On products of linear error correcting codes

Mirandola, D.

Chapter 3

Squares of Random Linear Codes

3.1 Overview

As shown in Chapter 1, the motivation for a systematic code-theoretic study of squares is quite strong. With a view to contributing to such an endeavor, our concern in this chapter is with the dimension of squares of random linear codes. Specifically, our purpose is to answer the following question: does the square of a code "typically" fill the whole space? We give a positive answer, for codes of dimension k and length roughly $k^2/2$ or smaller. Moreover, the convergence speed is exponential in the difference $k(k+1)/2 - n$, if this difference is at least linear in k. The proof uses random coding and combinatorial arguments, together with algebraic tools involving the precise computation of the number of quadratic forms of a given rank, and the number of their zeros.

Even though the main results of this chapter involve probability measures, we shall not give any introduction to probability theory, as we are only concerned with discrete probability and uniform distributions, hence essentially combinatorics. That is, given a finite sample space $\mathcal{U}$, an event $\mathcal{E}$ is a subset of $\mathcal{U}$, and its *probability* $\Pr(\mathcal{E})$ is simply defined to be the ratio between the size of the event itself and the size of the sample space. A *random variable* is a function defined over the sample space and with values in a subset of $\mathbb{R}$. The *expectation* of a random variable X is $\mathbb{E}[X] := \sum_{x \in \mathbb{R}} x \Pr(X = x)$. Here $\Pr(X = x)$ is a standard notation for the event corresponding to the preimage of x in the sample space. Observe that in the discrete case this is zero for all but a finite number of $x \in \mathbb{R}$, hence the sum defining the expectation is finite.

Throughout this chapter, $\mathbb{F}$ denotes a finite field of size q, where q is a fixed prime power, and all codes are $\mathbb{F}$-linear. Since a generating set of vectors for the square of a code $C \subseteq \mathbb{F}^n$ of dimension k can be constructed by taking all possible $k(k+1)/2$ products of two elements of a basis of the code C, it is reasonable to expect that a randomly chosen code of length $n < k(k+1)/2$ has a square which fills up the whole space, i.e. $C^2 = \mathbb{F}^n$. However, linear relations between products of elements of C are not typically independent random events, and one has to overcome a certain number of obstacles to prove such a statement. Our main result is indeed to show that when the difference $k(k+1)/2 - n$ goes to infinity as a function of k, however slowly, the probability that a random code of length n and dimension k has a square different from $\mathbb{F}^n$ goes to zero. We also study the speed of convergence, which is exponential in the difference $k(k+1)/2 - n$, if this difference is at least linear in k, and the limiting case $n = k(k+1)/2$. We shall also consider the slightly easier case when the length n is such that $n \geq k(k+1)/2$: we obtain that with probability tending to 1 when $n - k(k+1)/2$ goes to infinity, the dimension of the square of the random code is exactly $k(k+1)/2$. Again, this convergence is exponentially fast if $n - k(k+1)/2$ is at least linear in k. Previously, the best-known fact on this problem was given by Faugère et al. in [34] who proved that for $n \geq k(k+1)/2$ and for any function $\omega(k)$ that goes to infinity with k, the dimension of the square of the random code is at least $k(k+1)/2 - k\omega(k)$ with probability tending to 1 when k goes to infinity. Our techniques break significantly with the approach of [34] and combine the study of the dual distance of the square of a random code, and the distribution of zeros of random quadratic forms. In the rest of this section we describe our results precisely and give an overview of our proofs and the structure of the chapter.

We first define the probabilistic model we shall work with. For all positive integers $n \geq k$, we define $\mathcal{C}(n,k)$ to be the family of all codes of length n and dimension k whose first k coordinates make up an information set: equivalently, members of $\mathcal{C}(n,k)$ have a generator matrix which can be written in systematic form, i.e. as

$$G = \left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & A \\ & & 1 & \end{array}\right),$$

for some $k \times (n-k)$ matrix A. We endow $\mathcal{C}(n,k)$ with the uniform distribution. Since codes of $\mathcal{C}(n,k)$ are in one-to-one correspondence with $k \times (n-k)$ matrices A, choosing a random element of $\mathcal{C}(n,k)$ amounts to choosing a random uniform matrix A.

Remark 3.1.1. There are several possible choices for the probabilistic model. An alternative way of choosing a random code consists of choosing its generator

matrix uniformly at random among all $k \times n$ matrices. Yet another alternative is to consider the uniform distribution among all codes of length n and dimension k. The first alternative probability distribution has the disadvantage that the resulting code may be of dimension $< k$. The second alternative distribution is perhaps the most theoretically elegant but makes it somewhat cumbersome to use the puncturing arguments that we will work with, hence the above choice of a probabilistic model. In Section 3.5 we shall argue however that our results are not altered significantly under these alternative probability distributions.

Our main result is the following.

MAIN THEOREM 3.1.2. *Let $n\colon \mathbb{N} \to \mathbb{N}$ be such that $k(k+1)/2 \geq n(k) \geq k$ for all $k \in \mathbb{N}$ and define $t\colon \mathbb{N} \to \mathbb{N}, t(k) := k(k+1)/2 - n(k)$. Then there exist constants $\gamma, \delta \in \mathbb{R}_{>0}$ such that, for all large enough k,*

$$\Pr(C^2 = \mathbb{F}^{n(k)}) \geq 1 - 2^{-\gamma k} - 2^{-\delta t(k)},$$

where C is chosen uniformly at random from $\mathcal{C}(n(k), k)$.

For lengths n that are larger than $k(k+1)/2$, we also have:

THEOREM 3.1.3. *Let $n\colon \mathbb{N} \to \mathbb{N}$ be such that $n(k) \geq k(k+1)/2$ for all $k \in \mathbb{N}$ and define $s\colon \mathbb{N} \to \mathbb{N}, s(k) := n(k) - k(k+1)/2$. Then there exists a constant $\hat{\delta} \in \mathbb{R}_{>0}$ such that, for all large enough k,*

$$\Pr\left(\dim C^2 = \frac{k(k+1)}{2}\right) \geq 1 - 2^{-\hat{\delta} s(k)},$$

where C is chosen uniformly at random from $\mathcal{C}(n(k), k)$.

Strangely enough, Theorems 3.1.2 and 3.1.3 are not quite symmetrical. In particular the term $2^{-\gamma k}$ is absent from the statement of Theorem 3.1.3 but can not be avoided in Theorem 3.1.2: this is because with probability at least $1/q^k$, the random matrix G will contain a column of zeros, or two identical columns, in which case the square C^2 can not be equal to $\mathbb{F}^{n(k)}$. The two theorems will not require exactly the same methods and Theorem 3.1.2 will need more work than Theorem 3.1.3. We shall deal with them separately.

Our first step towards establishing Theorem 3.1.2 will be to estimate the expected minimum distance of the dual of the square of a random code of length $k(k+1)/2$. Specifically, we shall prove:

PROPOSITION 3.1.4. *There exist constants (depending only on q) $c, \widetilde{c} \in \mathbb{R}_{>0}$ such that, for all large enough k, if C is chosen uniformly at random from $\mathcal{C}(k(k+1)/2, k)$ then*

$$\Pr\left(d_{\min}((C^2)^{\perp}) \leq c \cdot \frac{k(k+1)}{2}\right) \leq 2^{-\widetilde{c}k}.$$

This last proposition enables us to use puncturing arguments. In our probabilistic model, a random code of length n can be obtained by first choosing a random code of length $n+t$ and then puncturing t times on a random position. The probability that a punctured code has the same dimension as the original code is well-separated from zero whenever the dual distance of the original code is large enough. This fact will be enough in itself to establish the following weaker version of Main Theorem 3.1.2.

THEOREM 3.1.5. *There exist constants (depending only on q) $c, \widetilde{c} \in \mathbb{R}_{>0}$ such that, if $n\colon \mathbb{N} \to \mathbb{N}$ satisfies*

$$k \leq n(k) \leq c \cdot \frac{k(k+1)}{2}$$

for all $k \in \mathbb{N}$ then, for all large enough k,

$$\Pr(C^2 = \mathbb{F}^{n(k)}) \geq 1 - 2^{-\widetilde{c}k},$$

where C is chosen uniformly at random from $\mathcal{C}(n(k), k)$.

However, in order to deal with block lengths that approach the upper bound $k(k+1)/2$ on the dimension of the square of C, and prove the full-fledged Main Theorem 3.1.2, we need some additional ingredients.

Given an code C of length n and dimension k and denoting by $\pi_1, \ldots, \pi_n \in \mathbb{F}^k$ the columns of a generator matrix of C, define the linear map

$$\begin{array}{rccc} \mathrm{ev}_C\colon & \mathrm{Quad}(\mathbb{F}^k) & \to & \mathbb{F}^n, \\ & Q & \mapsto & (Q(\pi_1), \ldots, Q(\pi_n)) \end{array}$$

where $\mathrm{Quad}(\mathbb{F}^k)$ denotes the vector space of quadratic forms on $\mathbb{F}^k$. As observed in Section 2.5.4, the image of ev_C does not depend on the choice of a generator matrix of C, and it is equal to C^2. In particular, $C^2 = \mathbb{F}^n$ if and only if ev_C is surjective. Moreover, by basic linear algebra $C^2 = \mathbb{F}^n$ if and only if

$$\dim \ker \mathrm{ev}_C = \dim \mathrm{Quad}(\mathbb{F}^k) - n = \frac{k(k+1)}{2} - n.$$

So it makes sense to focus on this kernel. We view its cardinality as a random variable, with distribution induced by the uniform distribution of C over $\mathcal{C}(n,k)$: formally, for all positive integers $n \geq k$ we define

$$X(n,k) := |\ker \mathrm{ev}_C|.$$

Our main intermediate result, of interest in its own right, is:

THEOREM 3.1.6. *We have that*

$$\lim_{k\to\infty} \mathbb{E}\left[X\left(\frac{k(k+1)}{2}, k\right)\right] = 2.$$

A simple use of Markov's inequality will then give us that, for a random code C of length $k(k+1)/2$, the probability that the codimension of C^2 does not exceed ℓ,

$$\Pr\left(\dim C^2 \geq \frac{k(k+1)}{2} - \ell\right)$$

tends to 1 when ℓ goes to infinity, furthermore exponentially fast if ℓ is linear in k. Puncturing arguments, again relying on Proposition 3.1.4, will enable us to conclude the proof of Theorem 3.1.2 when the block length n is well separated from $k(k+1)/2$.

As a by-product, Theorem 3.1.6 also enables us to deal easily with the case when $n \geq k(k+1)/2$. Theorem 3.1.3 will follow as a straightforward consequence.

We conclude this overview by giving a rough idea of the proof of Theorem 3.1.6. It involves computing the number of zeros of a quadratic form of given rank and the number of quadratic forms of given rank. The results we need are stated in Section 3.3 and proved in Section 2.4.

By definition, for all positive integers $m \geq k$ we have

$$\begin{aligned}\mathbb{E}[X(m,k)] &= \\ &= \mathbb{E}[|\{Q \in \mathrm{Quad}(\mathbb{F}^k) : Q(\pi_1) = \cdots = Q(\pi_m) = 0\}|],\end{aligned}$$

where we can assume that, for $i = 1, \ldots, k$, $\pi_i = e_i$ is the i-th unit vector while $\pi_{k+1}, \ldots, \pi_m \in \mathbb{F}^k$ have independent, uniform distribution over $\mathbb{F}^k$, by definition of the family $\mathcal{C}(m,k)$ and our probabilistic model.

Note that the conditions $Q(e_1) = \cdots = Q(e_k) = 0$ are independent (in the sense of linear algebra), hence the subspace

$$S := \{Q \in \mathrm{Quad}(\mathbb{F}^k) : Q(e_1) = \cdots = Q(e_k) = 0\}$$

of $\mathrm{Quad}(\mathbb{F}^k)$ has dimension $k(k-1)/2$. Moreover, as $\pi_{k+1}, \ldots, \pi_m \in \mathbb{F}^k$ are independent (in the sense of probability), we have

$$\begin{aligned}\Pr(Q(\pi_{k+1}) = \cdots = Q(\pi_m) = 0) &= \\ &= \Pr(Q(\pi_{k+1}) = 0)^{m-k} = \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}\end{aligned}$$

for any $Q \in \mathrm{Quad}(\mathbb{F}^k)$. Here $Z(Q)$ denotes the zero set of Q and q is the cardinality of $\mathbb{F}$. Finally, by linearity of the expectation we have

$$\begin{aligned}\mathbb{E}[X(m,k)] &= \\ &= \mathbb{E}[|\{Q \in S : Q(\pi_{k+1}) = \cdots = Q(\pi_m) = 0\}|] = \\ &= \sum_{Q \in S} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \qquad (3.1)\end{aligned}$$

Now if it were true (it is not) that all non-zero quadratic forms on $\mathbb{F}^k$ have q^{k-1} zeros, we would have, when we set $m = k(k+1)/2$,

$$\mathbb{E}[X(m,k)] = 1 + \frac{1}{q^{m-k}}(q^{\frac{k(k-1)}{2}} - 1) \longrightarrow 2$$

"proving" Theorem 3.1.6. However, even though it is false that all non-zero quadratic forms on $\mathbb{F}^k$ have q^{k-1} zeros, this still holds "on average": roughly speaking, most quadratic forms have q^{k-1} zeros, quadratic forms whose number of zeros is far from this value are those of small rank, and the number of such forms is so small that it contributes almost nothing to the expectation. In other words, the expectation behaves as if it were true that all non zero quadratic forms on $\mathbb{F}^k$ have q^{k-1} zeros.

The rest of the chapter is organized as follows. Section 3.2 is devoted to proving Proposition 3.1.4 and Theorem 3.1.5. In Section 3.3 we recall some basic definitions and state the results that we need on quadratic forms, namely the number of forms of a given rank, and the number of their zeros. This can be found in Section 2.4 as well, but we prefer to repeat those notions in order to make this section self-contained. In Section 3.4 we use the results of Section 2.4 to derive Theorem 3.1.6. Theorem 3.1.3 is then derived as an almost immediate consequence. We then apply the methods and results of Section 3.2 to conclude the proof of Theorem 3.1.2. Finally, in Section 3.5 we expand Remark 3.1.1, with the purpose of showing that, even though our probabilistic model may appear restrictive, our analysis gives all the ingredients necessary to consider different models.

3.2 Proof of Theorem 3.1.5

In this section we prove Proposition 3.1.4 and Theorem 3.1.5, the weaker version of our main result. We start by introducing some notation and classical results that we shall need.

Recall that, for all non-negative integers $n \geq k$, we define

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \prod_{i=1}^{k} \frac{q^{n-k+i} - 1}{q^i - 1},$$

the Gaussian binomial coefficient, and by convention we define a product with no factors to be equal to 1. As q is assumed to be fixed, it will be suppressed from the notation from here on.

Remark 3.2.1. For all non-negative integers $n \geq k$, we bound

$$\begin{bmatrix} n \\ k \end{bmatrix} \leq 2^k q^{k(n-k)}.$$

This holds as $\begin{bmatrix} n \\ k \end{bmatrix}$ is the product of k terms, and each term is bounded by $2q^{n-k}$.

DEFINITION 3.2.2 (entropy function). The q-ary entropy function is defined by

$$H_q(x) := x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x)$$

for all $0 < x \leq 1 - q^{-1}$.

Again, from here on q will be suppressed from the notation. In particular, all logarithms will be in base q. The following lemma is folklore, see e.g. [37, §2.10.3] for a proof.

LEMMA 3.2.3. *For all $0 < \delta \leq 1 - q^{-1}$ and all integers n, we have*

$$\sum_{i=0}^{\lfloor \delta n \rfloor} \binom{n}{i} (q-1)^i \leq q^{nH(\delta)}.$$

For ease of notation, we define $m \colon \mathbb{N} \to \mathbb{N}$ by $m(k) := k(k+1)/2$. Also, recall that, given a code C, we denote by $C^\perp$ its dual and by $d_{\min}(C)$ its minimum distance.

We prove now Proposition 3.1.4.

PROOF OF PROPOSITION 3.1.4. Let $C \in \mathcal{C}(m(k), k)$. By definition, C admits a generator matrix of the form

$$\left(\begin{array}{ccc|c} 1 & & & g_1 \\ & \ddots & & \vdots \\ & & 1 & g_k \end{array}\right).$$

Note that a uniform random selection of C from $\mathcal{C}(m(k), k)$ induces an independent, uniform random selection of $g_1, \ldots, g_k$ from $\mathbb{F}^{m(k)-k}$. We consider the code

$$\langle g_i g_j : 1 \leq i \leq k/2 < j \leq k \rangle$$

and we define D to be its dual. This is a code of length $k(k-1)/2$ and it is easy to see that

$$d_{\min}((C^2)^\perp) \geq d_{\min}(D).$$

In the following, when D is involved in some probability measure, we implicitly mean that it has the distribution induced by the uniform distribution of C on $\mathcal{C}(m(k), k)$. We remark that this does not necessarily correspond to a uniform distribution on the set of all possible D's.

For any positive integer w and any code C', denote by $\mathcal{E}_w(C')$ the event "there exists a non-zero codeword of C' of weight w". We shall now prove the following statement, which clearly implies the Proposition. There exist constants $c, \widetilde{c} \in \mathbb{R}_{>0}$ such that, for all large enough k,

$$\sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \leq 2^{-\widetilde{c}k}.$$

Note that, for any positive integer w,

$$\Pr(\mathcal{E}_w(D)) = \sum_{\substack{z \in \mathbb{F}^{k(k-1)/2} \\ \text{of weight } w}} \Pr(z \in D). \tag{3.2}$$

So we need to estimate, for all positive integers w and all vectors z of weight w, the probability that z belongs to D.

We do that as follows. For $1 \leq i \leq k/2$, let x_i be the projection of g_i on the support of z. Similarly, for $k/2 < j \leq k$, let y_j be the projection of g_j on the support of z. This defines k vectors in $\mathbb{F}^w$. Moreover, a uniform random selection of C from $\mathcal{C}(m(k), k)$ induces an independent, uniform random selection of the x_i's and the y_j's from $\mathbb{F}^w$. Note now that if we identify z with a vector of $\mathbb{F}^w$, we can define the non-degenerate bilinear form that to any two vectors a, b of $\mathbb{F}^w$ associates the quantity

$$(a|b)_z := (\mathbf{1} \,|\, zab)$$

where $\mathbf{1}$ denotes the all-one vector of $\mathbb{F}^w$ and $(\cdot \,|\, \cdot)$ denotes the standard inner product. Let us say that a and b are *z-orthogonal* if $(a|b)_z = 0$. The purpose of this definition is to note that $z \in D$ if and only if, for all $1 \leq i \leq k/2 < j \leq k$, x_i is z-orthogonal to y_j. In the computation that follows we assume that k is even, thus avoiding cumbersome floor and ceiling notation, and giving us the same number of x_i's and of y_j's, namely $k/2$. It is readily seen that the case k odd can be dealt with in a similar fashion.

For all positive integers $r < k/2$, denote by $\mathcal{H}_r$ the event "$\dim\langle x_i : 1 \leq i \leq k/2\rangle < r$". Conditioning by this event, we have

$$\begin{aligned} \Pr(z \in D) &= \Pr(\mathcal{H}_r) \Pr(z \in D | \mathcal{H}_r) + \\ &\quad + \Pr(\overline{\mathcal{H}}_r) \Pr(z \in D | \overline{\mathcal{H}}_r) \leq \\ &\leq \Pr(\mathcal{H}_r) + \Pr(z \in D | \overline{\mathcal{H}}_r), \end{aligned}$$

for any choice of r. In order to estimate $\Pr(\mathcal{H}_r)$, note that $\dim\langle x_i : 1 \leq i \leq k/2\rangle < r$ if and only if there exists an $(r-1)$-dimensional subspace of $\mathbb{F}^w$ containing all x_i's. The probability that an x_i falls into a given subspace of dimension $r-1$ is $1/q^{w-r+1}$ and since the x_i's are independent random variables,

the probability that all the x_i's fall into the same subspace is $1/q^{(w-r+1)k/2}$. We have therefore,

$$\Pr(\mathcal{H}_r) \leq \begin{bmatrix} w \\ r-1 \end{bmatrix} \frac{1}{q^{\frac{k}{2}(w-r+1)}} \leq \frac{2^r}{q^{(w-r)(k/2-r)}},$$

where we have used the upper bound of Remark 3.2.1 on the number $\begin{bmatrix} w \\ r-1 \end{bmatrix}$ of subspaces of dimension $r-1$.

On the other hand, $z \in D$ if and only if all y_j's are z-orthogonal to the space $\langle x_i : 1 \leq i \leq k/2 \rangle$, which has dimension at least r, under the condition $\overline{\mathcal{H}}_r$. Therefore, using the independence of the random variables y_i,

$$\Pr(z \in D | \overline{\mathcal{H}}_r) \leq \left(\frac{1}{q^r}\right)^{\frac{k}{2}} = \frac{1}{q^{\frac{rk}{2}}}.$$

Now fixing $r := \min\{w/2, k/4\}$ it follows that there exist two positive constants c' and c'' such that

$$\Pr(z \in D) \leq \frac{1}{q^{c'kw}} + \frac{1}{q^{c''k^2}}.$$

Applying this last upper bound to (3.2), we now have

$$\begin{aligned} \Pr(\mathcal{E}_w(D)) &= \sum_{\substack{z \in \mathbb{F}^{k(k-1)/2} \\ \text{of weight } w}} \Pr(z \in D) \leq \\ &\leq \binom{\frac{k(k-1)}{2}}{w} (q-1)^w \left(\frac{1}{q^{c'kw}} + \frac{1}{q^{c''k^2}}\right) \end{aligned}$$

for any positive integer w. Therefore, for any constant c we have

$$\begin{aligned} \sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \leq &\left(\sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} \frac{(q-1)^w}{q^{c'kw}} \right) + \\ &+ \frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} (q-1)^w. \end{aligned} \tag{3.3}$$

We deal with the two terms separately.

We bound the first sum in (3.3) as follows,

$$\begin{aligned} \sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} \frac{(q-1)^w}{q^{c'kw}} &\leq \sum_{w=1}^{cm(k)} \left(\frac{k(k-1)}{2}\right)^w \frac{(q-1)^w}{q^{c'kw}} \leq \\ &\leq \sum_{w=1}^{cm(k)} q^{w(-c'k+o(k))} \leq q^{-c'k+o(k)} \end{aligned}$$

since there are not more than $m(k) = q^{o(k)}$ terms in the sum and none is larger than $q^{-c'k+o(k)}$.

Writing $\binom{\frac{k(k-1)}{2}}{w} \leq \binom{m(k)}{w}$ for any $w \leq cm(k)$, the second term in (3.3) is upper bounded by

$$\frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{m(k)}{w} (q-1)^w.$$

We now set $c \leq 1 - q^{-1}$ and apply Lemma 3.2.3:

$$\frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{m(k)}{w} (q-1)^w \leq \frac{1}{q^{c''k^2}} q^{m(k)H(c)} \leq$$
$$\leq q^{(\frac{1}{2}H(c)-c'')k^2+o(k^2)}.$$

If c is such that $H(c) < 2c''$ we obtain an exponentially small upper bound. Putting everything together, we obtain

$$\sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \leq \frac{1}{q^{c'k+o(k)}} + \frac{1}{q^{\frac{1}{2}(c''-H(c)/2)k^2+o(k^2)}}$$

and the proposition is proved. □

Remark 3.2.4. In the proof of the previous proposition we can take $c'' = \frac{1}{8}$. Therefore the proposition holds for any c with $H(c) < 1/4$. For example, for $q = 2$, $c = 0.041$ suffices.

We can now prove Theorem 3.1.5.

Proof of Theorem 3.1.5. Let $c, \widetilde{c}$ be the constants given by Proposition 3.1.4. Let $n\colon \mathbb{N} \to \mathbb{N}$ be as in the hypothesis of the theorem. Given $C \in \mathcal{C}(n(k), k)$, we create $V \in \mathcal{C}(m(k), k)$ by adding $m(k) - n(k)$ columns to the systematic generator matrix of C. Moreover, if C and all the new columns are chosen uniformly at random from $\mathcal{C}(n(k), k)$ and $\mathbb{F}^k$ respectively then V has the uniform distribution on $\mathcal{C}(m(k), k)$. A codeword in the dual of C^2 gives a codeword in the dual of V^2 of the same weight (padding with zeros). Hence

$$\Pr\left(C^2 \neq \mathbb{F}^{n(k)}\right) \leq \Pr\left(d_{\min}((V^2)^{\perp}) \leq cm(k)\right) \leq 2^{-\widetilde{c}k}$$

by Proposition 3.1.4 and the conclusion follows. □

3.3 Quadratic Forms

In this section we state the results that we need in the proof of our Main Theorem, as well as the definitions necessary to read such results. For a more involved discussion, see Section 2.4, where we include full proofs of the results stated here as well. Even though these can be found, at least partly, in the literature, we have felt it necessary to derive what we need in a unified way.

Throughout this section, let $\mathbb{K}$ be an arbitrary field and let V be a finite dimensional $\mathbb{K}$-vector space.

DEFINITION 3.3.1. A *quadratic form* on V is a map $Q\colon V \to \mathbb{K}$ such that

(i) $Q(\lambda x) = \lambda^2 Q(x)$ for all $x \in V, \lambda \in \mathbb{K}$,
(ii) the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form on V.

We denote by $\mathrm{Quad}(V)$ the $\mathbb{K}$-vector space of all quadratic forms on V. The vector space V, endowed with a quadratic form Q on V, is called a $\mathbb{K}$-*quadratic space*.

Every quadratic form $Q \in \mathrm{Quad}(V)$ defines a bilinear form $\tilde{B}_Q \in \mathrm{Bil}(V)$ by

$$\tilde{B}_Q(x, y) := Q(x + y) - Q(x) - Q(y)$$

for all $x, y \in V$.

DEFINITION 3.3.2. The *radical* of the quadratic space V is the $\mathbb{K}$-vector space

$$\operatorname{Rad} V := \{x \in V : \tilde{B}_Q(x, y) = 0 \text{ for all } y \in V\}.$$

We say that V is *non-degenerate* (as a quadratic space) if $\tilde{B}_Q$ is non-degenerate (as a bilinear form), i.e. if $\operatorname{Rad} V = 0$.

DEFINITION 3.3.3. Let $\operatorname{Rad}^0 V := \{x \in \operatorname{Rad} V : Q(x) = 0\}$. We define the *rank* of Q to be

$$\operatorname{rk} Q := \dim V - \dim \operatorname{Rad}^0 V.$$

REMARK 3.3.4. Note that in the case $\operatorname{char} \mathbb{K} \neq 2$, it holds that $Q(x) = \frac{1}{2}\tilde{B}_Q(x, x)$ and therefore $\operatorname{Rad}^0 V = \operatorname{Rad} V$. Hence in this case (V, Q) is non-degenerate if and only if Q has full rank. This is not the case if $\operatorname{char} \mathbb{K} = 2$.

We are now ready to state the results we need. Theorem 3.3.5 counts the number of zeros of a given quadratic form. Theorem 3.3.6 counts the number of quadratic forms of a given rank.

THEOREM 3.3.5. *Let V be an $\mathbb{F}$-vector space of dimension k, Q a quadratic form on V of rank r. The number of vectors $x \in V$ such that $Q(x) = 0$ is*

a. q^{k-1} if r is odd,

b. either $q^{k-1} - (q-1)q^{k-\frac{r}{2}-1}$ or $q^{k-1} + (q-1)q^{k-\frac{r}{2}-1}$ if r is even.

THEOREM 3.3.6. *For all non-negative integers k, the number $N(k)$ of full-rank quadratic forms on an $\mathbb{F}$-vector space of dimension k is*

$$N(k) = q^{\lfloor \frac{k}{2} \rfloor (\lfloor \frac{k}{2} \rfloor + 1)} \prod_{i=1}^{\lceil \frac{k}{2} \rceil} (q^{2i-1} - 1) =$$

$$= \begin{cases} q^{\frac{k-1}{2}\frac{k+1}{2}} \prod_{i=1}^{\frac{k+1}{2}} (q^{2i-1} - 1) & \text{if } k \text{ is odd,} \\ q^{\frac{k}{2}(\frac{k}{2}+1)} \prod_{i=1}^{\frac{k}{2}} (q^{2i-1} - 1) & \text{if } k \text{ is even.} \end{cases}$$

For all non-negative integers $k \geq r$, the number of rank r quadratic forms on an $\mathbb{F}$-vector space of dimension k is

$$N(k, r) = \begin{bmatrix} k \\ r \end{bmatrix} N(r),$$

where $\begin{bmatrix} k \\ r \end{bmatrix}$ denotes the q-ary Gaussian binomial coefficient.

A more general result implying Theorem 3.3.5 appears in [47, Chapter 6, Section 2].

As to Theorem 3.3.6, the following references need to be mentioned. In [10, Lemma 9.5.9] the number of symmetric bilinear forms of given rank is computed. In the odd characteristic case, as symmetric bilinear forms correspond to quadratic forms and the two notions of rank coincide, this result is equivalent to Theorem 3.3.6. As to the arbitrary characteristic case, [10] refers to [33]. The latter uses the language of association schemes and gives a result that allows to compute (even though this is not explicitly stated) the number $N'(k, s)$ of quadratic forms of rank $r \in \{2s-1, 2s\}$ on an $\mathbb{F}$-vector space of dimension k. This result is slightly weaker than our theorem, as it allows to compute the sum $N(k, 2s-1) + N(k, 2s)$ instead of $N(k, 2s-1)$ and $N(k, 2s)$ separately, but it would be sufficient for the main purpose of this work.

3.4 Proof of Main Theorem 3.1.2

We recall the notation introduced in Section 3.1. Given a code C of length n and dimension k and denoting by $\pi_1, \ldots, \pi_n \in \mathbb{F}^k$ the *columns* of a generator

matrix of C (i.e. a matrix whose *rows* form a basis of C), we define the linear map

$$\begin{array}{rccc} \mathrm{ev}_C\colon & \mathrm{Quad}(\mathbb{F}^k) & \to & \mathbb{F}^n, \\ & Q & \mapsto & (Q(\pi_1),\dots,Q(\pi_n)) \end{array}$$

whose image is C^2.

Recall that we have defined the random variable $X(n,k) := |\ker \mathrm{ev}_C|$, with distribution induced by a uniform random selection of C from $\mathcal{C}(n,k)$. For simplicity, we will write X_k as a shorthand for $X(k(k+1)/2,k)$.

It is convenient to measure "how far" C^2 is from being the full space by defining, for all positive integers $n \geq k$ and all non-negative integers ℓ, the probabilities:

$$p_\ell(n,k) := \Pr(\mathrm{codim}\, C^2 \leq \ell),$$

where C is chosen uniformly at random from $\mathcal{C}(n,k)$. Using this notation, Main Theorem 3.1.2 claims that there exists $\delta \in \mathbb{R}_{>0}$ such that, for all large enough k, $p_0(n(k),k) \geq 1 - 2^{-\delta t(k)}$.

As mentioned before, crucial to the proof of Main Theorem 3.1.2 is to estimate the expected value of $X_k = X(k(k+1)/2,k)$: this is precisely the purpose of Theorem 3.1.6, that states that $\lim_{k\to\infty} \mathbb{E}[X_k] = 2$. We now proceed to its proof.

Proof of Theorem 3.1.6. In Section 3.1 we defined the space S of all quadratic forms vanishing at all unit vectors and we proved that, for all positive integers $m \geq k$,

$$\mathbb{E}[X(m,k)] = \sum_{Q\in S} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \tag{3.1}$$

We now fix a rank threshold, i.e. a fraction of k, and we classify the forms in S accordingly. Precisely, for any $0 < \alpha < 1$ we define

$$\begin{aligned} S^-(\alpha) &:= \{Q \in S : 0 < \mathrm{rk}\, Q \leq \alpha k\}, \\ S^+(\alpha) &:= \{Q \in S : \mathrm{rk}\, Q > \alpha k\}, \end{aligned}$$

so $S = \{0\} \cup S^+(\alpha) \cup S^-(\alpha)$. We observe that

$$|S^-(\alpha)| \leq q^{(-\frac{\alpha^2}{2}+\alpha)k^2+o(k^2)}. \tag{3.4}$$

Indeed, by Theorem 3.3.6 we have

$$|S^-(\alpha)| = \sum_{r=1}^{\alpha k} N(k,r) = \sum_{r=1}^{\alpha k} \begin{bmatrix} k \\ r \end{bmatrix} N(r).$$

We loosely bound $\begin{bmatrix} k \\ r \end{bmatrix} \leq q^{r(k-r+1)}$ and $N(r) \leq |\operatorname{Quad}(\mathbb{F}^r)| = q^{r(r+1)/2}$ and we obtain

$$|S^-(\alpha)| \leq \sum_{r=1}^{\alpha k} q^{r(k-r+1)} q^{r(r+1)/2} = \sum_{r=1}^{\alpha k} q^{-\frac{r^2}{2}+(k+\frac{3}{2})r} \leq$$
$$\leq \alpha k q^{(-\frac{\alpha^2}{2}+\alpha)k^2+\frac{3}{2}\alpha k},$$

proving (3.4). This yields

$$\frac{|S^-(\alpha)|}{|S|} \leq \frac{q^{(-\frac{\alpha^2}{2}+\alpha)k^2+o(k^2)}}{q^{\frac{k(k-1)}{2}}} = q^{-\frac{1}{2}(\alpha-1)^2k^2+o(k^2)}$$

which tends to 0 as $k \to \infty$. Hence, noting that $|S^+(\alpha)| = |S| - 1 - |S^-(\alpha)|$, we obtain

$$\lim_{k\to\infty} \frac{|S^+(\alpha)|}{|S|} = 1. \tag{3.5}$$

In view to using the observations (3.4) and (3.5) on the "density" of $S^+(\alpha)$ and $S^-(\alpha)$ in S, we apply the partition of S to (3.1) and write

$$\mathbb{E}[X(m,k)] =$$
$$= 1 + \sum_{Q\in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} + \sum_{Q\in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \tag{3.6}$$

We now prove that the first sum tends to 1 while the second one (for some suitable value of α) tends to 0.

By Theorem 3.3.5, the number of zeros of any form $Q \in S^+(\alpha)$ is bounded by

$$|Z(Q)| \leq q^{k-1} + (q-1)q^{k-\frac{\alpha k}{2}-1} \leq q^{k-1}\left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)$$

and

$$|Z(Q)| \geq q^{k-1} - (q-1)q^{k-\frac{\alpha k}{2}-1} \geq q^{k-1}\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right).$$

It follows that

$$\frac{1}{q}\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right) \leq \frac{|Z(Q)|}{q^k} \leq \frac{1}{q}\left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)$$

hence

$$\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{m-k} \frac{|S^+(\alpha)|}{q^{m-k}} \leq \sum_{Q\in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} \leq$$
$$\leq \left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{m-k} \frac{|S^+(\alpha)|}{q^{m-k}}.$$

Setting $m = k(k+1)/2$, we get

$$\left(1 - \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{\frac{k(k-1)}{2}} \frac{|S^+(\alpha)|}{|S|} \leq \sum_{Q \in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{\frac{k(k-1)}{2}} \leq$$
$$\leq \left(1 + \frac{1}{q^{\frac{\alpha k}{2}-1}}\right)^{\frac{k(k-1)}{2}} \frac{|S^+(\alpha)|}{|S|}.$$

So the first sum in (3.6) is bounded, from above and from below, by functions which tend to 1 (by (3.5)), hence it tends to 1, too.

We now prove that if we take any $0 < \alpha < 1 - \sqrt{\log_q(2q-1) - 1}$, the last sum in (3.6) tends to 0, which will conclude the proof of the theorem.

By Theorem 3.3.5, all forms $Q \in S^-(\alpha)$ satisfy

$$|Z(Q)| \leq q^{k-1} + (q-1)q^{k-2} = 2q^{k-1} - q^{k-2}.$$

This is trivial for odd rank forms, as they always have exactly q^{k-1} zeros. We get

$$\sum_{Q \in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} \leq \left(\frac{2q-1}{q^2}\right)^{m-k} |S^-(\alpha)|.$$

Setting $m = k(k+1)/2$ and using (3.4) we finally obtain

$$\sum_{Q \in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} \leq$$
$$\leq \left(\frac{2q-1}{q^2}\right)^{\frac{k(k-1)}{2}} q^{(-\frac{\alpha^2}{2}+\alpha)k^2 + o(k^2)} = q^{\mu(\alpha)k^2 + o(k^2)},$$

where $\mu(\alpha) := -\frac{1}{2}(\alpha^2 - 2\alpha + 2 - \log_q(2q-1)) < 0$ under the assumptions on α. Therefore the right hand side tends to 0. This concludes the proof. □

As a first consequence of Theorem 3.1.6, we derive a proof of Theorem 3.1.3.

Proof of Theorem 3.1.3. As before, set $m(k) := k(k+1)/2$. Given a code $C \in \mathcal{C}(n(k), k)$, we obtain a code $C' \in \mathcal{C}(m(k), k)$ puncturing the last $s(k)$ coordinates of C. We define $\mathcal{N}$ to be the event "$\dim C^2 = m(k)$" and, for all $j \in \mathbb{N}$, we define $\mathcal{E}_j$ to be the event "$|\ker \mathrm{ev}_{C'}| = j$". We observe that $\dim C^2 = m(k)$ if and only if $\ker \mathrm{ev}_C = 0$, and this holds if and only if for all nonzero $Q \in \ker \mathrm{ev}_{C'}$ there exists $i \in \{m(k)+1, \ldots, n(k)\}$ such that $Q(\pi_i) \neq 0$.

Hence, if in the case of $\mathcal{E}_j$ we write $\ker \mathrm{ev}_{C'} \setminus \{0\} = \{Q_1, \dots, Q_{j-1}\}$, we have

$$\begin{aligned}
&\Pr(\overline{\mathcal{N}}|\mathcal{E}_j) = \\
&\quad = \Pr\left(\bigcup_{i=1}^{j-1} \left\{Q_i(\pi_{m(k)+1}) = \cdots = Q_i(\pi_{n(k)}) = 0\right\}\right) \leq \\
&\quad \leq \sum_{i=1}^{j-1} \Pr(Q_i(\pi) = 0)^{s(k)},
\end{aligned}$$

for all $j \in \mathbb{N}$, where $\pi \in \mathbb{F}^k$ is chosen uniformly at random. Moreover, for any nonzero quadratic form $Q \in \mathrm{Quad}(\mathbb{F}^k)$,

$$\Pr(Q(\pi) = 0) \leq \frac{q^{k-1} + (q-1)q^{k-2}}{q^k} = \frac{2q-1}{q^2}.$$

Note that $(2q-1)/q^2$ is a constant strictly smaller than 1. It follows that

$$\Pr(\overline{\mathcal{N}}|\mathcal{E}_j) \leq \sum_{i=1}^{j-1} \left(\frac{2q-1}{q^2}\right)^{s(k)} = (j-1)\left(\frac{2q-1}{q^2}\right)^{s(k)}.$$

Applying the law of total probability to $\Pr(\overline{\mathcal{N}})$ together with the above observations we finally have

$$\begin{aligned}
\Pr(\overline{\mathcal{N}}) &= \sum_{j \in \mathbb{N}} \Pr(\mathcal{E}_j) \Pr(\overline{\mathcal{N}}|\mathcal{E}_j) \leq \\
&\leq \left(\frac{2q-1}{q^2}\right)^{s(k)} \sum_{j \in \mathbb{N}} \Pr(\mathcal{E}_j)(j-1) = \\
&= \left(\frac{2q-1}{q^2}\right)^{s(k)} (\mathbb{E}[X_k] - 1).
\end{aligned}$$

The conclusion follows by Theorem 3.1.6. □

Next, we derive from the estimation of the expectation of X_k given by Theorem 3.1.6, a lower bound for the probability of X_k being smaller than some fixed constant. Precisely, the following holds.

PROPOSITION 3.4.1. *For any $\varepsilon > 0$ there exists $k_\varepsilon \in \mathbb{N}$ such that, for all $k \geq k_\varepsilon$, for every non-negative integer ℓ we have*

$$\Pr\left(\dim C^2 \geq \frac{k(k+1)}{2} - \ell\right) \geq 1 - \frac{2+\varepsilon}{q^{\ell+1}},$$

where C is chosen uniformly at random from $\mathcal{C}(k(k+1)/2, k)$.

PROOF. We apply Markov's inequality to the random variable X_k, namely:

$$\Pr(X_k < \delta) \geq 1 - \frac{\mathbb{E}[X_k]}{\delta} \tag{3.7}$$

for any $\delta > 0$. By Theorem 3.1.6 there exists $k_\varepsilon \in \mathbb{N}$ such that, for all $k \geq k_\varepsilon$, we have $\mathbb{E}[X_k] \leq 2 + \varepsilon$, hence for any $\delta > 0$, (3.7) gives

$$\Pr(X_k < \delta) \geq 1 - \frac{2 + \varepsilon}{\delta}$$

if $k \geq k_\varepsilon$. Now setting $\delta = q^{\ell+1}$ and noting that $\Pr(X_k < q^{\ell+1}) = \Pr(\dim C^2 \geq k(k+1)/2 - \ell)$ we conclude. □

Proposition 3.4.1 together with Proposition 3.1.4 allow us to conclude the proof of Main Theorem 3.1.2.

PROOF OF MAIN THEOREM 3.1.2.

Let $k \leq n < m := k(k+1)/2$ be positive integers, and let $t := m - n$. We use a puncturing argument. The key observation is that a random code of length n can be obtained by first choosing a random code of length m and then deleting $m - n$ random coordinates. We shall look closely at the probability that non-zero words survive in the dual of the punctured code.

Precisely, consider a uniform random code $C \in \mathcal{C}(m, k)$: let $C' \in \mathcal{C}(n, k)$ be obtained from C by removing t random coordinates among the last $m-k$. Let these t coordinates be chosen uniformly, independently of C.

In order to estimate $p_0(n, k)$, we define the following events. Call $\mathcal{E}$ the event studied in Proposition 3.1.4, namely $d_{\min}((C^2)^\perp) \leq cm$ where c is the constant of Proposition 3.1.4. For all non-negative integers i, call $\mathcal{E}_i$ the event $\operatorname{codim} C^2 = i$. As before, bar denotes the complement event.

For any positive integer ℓ we have

$$p_0(n, k) \geq \sum_{i=1}^{\ell} \Pr(\overline{\mathcal{E}} \cap \mathcal{E}_i) \Pr(\operatorname{codim}(C')^2 = 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i). \tag{3.8}$$

Let C_0 be a fixed code of length m and suppose x is a codeword of $C_0^\perp$ of weight w. Puncture C_0 by removing t random coordinates among the last $m - k$. The probability that none of the random t coordinates belong to the support of x is at most

$$\frac{\binom{m-w}{t}}{\binom{m-k}{t}} \tag{3.9}$$

(and actually equal to (3.9) if the support of x contains the first k coordinates). If the dual code $C_0^\perp$ contains exactly $q^i - 1$ non-zero codewords all of which

have weight at least cm, then the probability that the t random coordinates miss the support of at least one codeword of $C_0^\perp$ is, by (3.9) and the union bound, bounded from above by

$$(q^i - 1)\frac{\binom{m-cm}{t}}{\binom{m-k}{t}}.$$

Now observing that a non-zero codeword in $((C')^2)^\perp$ exists only if there exists a non-zero codeword in $(C^2)^\perp$ with support disjoint from the chosen t coordinates, we obtain that, for all $i = 1, \ldots, \ell$,

$$\begin{aligned}\Pr(\operatorname{codim}(C')^2 \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) &\leq (q^i - 1)\frac{\binom{m-cm}{t}}{\binom{m-k}{t}} \leq \\ &\leq q^\ell \, \frac{\binom{m-cm}{t}}{\binom{m-k}{t}}.\end{aligned}$$

We bound the fraction as follows:

$$\begin{aligned}\frac{\binom{m-cm}{t}}{\binom{m-k}{t}} &= \frac{(m-cm)\cdots(m-cm-t+1)}{(m-k)\cdots(m-k-t+1)} \leq \\ &\leq \left(\frac{m-cm}{m-k}\right)^t = (1-c)^t\left(\frac{k+1}{k-1}\right)^t\end{aligned}$$

from which we obtain

$$\Pr(\operatorname{codim}(C')^2 \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) \leq q^{\ell + t(\log(1-c) + \log\frac{k+1}{k-1})}.$$

Since $\log\frac{k+1}{k-1}$ goes to zero when k goes to infinity and $\log(1-c)$ is negative, by fixing $\ell = \alpha t$ we get the existence of a positive β such that, for any k large enough,

$$\Pr(\operatorname{codim}(C')^2 \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) \leq q^{-\beta t}. \tag{3.10}$$

Now note that by the union bound

$$\begin{aligned}\Pr(\overline{\mathcal{E}} \cap \mathcal{E}_i) &= 1 - \Pr(\mathcal{E} \cup \overline{\mathcal{E}}_i) \geq 1 - \Pr(\mathcal{E}) - \Pr(\overline{\mathcal{E}}_i) = \\ &= \Pr(\mathcal{E}_i) - \Pr(\mathcal{E}).\end{aligned}$$

Therefore, (3.10) with (3.8) give

$$\begin{aligned}p_0(n,k) &\geq (1 - q^{-\beta t})\sum_{i=1}^{\ell}(\Pr(\mathcal{E}_i) - \Pr(\mathcal{E})) \\ &\geq (1 - q^{-\beta t})(1 - \Pr(\dim C^2 \leq m - \ell) - \ell \Pr(\mathcal{E})).\end{aligned} \tag{3.11}$$

Proposition 3.4.1 gives us, since $\ell = \alpha t$, that $\Pr(\dim C^2 \leq m - \ell) \leq 2^{\beta' t}$ for a constant β'. Proposition 3.1.4 gives us, since $\ell \leq k^2$, that $\ell \Pr(\mathcal{E}) \leq 2^{-\gamma k}$ for some constant γ. From (3.11) we therefore get

$$p_0(n,k) \geq 1 - 2^{-\gamma k} - 2^{-\delta t}.$$

for constants γ and δ. □

3.5 Changing the Probabilistic Model

In this section we expand Remark 3.1.1, with the purpose of showing that, even though our probabilistic model may appear restrictive, our analysis gives all the ingredients necessary to consider different models.

For all positive integers $n \geq k$ we define the following two families of codes. Let $\mathcal{A}(n,k)$ be the family of all codes of length n and dimension at most k with the following distribution: choose a $k \times n$ matrix A uniformly at random and pick the code spanned by the rows of A. Let $\mathcal{U}(n,k)$ be the family of all codes of length n and dimension k, with uniform distribution. Note that it is equivalent to a uniform random choice of a $k \times n$ full-rank matrix, as each such a code has the same number of bases, hence the same number of generator matrices.

We first argue that all our results hold if we replace $\mathcal{C}(n,k)$ with $\mathcal{A}(n,k)$. The two probability distributions are subtly different and it is not easy to derive results for $\mathcal{A}(n,k)$ from the results for $\mathcal{C}(n,k)$ seen as "black boxes". However, if we go over the proofs of our theorems, we see that they will carry over to $\mathcal{A}(n,k)$ with no significant change of strategy. Specifically, in the proof of Theorem 3.1.6, one will replace the study of the quantity $\sum_{Q \in S} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}$ in (3.1) by

$$\sum_{Q} \left(\frac{|Z(Q)|}{q^k}\right)^{m}$$

where Q ranges over all quadratic forms on k variables. The quantity to be studied is simply the expected number of quadratic forms that vanish on m random values. Going over the proof one will end up with exactly the same expected value. We sum over a space with q^k more quadratic forms but replace probabilities of the form $(|Z(Q)|/q^k)^{m-k}$ by $(|Z(Q)|/q^k)^m$ which behaves like $1/q^k$ times less. Regarding the probabilistic analysis that proves Proposition 3.1.4, we see that it is virtually unchanged when the first k coordinates become random. Also the puncturing argument that proves Theorem 3.1.2 sees only the punctured coordinates being chosen from $\{1, \ldots, m\}$ rather than from $\{k+1, \ldots, m\}$.

Regarding the second distribution $\mathcal{U}(n,k)$, we argue differently and relate it to $\mathcal{A}(n,k)$. From here on n and k will be suppressed from the notation, since they are assumed to be fixed. We add indices as $C \leftarrow \mathcal{A}$ or $C \leftarrow \mathcal{U}$ to our probability notation to make the probabilistic model explicit. Observe that for any fixed code C_0 of dimension k, we have

$$\Pr_{C \leftarrow \mathcal{A}}(C = C_0 | \dim C = k) = \Pr_{C \leftarrow \mathcal{U}}(C = C_0).$$

It follows that, if $\mathcal{P}(C)$ denotes a property that a code C may have,

$$\Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) = \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C) | \dim C = k).$$

We deduce from this observation that:

LEMMA 3.5.1. *For any property $\mathcal{P}$,*

$$\Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) \geq \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C)) - \Pr_{C \leftarrow \mathcal{A}}(\dim C < k).$$

PROOF. We have

$$\begin{aligned}\Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C)) &= \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C) | \dim C = k) \Pr_{C \leftarrow \mathcal{A}}(\dim C = k) + \\ &+ \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C) | \dim C < k) \Pr_{C \leftarrow \mathcal{A}}(\dim C < k) \leq \\ &\leq \Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) + \Pr_{C \leftarrow \mathcal{A}}(\dim C < k).\end{aligned}$$

□

Next, recall this well-known result on random matrices:

$$\Pr_{C \leftarrow \mathcal{A}}(\dim C < k) \leq \frac{1}{q^{n-k}}.$$

Together with Lemma 3.5.1 this gives us:

$$\Pr_{D \leftarrow \mathcal{U}}(\mathcal{P}(D)) \geq \Pr_{C \leftarrow \mathcal{A}}(\mathcal{P}(C)) - \frac{1}{q^{n-k}}.$$

We can now apply this to versions of our Theorems for $\mathcal{A}(n,k)$. In particular, our main Theorem 3.1.2 will read, under the uniform distribution $\mathcal{U}(n,k)$, that there exist some positive real constants γ, δ such that

$$\Pr_{C \leftarrow \mathcal{U}}(C^2 = \mathbb{F}^{n(k)}) \geq 1 - 2^{-\gamma k} - 2^{-\delta t(k)} - \frac{1}{q^{n(k)-k}}.$$

This simple argument is enough to recover an asymptotically optimal version of our main result for the uniform distribution, except for code rates that tend to 1.