of its independent points. Then, the nonlinear q-ary 1-perfect code*

$$C' = \Big(H_m \backslash \bigcup_{i=1}^{s} (T_i + x_i)\Big) \cup \bigcup_{i=1}^{s} (T_i + x_i + \alpha^{j_i} e_i) \tag{3}$$

has rank $r(C') = n - m + s$ and kernel $K_q(C') = \cap_{i=1}^{s} T_i$, $\forall s \in \{1, 2, \ldots, m\}$ and $\forall j_i \in \{0, 1, \ldots, q-2\}$.

Corollary 4.7 *Given a q-ary Hamming code H_m of length $n = \frac{q^m-1}{q-1}$, $m \geq 3$, $q = p^r$, $r > 1$, with $\{1, 2, \ldots, m\}$ as a set of its independent points. Then, the nonlinear q-ary 1-perfect code*

$$C' = \Big(H_m \backslash \bigcup_{i=1}^{s} (\alpha^{j_i} T_i^p + x_i)\Big) \cup \bigcup_{i=1}^{s} (\alpha^{j_i} T_i^p + x_i + \alpha^{j_i} e_i) \tag{4}$$

has rank $n-m+s$, p-rank $r(n-m)+s$ and p-kernel $K_p(C') = \cap_{i=1}^{s} \alpha^{j_i} T_i^p$, $\forall s \in \{1, 2, \ldots, m\}$ and $\forall j_i \in \{0, 1, \ldots, q-2\}$.

Corollary 4.8 *Let H_m be a q-ary Hamming code of length $n = \frac{q^m-1}{q-1}$, $m \geq 3$, $q = p^r$, $r > 1$, and let $1, \alpha, \ldots, \alpha^{r-1}$ be a basis of $\mathbb{F}_q$ over the sub-field $\mathbb{F}_p$. Then, the nonlinear q-ary 1-perfect code*

$$C' = \Big(H_m \backslash \bigcup_{j=1}^{s} (\alpha^{j-1} T_i^p + x_j)\Big) \cup \bigcup_{j=1}^{s} (\alpha^{j-1} T_i^p + x_j + \alpha^{j-1} e_i) \tag{5}$$

has rank $n-m+1$, p-rank $r(n-m)+s$ and kernel $K_p(C') = K_q(C') = \cap_{j=1}^{s} \alpha^{j-1} T_i^p$, $\forall s \in \{2, \ldots, r\}$ and $\forall i \in \{1, \ldots, n\}$.

In the same way as in the above results, we could construct nonlinear q-ary 1-perfect codes, C, with rank $n - m + m'$ and p-rank $r(n-m) + m'r'$, where $m' \leq m$ and $r' \leq r$, as long as there exists x_{ij}, $\forall i \in \{1, \ldots, m'\}$ and $\forall j \in \{1, \ldots, r'\}$, such that $\alpha^{j-1} T_i^p + x_{ij}$ and $\alpha^{k-1} T_s^p + x_{sk}$ are always disjoint. In this case, $K_p(C) = \cap_{i,j} \alpha^{j-1} T_i^p$ and $K_q(C) = K_q(T)$.

5 Bounds on the kernel dimensions

Fixed the rank, an upper bound on the kernel and p-kernel dimension, can be established using the same argument as in the binary case, [14].

Proposition 5.1 *A q-ary 1-perfect code of length n, C, with rank $r(C) = n - m + s$ over $\mathbb{F}_q$ and kernel $K_q(C)$ of dimension $n - m - \delta$ fulfills $q^\delta - \delta - 1 \geq s$.*

Corollary 5.2 *A q-ary 1-perfect code of length n, C, where $q = p^r$, with p-rank $r(n-m)+s$ and p-kernel $K_p(C)$ of dimension $r(n-m) - \delta$ fulfills $p^\delta - \delta - 1 \geq s$.*

If the p-rank of a q-ary 1-perfect code, C, is $r(n-m)+1$, we have the exact lower and upper bounds on $k_p(C)$, by Corollary 5.2 and next result. By Proposition 4.4 and Corollary 4.5, we can construct nonlinear q-ary 1-perfect codes with p-rank $r(n-m)+1$ and any p-kernel dimension, $k_p(C)$, between the lower and upper bounds.

Proposition 5.3 *Let C be a q-ary 1-perfect code of length $n = \dfrac{q^m - 1}{q - 1}$, $q = p^r$, with p-rank $r(n-m)+1$, then there exist $i \in \{1, 2, \ldots, n\}$ and $\alpha \in \mathbb{F}_q \backslash \{0\}$ such that αT_i^p is a subset of $K_p(C)$.*

Corollary 5.4 *Let C be a q-ary 1-perfect code of length $n = \dfrac{q^m - 1}{q - 1}$, $q = p^r$, with rank $n - m + 1$ and p-rank $r(n-m)+s$, then there exist $i \in \{1, 2, \ldots, n\}$ such that $\bigcap_{\alpha \in \mathbb{F}_q \backslash \{0\}} \alpha T_i^p$ is a subset of $K_p(C)$ and $K_q(C)$, $\forall s \in \{2, \ldots, r\}$.*

6 Conclusions

In [13], q-ary 1-perfect codes of length n and rank $n - m + s$ were constructed $\forall m \geq 4$ and $\forall s \in \{1, \ldots, m\}$. In this paper, we also constructed them when $q = p^r$, $r > 1$, for $m = 3$ and $\forall s \in \{1, 2, 3\}$ and for $m = 2$ and $s = 1$. The existence of q-ary 1-perfect codes for any $s \in \{2, \ldots, m\}$, when $m = 3$ if $q = p$ prime and $m = 2$ if $q = p^r$, $r > 1$, still remain open.

The switching constructions established in this paper give 1-perfect q-ary codes of given rank having kernels of minimal dimension. In the binary case, analogous constructions gave codes with kernels of *minimum* possible dimension for given ranks.

Theorem 6.1 *There exist a q-ary 1-perfect code of length n, C, when $q \geq 3$ prime, with rank $n - m + s$ and kernel of dimension*

$$k_q = \begin{cases} q^{m-1} - 1 & \text{if } s = 1 \quad \forall m \geq 3 \\ (q-1)^{s-1} q^{m-s} & \text{if } s > 1 \quad \forall m \geq 4 \end{cases}$$

Theorem 6.2 *There exist a q-ary 1-perfect code of length n, C, when $q = p^r$, $r > 1$ (except $m = 2$ and $q = 4$), with rank $n - m + s$ and kernel of dimension*

$$k_q = \begin{cases} \frac{q^{m-1}-1}{q-1}(q-2) & \text{if } s = 1 \quad \forall m \geq 2 \\ (q-s-1)(q-1)^{s-2} q^{m-s} & \text{if } s > 1 \quad \forall m \geq 3 \end{cases}$$

By results in section 5, the switching construction give also 1-perfect codes with rank $n-m+1$, any p-rank $r(n-m)+r'$ and the exact lower bound. The dimension of the kernel is k_q given in the previous theorems and the dimension of the p-kernel, $k_p \geq \frac{q^{m-1}-1}{q-1}(r(q-2)+1)$ if $r'=1$ and $k_p \geq \frac{q^{m-1}-1}{q-1}r(q-2)$ if $r'>1$. So, in particular, we established these results for the nonlinear 1-perfect codes with the same parameters as the ones given by Lindström [10], that is $m=2$.

The problem now is to establish a lower bound on the dimension of the kernel for 1-perfect q-ary codes of rank $n-m+s$, $\forall s \geq 2$. Key to this question seems to be the problem of the minimum kernel for full rank 1-perfect q-ary codes.

References

[1] S. V. Avgustinovich, F. I. Solov'eva, *On projections of perfect binary codes*, Proc. Seventh Joint Swedish-Russian Int. Workshop on Inform. Theory, St. Petersburg, Russia (1995), 25-26.

[2] S. V. Avgustinovich, F. I. Solov'eva, *On non-systematic perfect binary codes*, Problems of Information Transmission, **32** (1996), no 3, 258-261.

[3] S. V. Avgustinovich, O. Heden, F. I. Solov'eva, *On ranks and kernels of perfect codes*, sutmitted to Designs, Codes and Cryptography, (2002).

[4] H. Bauer, B. Ganter, F. Hergert, *Algebraic techniques for nonlinear codes*, Combinatorica, **3**(1983), 21-33.

[5] I. F. Blake and R. C. Mullin, The Mathematical Theory of Coding, Academic Press, New York, 1975

[6] T. Etzion, A. Vardy, *Perfect binary codes: constructions, properties, and enumeration*, IEEE Trans. on Information Theory, **40**(1994), 754-763.

[7] T. Etzion, *Nonequivalent q-ary perfect codes*, SIAM J. Discrete Math. **9** (1996), no 3, 413-423.

[8] F.I. MacWilliams and N.J. Sloane, *The theory of Error-Correcting codes*, North-Holland, New York, 1977.

[9] M. LeVan, *Designs and Codes*, PhD. Thesis, Auburn Univesity, 1995.

[10] B. Lindström *On group and nongroup perfect codes in q symbols*, Math. Scand., **25**(1969), 149-158.

[11] K. T. Phelps, M. LeVan, *Kernels of nonlinear Hamming codes*, Designs, Codes and Cryptography, **6**(1995), 247-257.

[12] K. T. Phelps, M. LeVan, *Switching equivalence classes of perfect codes*, Designs, Codes and Cryptography, **16**(1999), 179-184.

[13] K. T. Phelps, M. Villanueva, *Ranks of q-ary 1-perfect codes*, Designs, Codes and Cryptography, **27** (2002), 139-144.

[14] K. T. Phelps, M. Villanueva, *On Perfect Codes: Rank and Kernel*, Designs, Codes and Cryptography, **27** (2002), 183-194.

[15] K. T. Phelps, J. Rifà, M. Villanueva., *The Switching construction and kernels of q-ary 1-perfect codes*, Proceedings of ACCT-VIII, September 9-14, 2002, St. Petersburg, Russia, 222-225.

[16] J. Schönheim, *On linear and nonlinear single-error-correcting q-ary perfect codes*, Info. and Control, **12** (1968) 23-26.

[17] J. L. Vasil'ev, *On nongroup close-packed codes*, Problemy Kibernetiki, 8 (1963), 337-339.