Journal of Combinatorial Theory, Series A **99**, 180–190 (2002)
doi:10.1006/jcta.2002.3264

NOTE

On k-Wise Set-Intersections and k-Wise Hamming-Distances

Vince Grolmusz[1]

Department of Computer Science, Eötvös University, Budapest, Pázmány P. stny. 1/C, H-1117 Budapest, Hungary
E-mail: grolmusz@cs.elte.hu

and

Benny Sudakov[2]

Department of Mathematics, Princeton University, Princeton, New Jersy 08540; and Institute for Advanced Study, Princeton, New Jersy 08540
E-mail: bsudakov@math.princeton.edu

Received March 3, 2001

We prove a version of the Ray-Chaudhuri–Wilson and Frankl–Wilson theorems for k-wise intersections and also generalize a classical code-theoretic result of Delsarte for k-wise Hamming distances. A set of code-words $a^1, a^2, \ldots, a^k$ of length n have k-wise Hamming-distance ℓ, if there are exactly ℓ such coordinates, where not all of their coordinates coincide (alternatively, exactly $n - \ell$ of their coordinates are the same). We show a Delsarte-like upper bound: codes with few k-wise Hamming-distances must contain few code-words.

1. INTRODUCTION

In this paper, we give bounds on the size of set-systems and codes, satisfying some k-wise intersection-size or Hamming-distance properties. For $k = 2$, these theorems were proven by Ray-Chaudhuri and Wilson [13], Frankl and Wilson [9], and Delsarte [6, 5]. The $k > 2$ case was asked (partially) by Sós [14] and Füredi [10] proved, that for uniform set-systems with small sets, the order of magnitude of the largest set-system satisfying k-wise or just pair-wise intersection constraints are the same (his constant was huge). In [15] Vu considered families of sets with restricted k-wise intersection-size modulo two and obtain tight asymptotic bounds on

[1] Supported by Grant OTKA T030059, and the János Bolyai and Farkas Bolyai Fellowships.
[2] Research supported in part by NSF Grants DMS-0106589, CCR-9987845 and by the State of New Jersey.

0097-3165/02 $35.00

the size of such set-systems. Grolmusz [12] studied restricted k-wise set-intersections modulo arbitrary prime and proved a k-wise analog of the Deza–Frankl–Singhi theorem [7]. He also gave direct applications for explicit coloring of k-uniform hypergraphs without large monochromatic sets.

In this short paper, we first strengthen the result of [12], giving at the same time a much shorter proof, and then prove a k-wise version of the Delsarte-bounds [6, 5] for codes. In the last section, we present a construction which shows that some of our bounds are asymptotically tight.

2. SET SYSTEMS

In this section, we present results on set-systems with restricted k-wise intersections. We begin with the following extension of results from [13].

THEOREM 1. *Let L be a subset of nonnegative integers of size s. Let $k \geqslant 2$ be an integer and let $\mathscr{H}$ be a family of subset of n-element set such that $|H_1 \cap \cdots \cap H_k| \in L$ for any collection of k distinct sets from $\mathscr{H}$. Then*

$$|\mathscr{H}| \leqslant (k-1) \sum_{i=0}^{s} \binom{n}{i}.$$

If in addition the size of every member of $\mathscr{H}$ belongs to the set $\{k_1, \ldots, k_t\}$ and $k_i > s-t$ for every i, then

$$|\mathscr{H}| \leqslant (k-1) \sum_{i=s-t+1}^{s} \binom{n}{i}.$$

This theorem has the following modular version, which generalize the theorem of Frankl and Wilson [9] and strengthen the result from [12]. In case $p=2$ a slightly better bound appears in [15].

THEOREM 2. *Let p be a prime and L be a subset of $\{0, 1, \ldots, p-1\}$ of size s. Let $k \geqslant 2$ be an integer and let $\mathscr{H}$ be a family of subsets of n-element set such that $|H| \pmod{p} \notin L$ for every $H \in \mathscr{H}$ but $|H_1 \cap \cdots \cap H_k| \pmod{p} \in L$ for any collection of k distinct sets from $\mathscr{H}$. Then*

$$|\mathscr{H}| \leqslant (k-1) \sum_{i=0}^{s} \binom{n}{i}.$$

If in addition there exist $t \leqslant s$ integers $k_1, \ldots, k_t \in \{0, 1, \ldots, p-1\}$ so that $k_i > s-t$ for each i and $|H| \pmod{p} \in \{k_1, \ldots, k_t\}$ for every $H \in \mathscr{H}$, then

$$|\mathscr{H}| \leqslant (k-1) \sum_{i=s-t+1}^{s} \binom{n}{i}.$$

We start with the proof of Theorem 2 and then we show how to modify it to get Theorem 1. Our proof combines an approach introduced in [1] with some additional ideas.

Proof. Let $L = \{l_1, \ldots, l_s\}$ and let $\mathscr{H}$ be a set system satisfying assertion of the theorem. We repeat the following procedure until $\mathscr{H}$ is empty. At round i if $\mathscr{H} \neq \emptyset$, we choose a maximal collection $H_1, \ldots, H_d$ from $\mathscr{H}$ such that $|\bigcap_{j=1}^{d'} H_j| \pmod p \notin L$ for all $1 \leqslant d' \leqslant d$, but for any additional set $H' \in \mathscr{H}$ we have that $|\bigcap_{j=1}^{d} H_j \cap H'| \pmod p \in L$. Clearly, by definition such family always exists and $1 \leqslant d \leqslant k-1$. Denote $A_i = H_1$, $B_i = \bigcap_{j=1}^{d} H_j$ and remove all sets $H_1, \ldots, H_d$ from $\mathscr{H}$. Note that as the result of this process, we obtain at least $m \geqslant |\mathscr{H}|/(k-1)$ pairs of sets A_i, B_i. By definition, $|A_i \cap B_i| = |B_i| \pmod p \notin L$ but $|A_r \cap B_i| \pmod p \in L$ for any $r > i$. With each of the sets A_i, B_i, we associate its characteristic vector which we denote a_i, b_i, respectively.

Let $\mathbf{Q}$ denote the set of rational numbers. For $x, y \in \mathbf{Q}^n$, let $x \cdot y$ denote their standard scalar product. Clearly, $a_r \cdot b_i = |A_r \cap B_i|$. For $i = 1, \ldots, m$ let us define the multilinear polynomial f_i in n variables as

$$f_i(x) = \prod_{j=1}^{s} (x \cdot b_i - l_j),$$

where for each monomial, we reduce the exponent of each occurring variable to 1. Clearly,

$$f_i(a_i) = \prod_{j=1}^{s} (|A_i \cap B_i| - l_j) = \prod_{j=1}^{s} (|B_i| - l_j) \neq 0 \pmod p \quad \text{for all } 1 \leqslant i \leqslant m,$$

but

$$f_i(a_r) = \prod_{j=1}^{s} (|A_r \cap B_i| - l_j) = 0 \pmod p \quad \text{for } 1 \leqslant i < r \leqslant m.$$

We claim that the polynomials $f_1, \ldots, f_m$ are linearly independent as a functions over $\mathbf{F}_p$, the finite field of order p. Indeed, assume that $\sum \alpha_i f_i(x) = 0$ is a nontrivial linear relation, where $\alpha_i \in \mathbf{F}_p$. Let i_0 be the largest index such that $\alpha_{i_0} \neq 0$. Substitute a_{i_0} for x in this relation. Clearly, all terms but the one with index i_0 vanish, with the consequence $\alpha_{i_0} = 0$, contradiction. On the other hand, each f_i belongs to the space of multilinear polynomials of degree at most s. The dimension of this space is $\sum_{j=1}^{s} \binom{n}{i}$, implying the desired bound on m and thus on $|\mathscr{H}|$.

We now extend the idea above to prove the second part of the theorem. This extension uses a technique employed by Blokhuis [4] (see also [1]). For a subset $I \subseteq \{1, \ldots, n\} = [n]$ denote by v_I its characteristic vector and by $x_I = \prod_{i \in I} x_i$. In particular, $x_\emptyset = 1$ and it is easy to see that for any $J \subseteq [n]$, $x_I(v_J) = 1$ if and only if $I \subseteq J$ and zero otherwise. In what follows, we use the notation introduced in the first part of the proof.

In addition to polynomials f_i, we define a new set of multilinear polynomials

$$g_I(x) = x_I \cdot \prod_{j=1}^{t} \left(\sum_{i=1}^{n} x_i - k_j \right) \quad \text{for } I \subseteq [n].$$

Here again we reduce the exponent of each occurring variable to 1 to make g_I multilinear. We claim that the functions g_I are linearly independent over $\mathbf{F}_p$ for all $|I| \leqslant s - t$. Denote by $h(x) = \prod_{j=1}^{t} (\sum_{i=1}^{n} x_i - k_j)$. Since $k_i > s - t$ for all i, note that $h(v_I) \neq 0$ for all $|I| \leqslant s - t$. Let us arrange all the subsets of $\{1, 2, \ldots, n\}$ in a linear order, denoted by $\prec$, such that $J \prec I$ implies that $|J| \leqslant |I|$. Clearly if $|I|$, $|J| \leqslant s - t$ by definition, $g_I(v_J) = x_I(v_J)h(v_J)$ is equal to $h(v_J) \neq 0$ if $I = J$ and zero if $J \prec I$. Now the linear independence of $g_I(x)$ follows easily. Indeed, if $\sum_{|I| \leqslant s-t} \beta_I g_I(x) = 0$ is a nontrivial relation, let I_0 to be a minimal index (with respect to $\prec$), such that $\beta_{I_0} \neq 0$. By substituting $x = v_{I_0}$, we immediately obtain a contradiction.

To complete the argument, we show that the functions f_i remain linear independent even together with all the functions g_I for $|I| \leqslant s - t$. For a proof of this claim assume that

$$\sum_i \alpha_i f_i(x) + \sum_{|I| \leqslant s-t} \beta_I g_I(x) = 0$$

for some $\alpha_i, \beta_I \in \mathbf{F}_p$. Substitute $x = a_i$. All terms in the second sum vanish since $|A_i| \pmod{p} \in \{k_1, \ldots, k_t\}$ and hence $h(a_i) = 0$. In this case, we can deduce that all $\alpha_i = 0$ as previously. But then we get a relation only among the polynomials g_I and it was already proved that such relation should be trivial.

Therefore, we found $m + \sum_{i=0}^{s-t} \binom{n}{i}$ linearly independent functions, all of which belong to space of multilinear polynomials of degree at most s. As we already mentioned, the dimension of this space is $\sum_{j=1}^{s} \binom{n}{i}$. This implies the desired bound on m and thus on $|\mathscr{H}|$. ∎

An easy modification of above proof establishes Theorem 1.

Proof of Theorem 1 (*Sketch*). We repeat the following procedure. At step i, if $|H \cap H'| \in L$ for any two distinct sets in $\mathscr{H}$, then let H_1 be the largest set remaining in $\mathscr{H}$. Denote $A_i = B_i = H_1$ and remove H_1 from $\mathscr{H}$. Otherwise there exist a collection $H_1, \ldots, H_d$ from $\mathscr{H}$ such that $|\bigcap_{j=1}^{d'} H_j| \notin L$ for all

$1 \leqslant d' \leqslant d$, but for any additional set $H' \in \mathscr{H}$ we have that $|\bigcap_{j=1}^{d} H_j \cap H'| \in L$ and $2 \leqslant d \leqslant k-1$. Denote $A_i = H_1$, $B_i = \bigcap_{j=1}^{d} H_j$ and remove all sets $H_1, \ldots, H_d$ from $\mathscr{H}$. By definition, $|A_i \cap B_i| = |B_i|$ but $|A_r \cap B_i| \in L$ and has size strictly smaller than $|B_i|$ for all $r > i$. With each of the sets A_i, B_i, we associate its characteristic vector which we denote a_i, b_i, respectively.

We will also need a slightly different definition of polynomials f_i. For $i = 1, \ldots, m$ let us define the multilinear polynomial f_i in n variables as

$$f_i(x) = \prod_{l_j < |B_i|} (x \cdot b_i - l_j).$$

By our construction $f_i(a_i) \neq 0$ but $f_i(a_r) = 0$ for all $r > i$. Now the rest of the proof is identical with that of Theorem 2 and we omit it here. ∎

3. CODES

Let $A = \{0, 1, 2, \ldots, q-1\}$. The Hamming-distance of two elements of A^n is the number of coordinates in which they differ. A q-ary code of length n is simply a $C \subset A^n$. The following result is a classical inequality of Delsarte [6, 5]:

THEOREM 3 (Delsarte [5, 6]). *Let C be a q-ary code of length n. If the set of Hamming-distances which occur between distinct codewords of C has cardinality s, then*

$$|C| \leqslant \sum_{i=0}^{s} (q-1)^i \binom{n}{i}.$$

Frankl [8] proved the modular generalization of this result, and it was further strengthened by Babai *et al.* [3].

Our goal here is to give generalizations of this theorem for k-wise Hamming-distances.

DEFINITION 4. Let $a^i \in A^n$, for $i = 1, 2, \ldots, k$. Their k-wise Hamming-distance,

$$d_k(a^1, a^2, \ldots, a^k)$$

is ℓ, if there exist exactly ℓ coordinates, in which they are not all equal (Equivalently, their coordinates are all equal on $n - \ell$ positions.)

We prove the following theorems. The first one generalizes Delsarte's original bound [6, 5] to k-wise Hamming-distance:

THEOREM 5. *Let C be a q-ary code of length n. If the set of k-wise Hamming-distances which occur between k distinct codewords of C has cardinality s, then*

$$|C| \leqslant (k-1) \sum_{i=0}^{s} (q-1)^i \binom{n}{i}. \tag{1}$$

The second result is the modular version of Theorem 5, it is a k-wise generalization of the modular upper bound of Frankl [8] and also a result of Babai *et al.* [3]:

THEOREM 6. *Let C be a q-ary code of length n, p be a prime and let L be a subset of $\{1, \ldots, p-1\}$ of size s. If the set of k-wise Hamming-distances which occur between k distinct codewords of C lie in $L \bmod p$, then*

$$|C| \leqslant (k-1) \sum_{i=0}^{s} (q-1)^i \binom{n}{i}.$$

If in addition, there exist $t \leqslant s$ integers $w_1, \ldots, w_t \in \{0, 1, \ldots, p-1\}$, so that $w_i > s-t$ for each i and the weight of any member of C is congruent to some element of $\{w_1, \ldots, w_t\}$ modulo p, then

$$|C| \leqslant (k-1) \sum_{i=s-t+1}^{s} (q-1)^i \binom{n}{i}.$$

Two definitions are needed for the proof.

DEFINITION 7. Let a and b be two codewords of length n. Then let $a \sqcap b$ denote a codeword which contains only those coordinates of a and b which are equal. Let $|a \sqcap b|$ denote the length of word $a \sqcap b$.

For example, if $a = 01\,134\,230$, $b = 12\,134\,111$, then $a \sqcap b = 134$, and $|a \sqcap b| = 3$.

DEFINITION 8 (Babai *et al.* [3]). For a fixed integer $a \in A$, let $\varepsilon(a, x)$ be the polynomial in one variable with rational coefficients such that for every $b \in A$

$$\varepsilon(a, b) = \begin{cases} 1 & \text{if } b = a, \\ 0 & \text{if } b \neq a. \end{cases}$$

Since k-wise Hamming-distances which occur between k distinct codewords are always nonzero, then the proof of Theorem 5 follows from the statement of Theorem 6 if we choose a prime $p > n$. Therefore, we present only the proof of Theorem 6.

Proof. We start with the proof of the second part of the theorem. Our approach combines the ideas from [1, 3].

Let L be the set of k-wise Hamming-distances which occur between the elements of C and let $L' = \{l_1, \dots, l_s\} = \{(n-l) \pmod{p} | l \in L\}$. Note that since $0 \notin L$ we have $n \pmod{p} \notin L'$. Now repeat the following procedure until C is empty.

At round i if set C is still not empty we choose a maximal subset $a^1, \dots, a^d$ from C such that $|a^1 \sqcap a^2 \sqcap \cdots \sqcap a^{d'}| \pmod{p} \notin L'$ for all $1 \leqslant d' \leqslant d$, but for any additional word $a' \in C$ we have that $|a^1 \sqcap a^2 \sqcap \cdots \sqcap a^d \sqcap a'| \pmod{p} \in L'$. Clearly by definition, such codeword-set always exists and $1 \leqslant d \leqslant k-1$. Next define $c^i = a^1, b^i = a^1 \sqcap a^2 \sqcap \cdots \sqcap a^d$ and let $X_i \subseteq [n]$ be the set of indices of the coordinates in which a^j, $1 \leqslant j \leqslant d$ are all equal. Note that $|c^i \sqcap b^i| = |b^i| \pmod{p} \notin L'$ but $|c^i \sqcap b^i| \pmod{p} \in L'$ for any $r > i$. Finally, remove $a^1, \dots, a^m$ from C and proceed to the next round.

Let $f_i(x)$ be the following polynomial of n variables $x_1, \dots, x_n$:

$$f_i(x) = \prod_{u=1}^{s} \left(\sum_{j \in X_i} \varepsilon(b^i_j, x_j) - l_u \right),$$

where b^i_j is the value of the coordinate of b^i which corresponds to index $j \in X_i$ and the summation is restricted only to these indices. Note that by our construction, the number of such polynomials is at least $m = |C|/(k-1)$. By definition

$$f_i(c^i) = \prod_{u=1}^{s} (|c^i \sqcap b^i| - l_u) = \prod_{u=1}^{s} (|b^i| - l_u) \neq 0 \pmod{p},$$

but for all $r > i$.

$$f_i(c^r) = \prod_{u=1}^{s} (|c^r \sqcap b^i| - l_u) = 0 \pmod{p}.$$

Similar to the proof of Theorem 2, we next define an additional set of polynomials. Let $\delta(x)$ be the polynomial in one variable with rational coefficients such that $\delta(0) = 0$ and $\delta(i) = 1$ for all $i = 1, \dots, q-1$. Note that for any vector $x \in A^n$, the value of $\sum_{l=1}^{n} \delta(x_l)$ is equal to the weight of x. For all subsets $I \subset [n]$, $[I] \leqslant s-t$ and for all vectors $v \in \{1, \dots, q-1\}^I$, we define a polynomial

$$g_{I,v}(x) = \left(\prod_{i \in I} \varepsilon(x_i, v_i)\right) \prod_{j=1}^{t} \left(\sum_{l=1}^{n} \delta(x_l) - w_j\right),$$

where v_i are the entries of the vector v. Clearly, the number of such polynomials is equal to $\sum_{i=0}^{s-t} (q-1)^i \binom{n}{i}$, and by definition, the value $g_{I,v}(x)$ is an integer for all $x \in A^n$. In addition for every $x \in A^n$ with weight at most $s-t$, we have $g_{I,v}(x) \neq 0 \pmod{p}$ if and only if the vector x, restricted to I, equals v.

We claim that the polynomials f_i and $g_{I,v}$ are linearly independent over the rationals. For a proof of this claim assume that

$$\sum \alpha_i f_i(x) + \sum_{|I| \leqslant s-t} \beta_{I,v} g_{I,v}(x) = 0$$

is a nontrivial relation. Clearly, we can make all α_i and $\beta_{I,v}$ to be integers and in addition, since the above relation is nontrivial we can assume that not all of them are divisible by p. Let i_0 be the largest index such that $\alpha_{i_0} \neq 0 \pmod{p}$. Then, by substituting $x = c^{i_0}$ we obtain a contradiction. Indeed, $f_{i_0}(c^{i_0}) \neq 0 \pmod{p}$ but $f_i(c^{i_0}) = 0 \pmod{p}$ for all $i < i_0$ and also $g_{I,v}(c^{i_0}) = 0 \pmod{p}$, since the weight of c^{i_0} is equal w_j modulo p for some $1 \leqslant j \leqslant t$. Next suppose that all $\alpha_i = 0 \pmod{p}$, and let I_0 be the smallest set with the property $\beta_{I_0, v_0} \neq 0 \pmod{p}$ for some $v_0 \in \{1, \ldots, q-1\}^{I_0}$. Let $x_0 \in A^n$ be a vector which is equal to v_0 on the coordinates from I_0 and is zero everywhere else. Since all w_j are greater than the weight of x_0, by substituting $x = x_0$ into relation we obtain $g_{I_0, v_0}(x_0) \neq 0 \pmod{p}$, but as we explain above, $g_{I,v}(x_0) = 0 \pmod{p}$ for all $|I| \geqslant |I_0|$ and $v \neq v_0$. This contradiction proves the linear independence of f_i and $g_{I,v}$.

Next note that all our computations are over the domain where $x_i(x_i - 1) \ldots (x_i - q + 1) = 0$ for each variable $1 \leqslant i \leqslant n$. Thus, we can assume that in polynomials f_i and $g_{I,v}$, every variable x_i has exponent at most $q-1$. If not, we simply reduce these polynomials modulo $x_i(x_i - 1) \ldots (x_i - q + 1)$ for all i. Also, in addition, every term of f_i and $g_{I,v}$ is the monomial with at most s variables. The space of such polynomials has dimension $\sum_{i=0}^{s} (q-1)^i \binom{n}{i}$ and we have found $m + \sum_{i=0}^{s-t} (q-1)^i \binom{n}{i}$ independent functions in this space. This immediately implies the desired bound on m and hence on $|C|$.

Finally, we remark that the first part of this theorem follows already from independence of the polynomials f_i. This completes the proof. ∎

4. CONCLUDING REMARKS

(1) It is natural to ask how tight are the results of Theorems 1, 2, 5 and 6. In particular, do we need to have a multiplicative factor $(k-1)$ in all upper bounds? The following construction shows that in Theorem 2 this factor is indeed needed when p is fixed and n tends to infinity.

Let p be a fixed prime, $s<p$ and suppose $2^{t-1}<k-1\leqslant 2^t$ for some integer $t=o(n)$. Note that in this example, we do not fix the value of k and it can be as big as $2^{o(n)}$. Let X be an n-element set and let $Y_1,\dots,Y_t$ be disjoint subsets of X, each of size p. Denote by $Y=X-\bigcup_i Y_i$. By definition $|Y|=n'=n-\lceil\log_2(k-1)\rceil p=(1+o(1))n$. Since the number of subsets of $\{1,\dots,t\}$ is $2^t\geqslant k-1$, let $I_1,\dots,I_{k-1}$ be any $k-1$ of these distinct subsets of $\{1,\dots,t\}$. Finally, the family $\mathscr{H}$ consists of all subsets of X of the form $A\cup(\bigcup_{i\in I_j}Y_i)$ for all subsets A of Y of size s and all $1\leqslant j\leqslant k-1$. Clearly, the number of sets in the family $\mathscr{H}$ equals to

$$(k-1)\binom{n'}{s}=(1+o(1))(k-1)\binom{n}{s}$$

and it is easy to see that every set $H\in\mathscr{H}$ has size equal to s modulo p and every collections of k distinct sets from $\mathscr{H}$ satisfies that $|H_1\cap\cdots\cap H_k|=r(\mathrm{mod}\ p)$ for some integer $0\leqslant r\leqslant s-1$. Note, that the pairwise intersections of the sets of $\mathscr{H}$ do not satisfy the assumptions of the Frankl–Wilson theorem [9], since their sizes are not separated from the size of the sets itself; however, the k-wise intersection-sizes are already separated from s modulo p.

On the other hand, recently the second author together with Füredi [11] proved that the bound of Theorem 1 is not tight and the factor $(k-1)$ in this bound can be improved for all values of s and $k\geqslant 3$.

(2) An interesting open question is extension of the results of Theorems 2 and 6 to composite moduli. In this case, the polynomial upper bound is no longer valid in general. In particular for any $k\geqslant 2$, $q=6$ and $L=\{1,\dots,5\}$, there exist a family of subset of n-element set of superpolynomial size which satisfies the assertion of Theorem 2, see [12] for details. On the other hand for the special case of prime power moduli q and $s=q-1$, one can still get a polynomial upper bounds.

It is not difficult to see that our proofs of Theorems 2 and 6 together with the tools of Babai *et al.* [3, Theorem 6] and Babai and Frankl [2, Theorem 5.30] give the following two results, whose proof will be left to the reader.

THEOREM 9. *Let $k\geqslant 2$ and r be integers and p^α be a prime power. If $\mathscr{H}$ is a family of subset of n-element set such that $|H|=r$ $(\mathrm{mod}\ p^\alpha)$ for each $H\in\mathscr{H}$*

but $|H_1 \cap \cdots \cap H_k| \neq r \pmod{p^\alpha}$ *for all collections of k distinct sets from* $\mathscr{H}$, *then*

$$|\mathscr{H}| \leqslant (k-1) \sum_{i=0}^{p^\alpha - 1} \binom{n}{i}.$$

THEOREM 10. *Let C be a q-ary code of length n and* p^α *be a prime power. If the set of k-wise Hamming-distances which occur between k distinct codewords of C are never divisible by* p^α, *then*

$$|C| \leqslant (k-1) \sum_{i=0}^{p^\alpha - 1} (q-1)^i \binom{n}{i}.$$

(3) It is easy to see that when $k = 2$, one can deduce Theorem 2 from Theorem 6. But for $k \geqslant 3$ these two statements do not seem to be related and need different proofs.

ACKNOWLEDGMENT

The first author thanks Attila Sali for the remarks improving this work.

REFERENCES

1. N. Alon, L. Babai, and H. Suzuki, Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems, *J. Combin. Theory Ser. A* **58** (1991), 165–180.
2. L. Babai and P. Frankl, "Linear Algebra Methods in Combinatorics," Department of Computer Science, University of Chicago, 1992, preliminary version.
3. L. Babai, H. Snevily, and R. M. Wilson, A new proof for several inequalities on codes and sets, *J. Combin. Theory Ser. A* **71** (1995), 146–153.
4. A. Blokhuis, A new upper bound for the cardinality of 2-distance sets in Euclidean space, *in* "Convexity and Graph Theory," Jerusalem, 1981, pp. 65–66, North-Holland, Amsterdam, 1984.
5. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* **10** (1973).
6. P. Delsarte, The association schemes of coding theory, *in* "Combinatorics; Proceedings of the NATO Advanced Study Institute, Breukelen, 1974, Part 1: Theory of Designs, Finite Geometry and Coding Theory," pp. 139–157, Math. Centre Tracts, No. 55, Math. Centrum, Amsterdam, 1974.
7. M. Deza, P. Frankl, and N. M. Singhi, On functions of strength *t*, *Combinatorica* **3** (1983), 331–339.
8. P. Frankl, Orthogonal vectors in the *n*-dimensional cube and codes with missing distances, *Combinatorica* **6** (1986), 279–285.
9. P. Frankl and R. M. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.

10. Z. Füredi, On finite set-systems whose every intersection is a kernel of a star, *Discrete Math.* **47** (1983), 129–132.
11. Z. Füredi and B. Sudakov, Extremal set-systems with restricted k-wise intersections, in preparation.
12. V. Grolmusz, Set-systems with restricted multiple intersections and explicit Ramsey hypergraphs, "Technical Report DIMACS TR 2001-04," DIMACS, January 2001.
13. D. K. Ray-Chaudhuri and R. M. Wilson, On t-designs, *Osaka J. Math.* **12** (1975), 735–744.
14. V. T. Sós, Some remarks on the connection of graph theory, finite geometry and block designs, *in* Teorie Combinatorie; Proceedings of the Colloqium held in Rome 1973, pp. 223–233, 1976.
15. V. Vu, Extremal set systems with weakly restricted intersections, *Combinatorica* **19** (1999), 567–587.