On the Dimension of the Hull

Nicolas Sendrier

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On the dimension of the hull

Nicolas Sendrier

N° 2682

Octobre 1995

PROGRAMME 2

ISSN 0249-6399

INRIA
ROCQUENCOURT

On the dimension of the hull

Nicolas Sendrier

Programme 2 — Calcul symbolique, programmation et génie logiciel
Projet CODES

Rapport de recherche n°2682 — Octobre 1995 — 16 pages

Abstract: The hull [AK90],[AK92, p. 43] of a linear code is defined to be its intersection with its dual. We give here the number of distinct q-ary linear codes which have a hull of given dimension.

We will prove that, asymptotically, the proportion of q-ary codes whose hull has dimension l is a positive constant that only depends on l and q, and consequently that the average dimension of the hull is asymptotically a positive constant dependent of q.

Key-words: error correcting codes, self-dual codes, hull

(Résumé : tsvp)

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
Téléphone : (33 1) 39 63 55 11 – Télécopie : (33 1) 39 63 53 30

Sur la dimension de l'intersection d'un code et de son orthogonal

Résumé : Nous donnons ici le nombre de codes linéaires de longueur n et de dimension k sur $GF(q)$ ayant une intersection de dimension donnée avec leur orthogonal. Nous montrons que la dimension moyenne de cette intersection tend vers une constante strictement positive, dépendant de q, lorsque n et k tendent vers l'infini.

Mots-clé : code correcteur d'erreurs, codes auto-duaux, hull

1 Introduction

We will consider here linear codes over a finite field $GF(q)$. A $[q; n, k]$ code will be a linear code of length n and dimension k over $GF(q)$.

We will first study in §2 the properties of the Gaussian binomial coefficients, the coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ is the number of $[q; n, k]$ codes. The key result of this section is the inversion formula given in Corollary 2.

The hull [AK90] of a linear code is defined to be its intersection with its dual. In §4 we express the number $A_{n,k,l}$ of $[q; n, k]$ codes whose hull has dimension l in terms of the number of weakly self-dual codes of given parameters which is given in §3 (Theorem 1, due to Pless [Ple65]). Using the inversion formula of §2, we obtain an explicit expression of $A_{n,k,l}$ (Theorem 2). We then obtain an asymptotic equivalent of $A_{n,k,l}$, for fixed l when n and k go to infinity (Theorem 3), and we prove that under the same conditions, the ratio $A_{n,k,l}/\begin{bmatrix} n \\ k \end{bmatrix}$ is equivalent to a constant, dependent of q (Theorem 4). At last we give the average dimension of the hull of a linear code, which is asymptotically equal to $\sum_{i \geq 1} 1/(q^i + 1)$.

Most of the results above will be restricted to the case $n \geq 2k$, however, since the hull of a code is equal the the hull of its dual, this assumption can be made without losing any generality.

2 Gaussian binomial coefficients

Most of the result presented here can be found in [GR69] and [PA71].

Definition 1 *Let n and k be two integer. The* q-ary Gaussian binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ *is defined by*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}, \tag{1}$$

whenever $n \geq k \geq 0$, and $\begin{bmatrix} n \\ k \end{bmatrix} = 0$ otherwise.

Note that the Gaussian coefficients are connected to the usual binomial coefficients by $\lim_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix} = \binom{n}{k}$. The coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ is the number of subspaces of dimension k of a vector space of dimension n over $GF(q)$. More generally

Proposition 1 *Let U be a vector space over $GF(q)$ of dimension n, and let V be a subspace of U of dimension l. The number of subspaces C of U of dimension k containing V, that is $V \subset C \subset U$, is equal to $\begin{bmatrix} n-l \\ k-l \end{bmatrix}$.*

Proof. See for instance [MS77, Th. 4, p. 698]. □

We have the following identities:

Proposition 2 *Let $n \geq k \geq i$ be positive integers.*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}, \tag{2a}$$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ i \end{bmatrix} \begin{bmatrix} n-i \\ n-k \end{bmatrix} \Big/ \begin{bmatrix} k \\ i \end{bmatrix}, \tag{2b}$$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{q^n - 1}{q^{n-k} - 1} \begin{bmatrix} n-1 \\ k \end{bmatrix}, \tag{2c}$$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{q^{n-k+1} - 1}{q^k - 1} \begin{bmatrix} n \\ k-1 \end{bmatrix}, \tag{2d}$$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}. \tag{2e}$$

2.1 Asymptotic behavior

For all $i \geq 0$, let $[i] = (q-1)(q^2-1)\dots(q^i-1)$. Using the fact that $n(n+1)/2 - k(k+1)/2 - (n-k)(n-k+1)/2 = k(n-k)$, we can rewrite (1) as

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]}{[k][n-k]} = q^{k(n-k)} \frac{g_{q,n}}{g_{q,k}\, g_{q,n-k}}, \tag{3}$$

where the sequence $(g_{q,n})_{n \geq 0}$ is defined for all $q > 1$ by

$$g_{q,n} = \prod_{i=1}^{n} (1 - \frac{1}{q^i}). \tag{4}$$

This sequence is obviously decreasing and positive, we will see that it goes exponentially quickly to its limit. We will first need the following result.

Proposition 3 *[Com74, Ch. II, p. 106]*

$$\prod_{i \geq 0} (1 + t^i u) = \sum_{n \geq 0} \frac{t^{\binom{n}{2}} u^n}{(1-t)(1-t^2)\dots(1-t^n)}. \tag{5}$$

Proposition 4 *The sequence $(g_{q,n})_{n \geq 0}$ is strictly decreasing for $q > 1$, we will denote by $g_{q,\infty}$ its limit when n goes to infinity. We have*

$$\frac{g_{q,\infty}}{g_{q,n}} = \sum_{i \geq 0} \frac{1}{q^{ni}} \frac{(-1)^i}{(q-1)(q^2-1)\dots(q^i-1)}. \tag{6}$$

Proof. By definition (4) of $g_{q,n}$,

$$\frac{g_{q,\infty}}{g_{q,n}} = \prod_{i \geq n+1} \left(1 - \frac{1}{q^i}\right) = \prod_{i \geq 0} \left(1 - \frac{1}{q^{n+1} q^i}\right),$$

we then write (5) with $t = 1/q$ and $u = -1/q^{n+1}$, and we get (6). □

Corollary 1 *For all integer $n \geq 0$*

$$1 - \frac{1}{(q-1)q^n} \leq \frac{g_{q,\infty}}{g_{q,n}} \leq 1. \tag{7}$$

Proof. We can rewrite (6) as $\sum_{i\geq 0}(-1)^i G_i$, where $G_i^{-1} = (q-1)\dots(q^i-1)q^{ni}$. The sequence G_i is strictly positive and decreasing for $q > 1$, and thus, from a classical property of alternate series, we have the inequalities (7). □

2.2 An inversion formula

A classical inversion formula, given for instance in [Com74, p. 143], says that in any commutative ring with identity, if for all $n \geq 0$, $u_n = \sum_{k=0}^{n} \binom{n}{k} v_k$, then for all $n \geq 0$, we have $v_n = \sum_{k=0}^{n} \binom{n}{k}(-1)^{n-k} u_k$. A similar identity holds for Gaussian binomial coefficients. To obtain this formula we will first examine how the two basis $(x^n)_{n\geq 0}$ and $(p_n(x))_{n\geq 0}$, where $p_n(x) = (x-1)(x-q)\dots(x-q^{n-1})$, of the ring of polynomial over integers are related.

Proposition 5 *For all integer $n \geq 0$, let $p_n(x) = (x-1)(x-q)\dots(x-q^{n-1})$, we have*

1. $x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} p_k(x)$,

2. $p_n(x) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} (-1)^{n-k} q^{\binom{n-k}{2}} x^k$.

Proof. See [GR69] and [PA71]. □

Corollary 2 (Inversion formula) *Let $(u_i)_{i\geq 0}$ and $(v_i)_{i\geq 0}$ be two sequences. For all $k \geq 0$*

$$\left(\forall l, 0 \leq l \leq k, v_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} u_i\right) \Leftrightarrow \left(\forall l, 0 \leq l \leq k, u_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{l-i}{2}} v_i\right). \tag{8}$$

Proof. ([Com74, p. 118-119,143]) We can express $v_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} u_i$ as $U = PV$ where $U = (u_0, u_1, \dots)$, $V = (v_0, v_1, \dots)$ and P is an infinite triangular matrix of general term $\begin{bmatrix} l \\ i \end{bmatrix}$. The inverse P^{-1} of P is given for $u_i = p_i(x)$ and $v_i = x^i$ by Proposition 5, and its general term is $\begin{bmatrix} l \\ i \end{bmatrix}(-1)^{l-i} q^{\binom{l-i}{2}}$. And thus from $V = P^{-1}U$ we obtain $u_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix}(-1)^{l-i} q^{\binom{l-i}{2}} v_i$. □

3 Weakly self-dual codes

Definition 2 *A code C is said to be* weakly self-dual *(w.s.d.) if $C \subset C^{\perp}$.*

We will denote by $\sigma_{n,k}$ the number of w.s.d $[q; n, k]$ codes. We have [Seg59, Ple65, Ple68]:

Theorem 1 *Let n be a positive integer. The number of weakly self-dual $[q; n, k]$ codes is equal to*

1. *if n is odd and $k \leq (n-1)/2$*

$$\sigma_{n,k} = \prod_{i=1}^{k} \frac{q^{n-2i+1}-1}{q^i-1},$$

2. *if n and q are even and $k \leq n/2$*

$$\sigma_{n,k} = \frac{q^{n-k}-1}{q^n-1} \prod_{i=1}^{k} \frac{q^{n-2i+2}-1}{q^i-1},$$

3. *if $((n \equiv 0 \bmod 4)$ or $(n \equiv 2 \bmod 4$ and $q \equiv 1 \bmod 4))$ and $k \leq n/2$*

$$\sigma_{n,k} = \frac{q^{n/2-k}+1}{q^{n/2}+1} \prod_{i=1}^{k} \frac{q^{n-2i+2}-1}{q^i-1},$$

4. *if $n \equiv 2 \bmod 4$, $q \equiv 3 \bmod 4$ and $k \leq n/2-1$*

$$\sigma_{n,k} = \frac{q^{n/2-k}-1}{q^{n/2}-1} \prod_{i=1}^{k} \frac{q^{n-2i+2}-1}{q^i-1},$$

5. *else (k too large) $\sigma_{n,k} = 0$.*

Proposition 6 *Let $m = \lfloor n/2 \rfloor$. For all $k \leq m$, we have*

$$\sigma_{n,k} = s_{n,k} \frac{q^{k(n-k)}}{q^{k(k+1)/2}} \frac{g_{q^2,m}}{g_{q^2,m-k} g_{q,k}},$$

where

$$s_{n,k} = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ \dfrac{q^n - q^k}{q^n - 1} & \text{if } n \text{ and } q \text{ are even,} \\ \dfrac{q^{n/2} + \varepsilon q^k}{q^{n/2} + \varepsilon} & \text{if } n \text{ is even and } q \text{ is odd,} \end{cases}$$

with $\varepsilon = -1$ if $n \equiv 2 \bmod 4$ and $q \equiv 3 \bmod 4$ and $\varepsilon = 1$ otherwise.

Proof. If n is odd, we have $n = 2m+1$ and from Theorem 1

$$\begin{aligned} \sigma_{n,k} &= \prod_{i=1}^{k} \frac{q^{n+1-2i}-1}{q^i-1} = \frac{q^{nk+k-2\sum_{i=1}^{k} i}}{q^{k(k+1)/2}} \prod_{i=1}^{k} \frac{1-1/q^{2m+2-2i}}{1-1/q^i} \\ &= \frac{q^{k(n-k)}}{q^{k(k+1)/2}} \frac{g_{q^2,m}}{g_{q^2,m-k} g_{q,k}}. \end{aligned} \tag{9}$$

If n is even, we have $n = 2m$. From Theorem 1, it comes

$$\sigma_{n,k} = \frac{s_{n,k}}{q^k} \prod_{i=1}^{k} \frac{q^{n-2i+2}-1}{q^i-1} = \frac{s_{n,k}}{q^k} \sigma_{n+1,k},$$

and writing (9) for $\sigma_{n+1,k}$, we get

$$\sigma_{n,k} = \frac{s_{n,k}}{q^k} \frac{q^{k(n+1-k)}}{q^{k(k+1)/2}} \frac{g_{q^2,m}}{g_{q^2,m-k} g_{q,k}} = s_{n,k} \frac{q^{k(n-k)}}{q^{k(k+1)/2}} \frac{g_{q^2,m}}{g_{q^2,m-k} g_{q,k}}. \qquad \square$$

Proposition 7 *For all $k \leq n/2$,*

$$1 - \frac{1}{q^{n/2-k}} \leq s_{n,k} \leq 1 + \frac{1}{q^{n/2-k}}.$$

Proof. If $k \leq n/2$, we have the following inequalities

$$1 - \frac{1}{q^{n/2-k}} \leq \frac{q^{n/2}-q^k}{q^{n/2}-1} \leq \frac{q^n-q^k}{q^n-1} \leq 1 \leq \frac{q^{n/2}+q^k}{q^{n/2}+1} \leq 1 + \frac{1}{q^{n/2-k}},$$

which proves the result. $\square$

4 Hull of a linear code

Definition 3 *The hull of a linear code is defined to be the intersection of the code with its dual.*

We will denote by $\mathcal{H}(C) = C \cap C^\perp$ the hull of a code C.

Lemma 1 *Let V be a weakly self-dual $[q; n, l]$ code. The number of $[q; n, k]$ codes C such that $V \subset \mathcal{H}(C)$ is equal to $\begin{bmatrix} n-2l \\ k-l \end{bmatrix}$.*

Proof. Let C be a $[q; n, k]$ code. We have $V \subset \mathcal{H}(C) = C \cap C^\perp$ if and only if $V \subset C \subset V^\perp$, and from Proposition 1 the number of such codes is equal to $\begin{bmatrix} n-2l \\ k-l \end{bmatrix}$. $\square$

Lemma 2 *Let C be a $[q; n, k]$ code and let $\mathcal{H}(C)$ be its hull, the number of weakly self-dual $[q; n, l]$ codes V such that $V \subset \mathcal{H}(C)$ is equal to $\begin{bmatrix} \dim \mathcal{H}(C) \\ l \end{bmatrix}$.*

Proof. The hull $\mathcal{H}(C)$ of C is weakly self-dual, so is any of its subspace. The number of subspaces of dimension l of $\mathcal{H}(C)$ is $\begin{bmatrix} \dim \mathcal{H}(C) \\ l \end{bmatrix}$, and thus we get the result. $\square$

Proposition 8 *For all i, $0 \leq i \leq k$, let $A_{n,k,i}$ denote the number of $[q; n, k]$ code whose hull has dimension i. We have, for all l, $0 \leq l \leq k$,*

$$\begin{bmatrix} n-2l \\ k-l \end{bmatrix} \sigma_{n,l} = \sum_{i=l}^{k} \begin{bmatrix} i \\ l \end{bmatrix} A_{n,k,i}. \tag{10}$$

Proof. Let C be a $[q;n,k]$ code, from Lemma 2, $\mathcal{H}(C)$ contains $\begin{bmatrix}\dim \mathcal{H}(C)\\ l\end{bmatrix}$ different w.s.d. $[q;n,l]$ codes. From Lemma 1 any $[q;n,l]$ w.s.d. code is contained in the hull of $\begin{bmatrix}n-2l\\ k-l\end{bmatrix}$ different $[q;n,k]$ codes. Finally, the number of w.s.d. $[q;n,l]$ codes is $\sigma_{n,l}$ and we get

$$\sigma_{n,l} = \left(\sum_{\substack{C \subseteq GF(q)^n \\ \dim C = k}} \begin{bmatrix}\dim \mathcal{H}(C)\\ l\end{bmatrix} \right) \begin{bmatrix}n-2l\\ k-l\end{bmatrix}^{-1},$$

which leads to the result since $A_{n,k,i}$ is the number of $[q;n,k]$ codes whose hull has dimension i, and $\begin{bmatrix}i\\ l\end{bmatrix} = 0$ when $i < l$. □

Theorem 2 *Let n be a positive integer, and let $\sigma_{n,i}$ denote for all i the number of weakly self-dual $[q;n,i]$ codes. For all $k \le n/2$ and all $l \le k$, the number of $[q;n,k]$ codes whose hull has dimension l is equal to*

$$A_{n,k,l} = \sum_{i=l}^{k} \begin{bmatrix}n-2i\\ k-i\end{bmatrix} \begin{bmatrix}i\\ l\end{bmatrix} (-1)^{i-l} q^{\binom{i-l}{2}} \sigma_{n,i}. \tag{11}$$

Proof. For all l, $0 \le l \le k$, let

$$\begin{bmatrix}k\\ l\end{bmatrix} V_{n,k,l} = \begin{bmatrix}n-2k+2l\\ l\end{bmatrix} \sigma_{n,k-l} \quad \text{and} \quad \begin{bmatrix}k\\ l\end{bmatrix} U_{n,k,l} = A_{n,k,k-l}, \tag{12}$$

we write (10) with $k-l$ instead of l, and we get for all $l \le k$

$$\begin{bmatrix}k\\ l\end{bmatrix} V_{n,k,l} = \begin{bmatrix}n-2k+2l\\ l\end{bmatrix} \sigma_{n,k-l} = \sum_{i=k-l}^{k} \begin{bmatrix}i\\ k-l\end{bmatrix} A_{n,k,i} = \sum_{j=0}^{l} \begin{bmatrix}k-j\\ k-l\end{bmatrix} \begin{bmatrix}k\\ j\end{bmatrix} U_{n,k,j},$$

where $j = k-i$ in the last summation, and thus for all $l \le k$, using (2b)

$$V_{n,k,l} = \sum_{j=0}^{l} \frac{\begin{bmatrix}k-j\\ k-l\end{bmatrix}\begin{bmatrix}k\\ j\end{bmatrix}}{\begin{bmatrix}k\\ l\end{bmatrix}} U_{n,k,j} = \sum_{j=0}^{l} \begin{bmatrix}l\\ j\end{bmatrix} U_{n,k,j}. \tag{13}$$

We now apply the inversion formula of Corollary 2 to (13), and we have for all $l \le k$

$$\begin{aligned} \frac{A_{n,k,k-l}}{\begin{bmatrix}k\\ l\end{bmatrix}} &= U_{n,k,l} = \sum_{j=0}^{l} \begin{bmatrix}l\\ j\end{bmatrix} (-1)^{l-j} q^{\binom{l-j}{2}} V_{n,k,j} \\ &= \sum_{i=k-l}^{k} \begin{bmatrix}l\\ k-i\end{bmatrix} (-1)^{l-k+i} q^{\binom{l-k+i}{2}} \frac{\begin{bmatrix}n-2i\\ k-i\end{bmatrix}\sigma_{n,i}}{\begin{bmatrix}k\\ i\end{bmatrix}}, \end{aligned} \tag{14}$$

where $i = k - j$ in the last summation. If we then replace $k - l$ by l in (14) we obtain for all $l \leq k$

$$A_{n,k,l} = \sum_{i=l}^{k} \begin{bmatrix} n-2i \\ k-i \end{bmatrix} \frac{\begin{bmatrix} k-l \\ k-i \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix}}{\begin{bmatrix} k \\ i \end{bmatrix}} (-1)^{i-l} q^{\binom{i-l}{2}} \sigma_{n,i} = \sum_{i=l}^{k} \begin{bmatrix} n-2i \\ k-i \end{bmatrix} \begin{bmatrix} i \\ l \end{bmatrix} (-1)^{i-l} q^{\binom{i-l}{2}} \sigma_{n,i}. \qquad \square$$

The result above will be practically useful only when $k - l$ is small. When the number of terms in the summation (11) gets large, the formula becomes intractable. Furthermore, it gives no precise idea of the asymptotic behavior of $A_{n,k,l}$ when n and k get large.

4.1 Asymptotic behavior

For all l, $0 \leq l \leq k$, let

$$b_{n,k,l} = \frac{\begin{bmatrix} n-2k+2l \\ l \end{bmatrix} \sigma_{n,k-l} q^{k(k+1)/2}}{\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix}} \quad \text{and} \quad a_{n,k,l} = \frac{A_{n,k,k-l} q^{k(k+1)/2}}{\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix}}.$$

Proposition 9 *Let $m = \lfloor n/2 \rfloor$. For all $k \leq m$ and for all l, $0 \leq l \leq k$, we have*

$$b_{n,k,l} = q^{l(l+1)/2} \frac{g_{q^2,m} g_{q,n-2k+2l} g_{q,n-k}}{g_{q^2,m-k+l} g_{q,n-2k+l} g_{q,n}} s_{n,k-l}.$$

Proof. From Proposition 6, we have

$$\sigma_{n,k-l} = \frac{q^{(k-l)(n-k+l)}}{q^{(k-l)(k-l+1)/2}} \frac{g_{q^2,m}}{g_{q^2,m-k+l} g_{q,k-l}} s_{n,k-l}.$$

From (3) we have

$$\begin{bmatrix} n-2k+2l \\ l \end{bmatrix} = q^{l(n-2k+l)} \frac{g_{q,n-2k+2l}}{g_{q,l} g_{q,n-2k+l}},$$

and

$$\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} = q^{k(n-k)+l(k-l)} \frac{g_{q,n} g_{q,k}}{g_{q,k} g_{q,n-k} g_{q,l} g_{q,k-l}},$$

and thus, using $k(k+1)/2 - l(l+1)/2 = (k-l)(k-l+1)/2 + l(k-l)$,

$$\frac{\begin{bmatrix} n-2k+2l \\ l \end{bmatrix} \sigma_{n,k-l}}{\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix}} = \frac{q^{l(l+1)/2}}{q^{k(k+1)/2}} \frac{g_{q^2,m} g_{q,n-2k+2l} g_{q,n-k}}{g_{q^2,m-k+l} g_{q,n-2k+l} g_{q,n}} s_{n,k-l}. \qquad \square$$

Proposition 10 *For all l, $0 \leq l \leq k$, we have*

$$\sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} a_{n,k,i} = b_{n,k,l}. \tag{15}$$

Proof. We have $a_{n,k,l} = U_{n,k,l} q^{k(k+1)/2} / \begin{bmatrix} n \\ k \end{bmatrix}$ and $b_{n,k,l} = V_{n,k,l} q^{k(k+1)/2} / \begin{bmatrix} n \\ k \end{bmatrix}$, where $U_{n,k,l}$ and $V_{n,k,l}$ are defined by (12), and then (13) will give

$$\frac{\begin{bmatrix} n \\ k \end{bmatrix} b_{n,k,l}}{q^{k(k+1)/2}} = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} \frac{\begin{bmatrix} n \\ k \end{bmatrix} a_{n,k,i}}{q^{k(k+1)/2}}.$$

□

Lemma 3 *Let $m = \lfloor n/2 \rfloor$, for all $i \leq m$,*

$$\frac{g_{q^2,m} g_{q,n-i}}{g_{q^2,m-i} g_{q,n}} \leq 1.$$

Proof. By definition of the sequences $g_{q,n}$ and $g_{q^2,n}$, we have

$$\frac{g_{q^2,m} g_{q,n-i}}{g_{q^2,m-i} g_{q,n}} = \frac{\prod_{j=m-i+1}^{m} 1 - 1/q^{2j}}{\prod_{j=n-i+1}^{n} 1 - 1/q^{j}} = \prod_{j=1}^{i} \frac{1 - 1/q^{2m-2j+2}}{1 - 1/q^{n-j+1}}.$$

For all j, $1 \leq j \leq i$, and whatever is the parity of n, we have $1 - 1/q^{2m-2j+2} \leq 1 - 1/q^{n-j+1}$, which gives us the result. □

Lemma 4 *Let $m = \lfloor n/2 \rfloor$, for all $i \leq m$,*

$$\frac{g_{q^2,\infty} g_{q,n-2i}}{g_{q^2,m-i} g_{q,\infty}} \geq 1.$$

Proof. We have, by definition,

$$\frac{g_{q^2,\infty} g_{q,n-2i}}{g_{q^2,m-i} g_{q,\infty}} = \frac{\prod_{j>m-i} 1 - 1/q^{2j}}{\prod_{j>n-2i} 1 - 1/q^{j}} = \prod_{j>0} \frac{1 - 1/q^{2m-2i+2j}}{1 - 1/q^{n-2i+j}}.$$

For all $j > 0$, and whatever is the parity of n, we have $1 - 1/q^{2m-2i+2j} \geq 1 - 1/q^{n-2i+j}$. □

Proposition 11 *Let $\delta_{n,k,l} = q^{l(l+1)/2} - b_{n,k,l}$. For all l, $0 \leq l \leq k$, we have*

$$-\frac{q^{l(l-1)/2}}{q^{n/2-k}} \leq \delta_{n,k,l} \leq \frac{q}{q-1} \frac{q^{l(l-1)/2}}{q^{n/2-k}}.$$

Proof. Let $m = \lfloor n/2 \rfloor$, we have

$$b_{n,k,l} = q^{l(l+1)/2} \frac{g_{q^2,m} g_{q,n-2k+2l} g_{q,n-k}}{g_{q^2,m-k+l} g_{q,n-2k+l} g_{q,n}} s_{n,k-l},$$

using Lemma 3, Lemma 4 and the fact that $g_{q,n}$ and $g_{q^2,n}$ are decreasing, we obtain

$$\frac{g_{q,\infty}}{g_{q,n-2k+l}} s_{n,k-l} \leq \frac{b_{n,k,l}}{q^{l(l+1)/2}} \leq s_{n,k-l}.$$

From Corollary 1 and Proposition 7, we get

$$L = \left(1 - \frac{1}{(q-1)q^{n-2k+l}}\right)\left(1 - \frac{1}{q^{n/2-k+l}}\right) \leq \frac{b_{n,k,l}}{q^{l(l+1)/2}} \leq 1 + \frac{1}{q^{n/2-k+l}}.$$

Let's consider the left-hand term L of this inequality

$$\begin{aligned} L &\geq 1 - \frac{1}{(q-1)q^{n-2k+l}} - \frac{1}{q^{n/2-k+l}} \\ &\geq 1 - \frac{1}{(q-1)q^{n/2-k+l}} - \frac{1}{q^{n/2-k+l}} = 1 - \frac{q}{(q-1)q^{n/2-k+l}}, \end{aligned}$$

and finally, we have

$$1 - \frac{q}{(q-1)q^{n/2-k+l}} \leq \frac{b_{n,k,l}}{q^{l(l+1)/2}} \leq 1 + \frac{1}{q^{n/2-k+l}},$$

which concludes the proof. □

Proposition 12 *Let $(u_l)_{l\geq 0}$ be the sequence solution of $\sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} u_i = q^{l(l+1)/2}$, and let $\gamma_{n,k,l} = u_l - a_{n,k,l}$. For all l, $0 \leq l \leq k$, we have $\sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} \gamma_{n,k,i} = \delta_{n,k,l}$.*

This proposition states that equation (15) can be cut into two pieces. We have for all l, $0 \leq l \leq k$,

$$\begin{cases} a_{n,k,l} = u_l + \gamma_{n,k,l} \\ b_{n,k,l} = q^{l(l+1)/2} + \delta_{n,k,l} \end{cases} \text{ and } \begin{cases} \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} u_i = q^{l(l+1)/2} \\ \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} \gamma_{n,k,i} = \delta_{n,k,l} \end{cases}$$

We will now examine these equation and prove that u_l is asymptotically proportional to $q^{l(l+1)/2}$, and that the term $\gamma_{n,k,l}$ can be neglected for fixed l when n and k grow.

4.1.1 First order term

We now wish to solve the equation $\sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} u_i = q^{l(l+1)/2}$. By use of the inversion formula (8) we get

$$u_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i}{2}}. \tag{16}$$

Lemma 5 *For all $l \geq 0$, we have*

$$w_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i+1}{2}} = \begin{cases} 0 & \text{if } l \text{ is odd,} \\ u_l & \text{if } l \text{ is even.} \end{cases} \tag{17}$$

Proof. From $\binom{l-i+1}{2} = \binom{l-i}{2} + l - i$ and (16) we get

$$w_l = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i+1}{2}} = u_l + \sum_{i=0}^{l-1} \begin{bmatrix} l \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i}{2}} (q^{l-i} - 1),$$

and from (2c), we have $\begin{bmatrix} l \\ i \end{bmatrix}(q^{l-i} - 1) = \begin{bmatrix} l-1 \\ i \end{bmatrix}(q^l - 1)$, thus

$$w_l = u_l + (q^l - 1) \sum_{i=0}^{l-1} \begin{bmatrix} l-1 \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i}{2}} = u_l - (q^l - 1) w_{l-1}.$$

Now, $w_l = 0$ when l is odd because the terms for i and $l - i$ in the sum are the opposite of each other. And when l is even, $l - 1$ is odd and $w_l = u_l - (q^l - 1)w_{l-1} = u_l$. □

Proposition 13 *Let u_l be the sequence defined by*

$$\sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} u_i = q^{l(l+1)/2}.$$

We have for all $l \geq 0$

$$u_l = \prod_{\substack{0 \leq i \leq l \\ i \ even}} q^i \prod_{\substack{0 \leq i \leq l \\ i \ odd}} (q^i - 1),$$

or equivalently $u_0 = 1$ and for all $l > 0$

$$u_l = \begin{cases} u_{l-1} q^l & \text{if } l \text{ is even,} \\ u_{l-1}(q^l - 1) & \text{if } l \text{ is odd.} \end{cases}$$

Proof. We will prove the result by induction. Clearly $u_0 = 1$. From (16) and (2e), we have

$$\begin{aligned} u_l &= \sum_{i=0}^{l} \left(\begin{bmatrix} l-1 \\ i-1 \end{bmatrix} q^{l-i} + \begin{bmatrix} l-1 \\ i \end{bmatrix} \right) (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i}{2}} \\ &= \sum_{i=1}^{l} \begin{bmatrix} l-1 \\ i-1 \end{bmatrix} (-1)^{l-i} q^{l-i} q^{\binom{i+1}{2}+\binom{l-i}{2}} + \sum_{i=0}^{l-1} \begin{bmatrix} l-1 \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{i+1}{2}+\binom{l-i}{2}} \\ &= \underbrace{q^l \sum_{i=0}^{l-1} \begin{bmatrix} l-1 \\ i \end{bmatrix} (-1)^{l-i-1} q^{\binom{i+2}{2}-(i+1)+\binom{l-i-1}{2}}}_{=u_{l-1}} - \underbrace{\sum_{i=0}^{l-1} \begin{bmatrix} l-1 \\ i \end{bmatrix} (-1)^{l-i-1} q^{\binom{i+1}{2}+\binom{l-i}{2}}}_{=w_{l-1}} \end{aligned}$$

Thus we have $u_l = q^l u_{l-1} - w_{l-1}$, where w_l is defined by (17). Lemma 5 then gives $u_l = q^l u_{l-1}$ if l is even, and $u_l = (q^l - 1)u_{l-1}$ if l is odd. □

Corollary 3 *For all $l \geq 0$, we have*

$$u_l = q^{l(l+1)/2} \frac{g_{q,l}}{g_{q^2,\lfloor l/2 \rfloor}}.$$

Proof. From Proposition 13, we have

$$u_l = q^{l(l+1)/2} \prod_{\substack{0 \leq i \leq l \\ i \ odd}} \left(1 - \frac{1}{q^i}\right) = q^{l(l+1)/2} \prod_{0 \leq i \leq l} \left(1 - \frac{1}{q^i}\right) \prod_{0 \leq i \leq \lfloor l/2 \rfloor} \left(1 - \frac{1}{q^{2i}}\right)^{-1},$$

which exactly means $u_l = q^{l(l+1)/2} g_{q,l} / g_{q^2,\lfloor l/2 \rfloor}$. □

4.1.2 Second order term

Proposition 14 *For all l, $0 \leq l \leq k$, we have*

$$|\gamma_{n,k,l}| \leq (l+1) \frac{q}{q-1} \frac{q^{l(l-1)/2}}{g_{q,\lfloor l/2 \rfloor} q^{n/2-k}}.$$

Proof. The inversion formula gives

$$\gamma_{n,k,l} = \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} (-1)^{l-i} q^{\binom{l-i}{2}} \delta_{n,k,i},$$

$$|\gamma_{n,k,l}| \leq \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} q^{\binom{l-i}{2}} |\delta_{n,k,i}| \leq \frac{q}{(q-1)q^{n/2-k}} \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} q^{\binom{l-i}{2}+\binom{i}{2}},$$

and since $\binom{l-i}{2} + \binom{i}{2} = \binom{l}{2} - i(l-i)$, we have

$$|\gamma_{n,k,l}| \leq \frac{q}{q-1} \frac{q^{\binom{l}{2}}}{q^{n/2-k}} \sum_{i=0}^{l} \begin{bmatrix} l \\ i \end{bmatrix} \frac{1}{q^{i(l-i)}} = \frac{q}{q-1} \frac{q^{\binom{l}{2}}}{q^{n/2-k}} \sum_{i=0}^{l} \frac{g_{q,l}}{g_{q,i} g_{q,l-i}}.$$

Finally, we have $g_{q,l} \leq g_{q,i}$ and $g_{q,l} \leq g_{q,l-i}$, thus $g_{q,l}/(g_{q,i} g_{q,l-i}) \leq \min(1/g_{q,i}, 1/g_{q,l-i}) \leq 1/g_{q,\lfloor l/2 \rfloor}$, and

$$|\gamma_{n,k,l}| \leq \frac{q}{q-1} \frac{q^{\binom{l}{2}}}{q^{n/2-k}} \frac{l+1}{g_{q,\lfloor l/2 \rfloor}}.$$

□

Corollary 4 *There exists a constant K, only dependent of q, such that for all l, $0 \leq l \leq k$,*

$$\frac{|\gamma_{n,k,l}|}{u_l} \leq K \frac{k}{q^{n/2-k+l}}.$$

Proof. From Proposition 14 and Corollary 3, we can easily find such a constant. □

4.2 Dimension of the hull

Theorem 3 *Let n be a positive integer. For all $k \leq n/2$ and all $l \leq k$, the number of $[q; n, k]$ codes whose hull has dimension l is equal to*

$$A_{n,k,l} = \begin{bmatrix} n \\ k \end{bmatrix} \frac{1}{q^{l(l+1)/2}} \frac{g_{q,k}}{g_{q^2,\lfloor (k-l)/2 \rfloor} g_{q,l}} \left(1 + O\left(\frac{k}{q^{n/2-l}}\right)\right).$$

Proof. By definition, we have $A_{n,k,k-l} q^{k(k+1)/2} = \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} a_{n,k,l}$. We have $a_{n,k,k-l} = u_{k-l} + \gamma_{n,k,k-l}$ and thus from Corollary 4, we get

$$A_{n,k,l} q^{k(k+1)/2} = \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} u_{k-l} \left(1 + O\left(\frac{k}{q^{n/2-l}}\right)\right).$$

Finally from Corollary 3 and (3) we obtain the result. □

This result gives an accurate estimate as long as l is not close to $n/2$, this will always be the case if $n - 2k$ is large. If $n - 2k$ is small and l is close to k, then formula (11) of Theorem 2 will apply.

The fraction $A_{n,k,l} / \begin{bmatrix} n \\ k \end{bmatrix}$ represents the proportion of $[q; n, k]$ codes whose hull has a given dimension l. The next theorem states that this ratio is independent from n and k when these numbers grow.

Theorem 4 *Let $A_{n,k,l}$ denote the number of $[q; n, k]$ codes whose hull has dimension l. For all l, the proportion $A_{n,k,l} / \begin{bmatrix} n \\ k \end{bmatrix}$ of such codes is convergent when n and k goes to infinity. We will denote R_l this limit. We have for all $l \geq 0$,*

$$R_l = \frac{R_0}{g_{q,l} q^{l(l+1)/2}} = \frac{R_0}{(q-1)(q^2-1)\dots(q^l-1)} \text{ where } R_0 = \frac{g_{q,\infty}}{g_{q^2,\infty}}.$$

Proof. Immediate application of Theorem 3. □

Corollary 5 *The average dimension of the hull of a q-ary linear code is asymptotically equal to*

$$\sum_{l \geq 1} l R_l = \sum_{i \geq 1} \frac{1}{q^i + 1}.$$

Proof. Let's apply (5) with $t = 1/q$ and $u = tz$, we obtain

$$\prod_{i \geq 0} \left(1 + \frac{z}{q^{i+1}}\right) = \sum_{n \geq 0} \frac{z^n}{(q-1)(q^2-1)\dots(q^l-1)},$$

from which we obtain the series

$$\mathcal{R}(z) = \sum_{l \geq 0} R_l z^l = R_0 \prod_{i \geq 1} \left(1 + \frac{z}{q^i}\right).$$

(Remark that when $z = 1$ we have

$$\mathcal{R}(1) = \sum_{l \geq 0} R_l = R_0 \prod_{i \geq 1} \left(1 + \frac{1}{q^i}\right) = R_0 \frac{\prod_{i \geq 1}(1 - 1/q^{2i})}{\prod_{i \geq 1}(1 - 1/q^i)} = R_0 \frac{g_{q^2,\infty}}{g_{q,\infty}} = 1$$

which was predictable.) The average dimension of the hull can be obtained by differentiation of the series $\mathcal{R}(z)$,

$$\frac{d\mathcal{R}(z)}{dz} = \sum_{l \geq 1} l R_l z^{l-1} = \sum_{i \geq 1} \frac{1}{q^i} \frac{\mathcal{R}(z)}{1 + z/q^i} = \mathcal{R}(z) \sum_{i \geq 1} \frac{1}{q^i + z},$$

and thus, for $z = 1$,

$$\sum_{l \geq 1} l R_l = \sum_{i \geq 1} \frac{1}{q^i + 1}. \qquad \square$$

5 Conclusion

We proved here that when the size of a code gets large its hull has a constant average dimension. Additionally, from Theorem 3, the correcting term is exponentially smaller than the dominant term term. For instance, in the binary case with $n = 40$ and $k = 20$, the average dimension of the hull computed by the asymptotic formula has a relative difference of 10^{-6} with the exact value computed with (11). This figure drops to 10^{-15} when $n = 2k = 100$.

The dimension of the hull is a strictly positive constant, practically, this means that the hull will be a vector space whose dimension is small but not necessarily zero, at least for small values of q. We may then use the hull to obtain non trivial information on codes for which the usual invariants (minimum distance, weight distribution ...) are difficult to compute.

At last, if we remark that $\mathcal{H}(C) = C \cap C^\perp = (C + C^\perp)^\perp$, it appears that the hull can be computed by a Gaussian elimination on a $n \times n$ matrix, where n is the length of the code.

Acknowledgment

The author wishes to thank Ph. Flajolet for his indications of great import. He is also particularly thankful to E.F. Assmus, Jr for his valuable advice and for his interest in this work.

References

[AK90] E.F. Assmus, Jr and J.D. Key. Affine and projective planes. *Discrete Mathematics*, 83:161–187, 1990.

[AK92] E.F. Assmus, Jr and J.D. Key. *Designs and their Codes*. Cambridge University Press, 1992.

[Com74] L. Comtet. *Advanced Combinatorics*. Reidel, Dordrecht, 1974.

[GR69] J. Goldman and G.-C. Rota. The number of subspaces of a vector space. In W.T. Tutte, editor, *Recent Progress in Combinatorics*, pages 75–83. Academic Press, 1969.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[PA71] G. Pólya and G.L. Alexanderson. Gaussian binomial coefficients. *Elemente der Mathematik*, 26:102–109, 1971.

[Ple65] V. Pless. The number of isotropic subspaces in a finite geometry. *Rend. Sc. Fis. Mat. e Nat., Accad. Naz. Lincie, Ser. VIII*, 39:418–421, December 1965.

[Ple68] V. Pless. On the uniqueness of the Golay codes. *Journal of Combinatorial theory*, 5:215–228, 1968.

[Seg59] B. Segre. Le geometrie di Galois. *Annali di Mat. Pura Appl., Ser. 4a*, 49:1–96, 1959.

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 46 avenue Félix Viallet, 38031 GRENOBLE Cedex 1
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105,
78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
ISSN 0249-6399