Squares of random linear codes

Ignacio Cascudo[*], Ronald Cramer[†], Diego Mirandola[‡], Gilles Zémor[§]

December 23, 2014

Abstract

Given a linear code C, one can define the d-th power of C as the span of all componentwise products of d elements of C. A power of C may quickly fill the whole space. 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 $\frac{1}{2}k^2$ or smaller. Moreover, the convergence speed is exponential if the difference $k(k+1)/2 - n$ 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.

1 Introduction

Let K be a field and denote by $*$ the coordinatewise product of vectors of K^n, so that:

$$(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

When V and W are subspaces of K^n let us denote similarly by $V * W$ the subspace generated by all $*$-products of vectors of V and W, i.e. $V * W := \langle x * y : x \in V, y \in W \rangle$. We also use the shorthand $V^{*1} = V$, $V^{*2} := V * V$ and define inductively the powers of V, $V^{*d} := V * V^{*(d-1)}$ for $d > 1$.

When $K = \mathbb{F}_q$ is a finite field and C is a q-ary linear code, asking what are the possible parameters of the linear code C^{*2} arises in a number of different contexts and has attracted a lot of attention recently. Possibly one of the earliest appearances of this question in coding theory goes back to [27] where it is relevant to the notion of error-locating pairs used for algebraic decoding.

"Products" and "squares" of codes are the primary focus of work on secret sharing [8, 3, 4, 5] and its application to secure multi-party computation [14]. To share a secret vector $s \in \mathbb{F}_q^k$ among n players using a linear code $C \subseteq \mathbb{F}_q^{n+k}$, one standardly chooses a random codeword with some fixed k-tuple of coordinates equal to s: the other coordinates are the shares. When two secrets s and t are shared in this way, summing coordinatewise the share vectors gives naturally a share vector of the coordinatewise sum $s + t$ of the secrets.

[*]Aarhus University, Denmark. Research partially carried out while the author was at CWI Amsterdam, The Netherlands. Email: `ignacio@cs.au.dk`.

[†]CWI Amsterdam and Mathematical Institute, Leiden University, The Netherlands. Email: `cramer@cwi.nl`.

[‡]CWI Amsterdam and Mathematical Institute, Leiden University, The Netherlands, and Mathematical Institute, Bordeaux University, France. Email: `diego@cwi.nl`.

[§]Mathematical Institute, Bordeaux University, France. Email: `zemor@math.u-bordeaux.fr`.

Material in this paper was presented at the "Mathematics of Information-Theoretic Cryptography" workshop, Leiden, May 13-25 2013 and at the "Algebra, Codes and Networks" workshop, Bordeaux, June 16-20 2014.

When one considers the $*$-product of the share vectors, one obtains a share of the product $s * t$, but for a different secret-sharing scheme, namely that associated to the $*$-product code C^{*2}. Since the parameters of a code are relevant to the associated secret-sharing scheme, studying the parameters of C^{*2} becomes important. More precisely, interest is focused on families of linear codes $(C_i)_{i\in\mathbb{N}}$ of unbounded length, such that the families of the dual codes $(C_i^{\perp})_{i\in\mathbb{N}}$ and of the squares $(C_i^{*2})_{i\in\mathbb{N}}$ are asymptotically good. A family of codes satisfying this property yields linear secret-sharing schemes on arbitrarily many players with good parameters (privacy, reconstruction, multiplication) [3]. Such families were first constructed, over almost all finite fields, in [8] using techniques from algebraic geometry (asymptotically good towers of algebraic function fields). This work was subsequently extended in [3, 4] involving novel algebraic-geometric ideas. We remark that no elementary construction is known so far.

Secret sharing has as main motivation and application secure multi-party computation (MPC). Any linear secret-sharing scheme yields an MPC protocol [14], and the family of all malicious coalitions of players the protocol can tolerate depends on the parameters of the LSSS listed above.

Besides its original application, the result of [8] played a central role in the paper [21] on the "secure MPC in the head" paradigm: here secure MPC is used as an abstract primitive for efficient two-party cryptography. Among other subsequent fundamental results, let us mention that asymptotically good codes whose dual and square are also asymptotically good are an essential ingredient in the recent constructions of efficient unconditionally secure oblivious transfer protocols from noisy channels [20, 26].

The same issue is also pertinent to algebraic complexity theory: there one wishes to express multiplication in the extension field $\mathbb{F}_{q^m}$ through a bilinear algorithm involving a small number of multiplications in $\mathbb{F}_q$, see [1, 7, 28, 6] for recent developments.

Motivated in part by these applications, asymptotically good codes whose squares are also asymptotically good (and we impose no conditions on the duals) have been shown to exist for all finite fields in [29]. This construction carefully combines algebraic geometric codes that have asymptotically good higher powers, which can be constructed over large enough finite fields, with a field descent concatenation technique. Again, no elementary construction is known in this case.

Powers of linear codes also turn up in lattice constructions, as was recently elaborated on in [22]. If C is a binary linear code, then, abusing notation by identifying C with its natural lift in $\mathbb{Z}^n$, the most natural lattice construction from C is $\Lambda = C + 2\mathbb{Z}^n$ (construction A in Conway and Sloane's terminology [10]). The minimum Euclidean norm of a lattice vector is then $\min(\sqrt{d_{\min}(C)}, 2)$, where $d_{\min}(C)$ is the minimum Hamming distance of the code C. If one wishes to generate from the code C a lattice with larger Euclidean distance, one may try to construct the lattice generated by $C + 4\mathbb{Z}^n$: a close look shows that this lattice actually equals

$$C + 2C^{*2} + 4\mathbb{Z}^n$$

and its minimum Euclidean norm is

$$\min\left(\sqrt{d_{\min}(C)}, 2\sqrt{d_{\min}(C^{*2})}, 4\right).$$

One may generalize the construction to $C + 2C^{*^2} + 4C^{*4} + 8\mathbb{Z}^n$ and so on, or more generally to (construction D [10]) $C_0 + 2C_1 + \cdots + 2^{\ell-1}C_{\ell-1} + 2^{\ell}\mathbb{Z}^n$, which is a lattice if and only if $C_j^{*2} \subset C_{j+1}$, a fact not usually explicitely stated in the literature.

Finally, there has been some recent use of $*$-squares in the cryptanalysis of variants of the McEliece cryptosystem [18, 11, 12, 13]. The idea that is exploited is that Goppa codes have a $*$-square that has a substantially smaller dimension than typical random linear codes: this allows to build a distinguisher which can be used to attack the cryptosystem.

The motivation for a systematic code-theoretic study of $*$-squares is therefore quite strong. For a wide collection of results on the topic see [30] and references therein. With a view to contribute to such an endeavour, our concern in the present work is with the dimension of squares of random linear codes: we see that this is especially relevant in particular to the last application to cryptanalysis.

Since a generating set of vectors for the square of a code C 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 block length $n < k(k+1)/2$ has a $*$-square which fills up the whole space, i.e. $C^{*2} = \mathbb{F}_q^n$. 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 $\mathbb{F}_q^n$ goes to zero. We also study the speed of convergence, which is exponential if the difference $k(k+1)/2 - n$ 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 blocklength 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 [18] 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 [18] 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 next section we describe our results precisely and give an overview of our proofs and the structure of the paper.

2 Overview

Throughout this paper, q denotes a fixed prime power and $\mathbb{F}_q$ a field with q elements.

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 $[n,k]$-codes over $\mathbb{F}_q$ 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 2.1. *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 6 we shall argue however that our results are not altered significantly under these alternative probability distributions.

Our main result is:

MAIN THEOREM 2.2. *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,*

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

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 2.3. *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 2.2 and 2.3 are not quite symmetrical. In particular the term $2^{-\gamma k}$ is absent from the statement of Theorem 2.3 but can not be avoided in Theorem 2.2: 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 $\mathbb{F}_q^{n(k)}$. The two theorems will not require exactly the same methods and Theorem 2.2 will need more work than Theorem 2.3. We shall deal with them separately.

Our first step towards establishing Theorem 2.2 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 2.4. *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 2.2.

THEOREM 2.5. *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,

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

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 2.2, we need some additional ingredients.

Given an $[n,k]$-code C and denoting by $\pi_1,\dots,\pi_n \in \mathbb{F}_q^k$ the columns of a generator matrix of C, define the linear map

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

where $\mathrm{Quad}(\mathbb{F}_q^k)$ denotes the vector space of quadratic forms on $\mathbb{F}_q^k$. Then one can see that the image of ev_C does not depend on the choice of a generator matrix of C, and it is equal to C^{*2}, see [30, §1.31]. In particular, $C^{*2} = \mathbb{F}_q^n$ if and only if ev_C is surjective. Moreover, by basic linear algebra $C^{*2} = \mathbb{F}_q^n$ if and only if

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

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 2.6. *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 2.4, will enable us to conclude the proof of Theorem 2.2 when the block length n is well separated from $k(k+1)/2$.

As a by-product, Theorem 2.6 also enables us to deal easily with the case when $n \geq k(k+1)/2$. Theorem 2.3 will follow as a straightforward consequence.

We conclude this overview by giving a rough idea of the proof of Theorem 2.6. 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 precisely in Section 4 and a detailed proof is provided in the Appendix.

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

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

where we can assume that, for $i = 1,\dots,k$, $\pi_i = e_i$ is the i-th unit vector while $\pi_{k+1},\dots,\pi_m \in \mathbb{F}_q^k$ have independent, uniform distribution over $\mathbb{F}_q^k$, 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

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

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

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

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

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

Now if it were true (it is not) that all non-zero quadratic forms on $\mathbb{F}_q^k$ 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 2.6. However, even though it is false that all non-zero quadratic forms on $\mathbb{F}_q^k$ 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 $\mathbb{F}_q^k$ have q^{k-1} zeros.

The rest of the paper is organized as follows. Section 3 is devoted to proving Proposition 2.4 and Theorem 2.5. Section 4 states the results that we need on quadratic forms, namely the number of forms of a given rank, and the number of their zeros. Some of these results can be found in the literature, but only in part, and we have felt it useful to derive what we need in a unified way: this is provided in the Appendix so as not to disrupt the flow of the paper. Finally, in Section 5 we use the results of Section 4 to derive Theorem 2.6. Theorem 2.3 is then derived as an almost immediate consequence. We then apply the methods and results of Section 3 to conclude the proof of Theorem 2.2.

3 Proof of Theorem 2.5

In this section we prove Proposition 2.4 and Theorem 2.5, the weaker version of our main result. We start by introducing some notation and classical results that we shall need.

Definition 3.1 (Gaussian binomial coefficient). *For all non-negative integers $n \geq k$, we define the q-ary Gaussian binomial coefficient to be*

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

By convention, we define a product with no factors to be equal to 1. This is the case if $k = 0$. As q is assumed to be fixed, it will be suppressed from the notation from here on. It is well-known that the Gaussian binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ equals the number of k-dimensional subspaces of any $\mathbb{F}_q$-vector space of dimension n.

Remark 3.2. *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 3.3 (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. [19, §2.10.3] for a proof.

Lemma 3.4. *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 2.4.

Proof of Proposition 2.4. 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 $\mathbb{F}_q^{m(k)-k}$. 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,

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

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 $\mathbb{F}_q^w$. 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 $\mathbb{F}_q^w$. Note now that if we identify z with a vector of $\mathbb{F}_q^w$, we can define the non-degenerate bilinear form that to any two vectors a, b of $\mathbb{F}_q^w$ associates the quantity

$$(a|b)_z := \mathbf{1} \cdot (z * a * b)$$

where $\mathbf{1}$ denotes the all-one vector of $\mathbb{F}_q^w$ and $\cdot$ 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 $1 \le i \le k/2 < j \le k$, 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 "$\dim\langle x_i : 1 \le i \le k/2\rangle < r$". Conditioning by this event, we have

$$\Pr(z \in D) = \Pr(\mathcal{H}_r)\Pr(z \in D|\mathcal{H}_r) + \Pr(\overline{\mathcal{H}}_r)\Pr(z \in D|\overline{\mathcal{H}}_r) \le \Pr(\mathcal{H}_r) + \Pr(z \in D|\overline{\mathcal{H}}_r),$$

for any choice of r. In order to estimate $\Pr(\mathcal{H}_r)$, note that $\dim\langle x_i : 1 \le i \le k/2\rangle < r$ if and only if there exists an $(r-1)$-dimensional subspace of $\mathbb{F}_q^w$ 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,

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

where we have used the upper bound of Remark 3.2 on the number $\left[{w \atop r-1}\right]$ 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 $\langle x_i : 1 \le i \le k/2\rangle$, which has dimension at least r, under the condition $\overline{\mathcal{H}}_r$. Therefore, using the independence of the random variables y_i,

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

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

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

Applying this last upper bound to (2), we now have

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

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

$$\sum_{w=1}^{cm(k)} \Pr(\mathcal{E}_w(D)) \le \left(\sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w} \frac{(q-1)^w}{q^{c'kw}}\right) + \frac{1}{q^{c''k^2}} \sum_{w=1}^{cm(k)} \binom{\frac{k(k-1)}{2}}{w}(q-1)^w. \qquad (3)$$

We deal with the two terms separately.

We bound the first sum in (3) as follows,

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

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) 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 3.4:

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

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 3.5. *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 2.5.

Proof of Theorem 2.5. Let $c, \widetilde{c}$ be the constants given by Proposition 2.4. 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 $\mathbb{F}_q^k$ 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

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

by Proposition 2.4 and the conclusion follows. △

4 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 Appendix A, 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 K be an arbitrary field.

Definition 4.1 (quadratic form). *Let V be a finite dimensional K-vector space. A quadratic form on V is a map $Q\colon V \to K$ such that*

(i) $Q(\lambda x) = \lambda^2 Q(x)$ *for all* $x \in V, \lambda \in K$,

(ii) the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ *is a bilinear form on* V.

The K*-vector space of all quadratic forms on* V *is denoted by* $\mathrm{Quad}(V)$. *A pair* (V, Q) *where* V *is a finite dimensional* K*-vector space and* Q *is a quadratic form on* V *is called a* K*-quadratic space.*

Let (V, Q) be a K-quadratic space. With abuse of terminology, from here on we call V a quadratic space, omitting the quadratic form Q which defines the quadratic space structure on the vector space V. We define a symmetric bilinear form $\tilde{B}_Q$ on V by

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

for all $x, y \in V$.

Definition 4.2 (radical). *The radical of the quadratic space* V *is the* 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 4.3 (rank). *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 4.4. *Note that in the case* $\operatorname{char} K \neq 2$, *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. In the appendix we show that this is not the case if* $\operatorname{char} K = 2$.

We are now ready to state the results we need. Theorem 4.5 counts the number of zeros of a given quadratic form. Theorem 4.6 counts the number of quadratic forms of a given rank.

Theorem 4.5. *Let* (V, Q) *be an* $\mathbb{F}_q$*-quadratic space, set* $k := \dim V$ *and* $r := \operatorname{rk} Q$. *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 4.6. *For all non-negative integers* k, *the number of full-rank quadratic forms on an* $\mathbb{F}_q$*-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* $\mathbb{F}_q$*-vector space of dimension* k *is*

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

where $\left[\begin{smallmatrix} k \\ r \end{smallmatrix}\right]$ *denotes the* q*-ary Gaussian binomial coefficient (see Definition 3.1).*

A more general result implying Theorem 4.5 appears in [24, Chapter 6, Section 2].

As to Theorem 4.6, the following references need to be mentioned. In [2, 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 4.6. As to the arbitrary characteristic case, [2] refers to [17]. 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 $\mathbb{F}_q$-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.

5 Proof of Main Theorem 2.2

We recall the notation introduced in Section 2. Given an $[n,k]$-code C and denoting by $\pi_1,\dots,\pi_n \in \mathbb{F}_q^k$ the *columns* of a generator matrix of C (i.e. a matrix whose *rows* form a basis of C), we define the linear map

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

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:

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

where C is chosen uniformly at random from $\mathcal{C}(n,k)$. Using this notation, Main Theorem 2.2 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 2.2 is to estimate the expected value of $X_k = X(k(k+1)/2,k)$: this is precisely the purpose of Theorem 2.6, that states that $\lim_{k\to\infty} \mathbb{E}[X_k] = 2$. We now proceed to its proof.

Proof of Theorem 2.6. In Section 2 we defined the space S of all quadratic forms vanishing at all unit vectors and we proved that, for all positive integers $m \geq k$,

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

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

$$S^-(\alpha) := \{Q \in S : 0 < \operatorname{rk} Q \leq \alpha k\}, \quad S^+(\alpha) := \{Q \in S : \operatorname{rk} Q > \alpha k\},$$

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

$$|S^-(\alpha)| \leq q^{(-\frac{\alpha^2}{2}+\alpha)k^2+o(k^2)}. \tag{4}$$

Indeed, by Theorem 4.6 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 $\begin{bmatrix} k \\ r \end{bmatrix} \le q^{r(k-r+1)}$ and $N(r) \le |\operatorname{Quad}(\mathbb{F}_q^r)| = q^{r(r+1)/2}$ and we obtain

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

proving (4). This yields

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

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

$$\lim_{k\to\infty} \frac{|S^+(\alpha)|}{|S|} = 1. \tag{5}$$

In view to using the observations (4) and (5) on the "density" of $S^+(\alpha)$ and $S^-(\alpha)$ in S, we apply the partition of S to (1) and write

$$\mathbb{E}[X(m,k)] = 1 + \sum_{Q\in S^+(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k} + \sum_{Q\in S^-(\alpha)} \left(\frac{|Z(Q)|}{q^k}\right)^{m-k}. \tag{6}$$

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

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

and

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

It follows that

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

hence

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

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

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

So the first sum in (6) is bounded, from above and from below, by functions which tend to 1 (by (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 (6) tends to 0, which will conclude the proof of the theorem.

By Theorem 4.5, 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 (4) we finally obtain

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

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 2.6, we derive a proof of Theorem 2.3.

Proof of Theorem 2.3. 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 $\ker \mathrm{ev}_{C'} \setminus \{0\} = \{Q_1, \ldots, Q_{j-1}\}$, we have

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

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

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

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

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

The conclusion follows by Theorem 2.6. △

Next, we derive from the estimation of the expectation of X_k given by Theorem 2.6, a lower bound for the probability of X_k being smaller than some fixed constant. Precisely, the following holds.

Proposition 5.1. *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:

$$\Pr(X_k < \delta) \geq 1 - \frac{\mathbb{E}[X_k]}{\delta} \tag{7}$$

for any $\delta > 0$. By Theorem 2.6 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 $\delta > 0$, (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 5.1 together with Proposition 2.4 allow us to conclude the proof of Main Theorem 2.2.

Proof of Main Theorem 2.2. 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 2.4, namely $d_{\min}((C^{*2})^\perp) \leq cm$ where c is the constant of Proposition 2.4. 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

$$p_0(n, k) \geq \sum_{i=1}^{\ell} \Pr(\overline{\mathcal{E}} \cap \mathcal{E}_i) \Pr(\operatorname{codim}(C')^{*2} = 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i). \tag{8}$$

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

$$\frac{\binom{m-w}{t}}{\binom{m-k}{t}} \tag{9}$$

(and actually equal to (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 (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 $i = 1, \ldots, \ell$,

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

We bound the fraction as follows:

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

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,

$$\Pr(\operatorname{codim}(C')^{*2} \neq 0 | \overline{\mathcal{E}} \cap \mathcal{E}_i) \leq q^{-\beta t}. \tag{10}$$

Now note that by the union bound

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

Therefore, (10) with (8) give

$$\begin{aligned} p_0(n,k) &\geq (1 - q^{-\beta t}) \sum_{i=1}^{\ell} (\Pr(\mathcal{E}_i) - \Pr(\mathcal{E})) \\ &\geq (1 - q^{-\beta t})(1 - \Pr(\dim C^{*2} \leq m - \ell) - \ell \Pr(\mathcal{E})). \end{aligned} \tag{11}$$

Proposition 5.1 gives us, since $\ell = \alpha t$, that $\Pr(\dim C^{*2} \leq m - \ell) \leq 2^{\beta' t}$ for a constant β'. Proposition 2.4 gives us, since $\ell \leq k^2$, that $\ell \Pr(\mathcal{E}) \leq 2^{-\gamma k}$ for some constant γ. From (11) we therefore get

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

for constants γ and δ. △

6 Changing the probabilistic model

In this section we expand Remark 2.1, 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 2.6, one will replace the study of the quantity $\sum_{Q\in S}\left(\frac{|Z(Q)|}{q^k}\right)^{m-k}$ in (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 2.4, we see that it is virtually unchanged when the first k coordinates become random. Also the puncturing argument that proves Theorem 2.2 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 6.1. *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 6.1 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 2.2 will read, under the uniform distribution $\mathcal{U}(n,k)$, that there exist some positive real constants γ,δ such that

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

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.

References

[1] S. Ballet, J. Pieltant. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. *J. Complexity*, Vol. 27, pp. 230-245, 2011.

[2] A. E. Brouwer, A. M. Cohen, A. Neumaier. *Distance-Regular Graphs.* Springer Verlag, 1989.

[3] I. Cascudo, H. Chen, R. Cramer, C. Xing. Asymptotically good ideal linear secret sharing with strong multiplication over *any* finite field. *Proc. of 29th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5677, pp. 466-486, August 2009.

[4] I. Cascudo, R. Cramer, C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. *Proc. of 31st Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 6842, pp. 685-705, August 2011.

[5] I. Cascudo, R. Cramer, C. Xing. The Arithmetic Codex. IACR Cryptology ePrint Archive 2012: 388 (2012). A 5-page summary also appeared in Proceedings of IEEE Information Theory Workshop (ITW) 2012.

[6] I. Cascudo, R. Cramer, C. Xing. Torsion Limits and Riemann-Roch Systems for Function Fields and Applications. *IEEE Trans. Inform. Theory*, Vol. 60, pp. 3871-3888, July 2014.

[7] I. Cascudo, R. Cramer, C. Xing, A. Yang. Asymptotic bound for multiplication complexity in the extensions of small finite fields. *IEEE Trans. Inform. Theory*, Vol. 58, pp. 4930-4935, July 2012.

[8] H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Proc. of 26th Annual IACR CRYPTO*, Springer Verlag LNCS, vol. 4117, pp. 516-531, Santa Barbara, Ca., USA, August 2006.

[9] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Proc. of 27th Annual IACR EUROCRYPT*, Barcelona, Spain, Springer Verlag LNCS, vol. 4515, pp. 291-310, 2007.

[10] J. H. Conway, N. J. A. Sloane. *Sphere packings, lattices and groups.* Springer, 1999 (3rd Edition).

[11] A. Couvreur, P. Gaborit, V. Gauthier, A. Otmani, J.-P. Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Presented at WCC 2013, to appear in *Des. Codes Crypto.* Preprint: `http://arxiv.org/abs/1307.6458`

[12] A. Couvreur, A. Otmani, J.-P. Tillich. New Identities Relating Wild Goppa Codes. Preprint: `http://arxiv.org/abs/1310.3202`

[13] A. Couvreur, A. Otmani, J.-P. Tillich. Polynomial Time Attack on Wild McEliece Over Quadratic Extensions. *Proceedings of 33rd Annual IACR EUROCRYPT*, Copenhagen, Denmark, Springer Verlag LNCS, vol. 8441, pp. 17-39, May 2014.

[14] R. Cramer, I. Damgaard, U. Maurer. General secure multi-party computation from any linear secret sharing scheme. *Proceedings of 19th Annual IACR EUROCRYPT*, Brugge, Belgium, Springer Verlag LNCS, vol. 1807, pp. 316-334, May 2000.

[15] J. Dieudonné. *La Géométrie des Groupes Classiques*, 2nd edition. Springer-Verlag, 1963.

[16] R. H. Dye. On the Arf Invariant. *Journal of Algebra*, pp. 36-39, 1978.

[17] Y. Egawa. Association Schemes of Quadratic Forms. *Journal of Combinatorial Theory*, Series A 38, pp. 1-14, 1985.

[18] J-C. Faugère, V. Gauthier-Umana, A. Otmani, L. Perret, J-P. Tillich, *A distinguisher for high rate McEliece cryptosystems.* Proceedings IEEE Information Theory Workshop, Paraty, Brazil 2011.

[19] W. C. Huffman, V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2003.

[20] Y. Ishai, E. Kushilevitz, R. Ostrovsky, M. Prabhakaran, A. Sahai, J. Wullschleger. Constant-Rate Oblivious Transfer from Noisy Channels. *Crypto 2011*, LNCS 6841, pp. 667-684, 2011.

[21] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Zero-knowledge proofs from secure multiparty computation. *SIAM J. Comput.*, Vol. 39(3), pp. 1121-1152, 2009.

[22] W. Kositwattanarerk, F. Oggier. On construction D and related constructions of lattices from linear codes. Presented at WCC 2013, to appear in Des. Codes Crypto. Preprint: `http://arxiv.org/abs/1308.6175`

[23] T. Y. Lam. *Introduction to Quadratic Forms over Fields.* Graduate Studies in Mathematics 67, American Mathematical Society, 2005.

[24] R. Lidl, H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

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

[26] F. Oggier, G. Zémor. Coding constructions for efficient oblivious transfer from noisy channels. Preprint.

[27] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, Vol. 106/107, pp. 369-381, 1992.

[28] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *J. Complexity*, Vol. 28, pp. 489-517, 2012.

[29] H. Randriambololona. Asymptotically good binary linear codes with asymptotically good self-intersection spans. *IEEE Trans. Inform. Theory*, Vol. 59, pp. 3038-3045, May 2013.

[30] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. Preprint: `http://arxiv.org/abs/1312.0022`.

[31] J. -P. Serre. *A Course in Arithmetic.* Graduate Texts in Mathematics 7, Springer, 1973.

A Quadratic forms

This appendix is meant to be a continuation of Section 4. In particular, we refer to that section for the definitions of quadratic form, radical and rank.

Let K be a field, let (V, Q) be a K-quadratic space.

With abuse of terminology, V itself is called a quadratic space. Recall that V, as a vector space, is finite dimensional by definition. Any subspace W of V inherits a natural structure of quadratic space, defined by the restriction of Q to W.

Recall that we defined a symmetric bilinear form $\tilde{B}_Q$ on V by

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

for all $x, y \in V$. If $\operatorname{char} K \neq 2$ we also define the symmetric bilinear form $B_Q := \frac{1}{2}\tilde{B}_Q$, which satisfies $B_Q(x, x) = Q(x)$ for all $x \in V$. If $\operatorname{char} K = 2$ note that $\tilde{B}_Q$ is alternating, i.e. $\tilde{B}_Q(x, x) = 0$ for all $x \in V$. As a shorthand, if there is no ambiguity we write $x \cdot y$ instead of $\tilde{B}_Q(x, y)$ for $x, y \in V$.

A remark concerning the definitions of radical and rank follows. If $\operatorname{char} K \neq 2$ then Q vanishes on $\operatorname{Rad} V$: indeed, for all $x \in \operatorname{Rad} V$ we have $Q(x) = B_Q(x, x) = \frac{1}{2}x \cdot x = 0$ by definition of the radical. If $\operatorname{char} K = 2$ this is not always the case: for example, consider the quadratic form on $\mathbb{F}_2$ defined by $Q(x) := x^2$; note that $\tilde{B}_Q$ is identically zero, hence the radical is the whole space, but Q does not vanish at $x = 1$. So in the characteristic 2 case $\operatorname{Rad}^0 V$, the zero locus of the restriction of Q to $\operatorname{Rad} V$, is not necessarily trivial. Following [15], we have defined the rank of a quadratic form to be the codimension of this zero locus.

In the characteristic 2 case, under the additional assumption that K is perfect, i.e. squaring is an automorphism of K (which is always the case if K is a finite field), one can prove that the difference between the rank of Q and the codimension of the radical of V is either zero or one.

We define orthogonality and isotropy with respect to $\tilde{B}_Q$, as follows.

Two vectors $x, y \in V$ are orthogonal if $x \cdot y = 0$. Two subspaces $V_1, V_2 \subseteq V$ are orthogonal if $x \cdot y = 0$ for all $x \in V_1, y \in V_2$. We use the symbol $\perp$ for the orthogonality relation. The orthogonal of a subspace $V_1 \subseteq V$ is

$$V_1^{\perp} := \{x \in V : x \cdot y = 0 \text{ for all } y \in V_1\}.$$

Note that $V_1 \cap V_1^{\perp} = \operatorname{Rad} V_1$, so $\operatorname{Rad} V_1 = 0$ implies $V_1 \cap V_1^{\perp} = 0$. Moreover, by basic linear algebra $\dim V_1 + \dim V_1^{\perp} = \dim V$. Hence in this case $V_1^{\perp}$ is a complement of V_1, called the orthogonal complement of V_1. Finally, a decomposition of V is orthogonal if the components are pairwise orthogonal.

A non-zero vector $x \in V$ is isotropic if $x \cdot x = 0$. A subspace of V is isotropic if it contains an isotropic vector, anisotropic otherwise. Note that if $\operatorname{char} K = 2$ then every vector is isotropic, as $\tilde{B}_Q$ is alternating, hence it does not make sense to use this notion.

A quadratic space (V, Q) is classified according to the orthogonal decomposition induced on V by Q. The "building blocks" in this decomposition are hyperbolic and symplectic planes, that are defined below.

Definition A.1 (hyperbolic plane). *Assume that* $\operatorname{char} K \neq 2$. *A hyperbolic plane is a non-degenerate* 2*-dimensional subspace which admits a basis of isotropic vectors.*

Note that any hyperbolic plane H admits a basis $\{v_1, v_2\}$ of isotropic vectors such that $v_1 \cdot v_2 = 1$. Indeed, for any basis $\{v_1, w\}$, with v_1, w isotropic, it holds that $\alpha := v_1 \cdot w \neq 0$ as H is non-degenerate, hence $\{v_1, v_2\}$ with $v_2 := \alpha^{-1}w$ satisfies the property.

Theorem A.2 (Witt's decomposition). *Assume that* $\operatorname{char} K \neq 2$. *Then the quadratic space* V *orthogonally decomposes as*

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} H_i \oplus W,$$

where the H_i*'s are hyperbolic planes and* W *is anisotropic. Moreover, if* K *is finite then* $\dim W \leq 2$.

Proof. Any complement of $\operatorname{Rad} V$ is non-degenerate and orthogonal to $\operatorname{Rad} V$, so we may assume that $\operatorname{Rad} V = 0$, i.e. V is non-degenerate. If V is anisotropic we are done, with $m = 0$ and $V = W$. Otherwise there exists an isotropic vector $v_1 \in V$, hence $x \in V$ such that $\alpha := v_1 \cdot x \neq 0$, as V is non-degenerate. Now take

$$v_2 := \frac{1}{\alpha} x - \frac{x \cdot x}{2\alpha^2} v_1,$$

$H_1 := \langle v_1, v_2 \rangle$ and apply induction.

If K is finite then $\dim W \leq 2$, as any quadratic form on a non-degenerate space of dimension larger than 2 has a non trivial zero, which is an isotropic vector of V. This is a consequence of the Chevalley-Warning Theorem, see for example [31]. △

Definition A.3 (symplectic plane). *Assume that* $\operatorname{char} K = 2$. *A symplectic plane is a subspace which admits a basis* $\{v_1, v_2\}$ *such that* $v_1 \cdot v_2 = 1$.

Non-degeneracy is implied by this definition.

Theorem A.4. *Assume that* $\operatorname{char} K = 2$. *Then the quadratic space* V *orthogonally decomposes as*

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} S_i,$$

where the S_i*'s are symplectic planes. Moreover, all but at most one among the* S_i*'s admit a* K*-basis* $\{v_1, v_2\}$ *such that* $v_1 \cdot v_2 = 1$ *and* $Q(v_1) = Q(v_2) = 0$.

Proof. Again, we may assume that V is non-degenerate. Let $v_1 \in V$, let $x \in V$ be such that $\alpha := v_1 \cdot x \neq 0$. Take $v_2 := \frac{1}{\alpha} x$, $S_1 := \langle v_1, v_2 \rangle$ and argue by induction. For the last statement, see [16] or [15, Chapter I, Section 16]. △

Remark A.5. *Stronger results actually hold. The decompositions above are, in some sense, unique: for example, in a Witt decomposition, the number* m *of hyperbolic planes is unique while the anisotropic space* W *is unique up to "isometry". For details, see [23, 31] for Theorem A.2 and [16, 15] for Theorem A.4. However, these stronger results are not needed here.*

A.1 Number of zeros of a quadratic form

Let (V, Q) *be a quadratic space over the finite field* $\mathbb{F}_q$.

In this section we compute the number of zeros in V of the quadratic form Q, as a function of the dimension k of V, the rank r of Q and the cardinality q of the base field. Even though the definition of rank is essentially dependent on $\operatorname{char} \mathbb{F}_q$, the formula we give is characteristic-free.

Theorem A.6. *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.*

Remark A.7. *The "±" in claim b of Theorem A.6 (and of the forthcoming Theorem A.9) only depends on the "last component" in the orthogonal decomposition of* V *given by Theorem A.2 or Theorem A.4.*

In [24, Chapter 6, Section 2] the number of vectors $x \in V$ such that $Q(x) = b$, for any full-rank quadratic form Q on V and any $b \in \mathbb{F}_q$, is computed. Theorem A.9 below, whence Theorem A.6 easily follows, is an instance of this result. However, for completeness, and to show an application of the classification theorems, we include a full proof of Theorem A.9.

Here, it is convenient to view quadratic forms as polynomials, as follows. This correspondence holds over an arbitrary field K (so we abandon for a moment the assumption that the base field is finite). Fixing a K-basis $\{v_1, \dots, v_k\}$ of V we can associate to Q a homogeneous quadratic k-variate polynomial $f_Q \in K[X_1, \dots, X_k]$ such that, for all $(\alpha_1, \dots, \alpha_k) \in K^k$,

$$Q(\alpha_1 v_1 + \cdots + \alpha_k v_k) = f_Q(\alpha_1, \dots, \alpha_k),$$

namely

$$f_Q := \sum_{1 \le i \le k} Q(v_i) X_i^2 + \sum_{1 \le i < j \le k} \tilde{B}_Q(v_i, v_j) X_i X_j \in K[X_1, \dots, X_k].$$

Clearly there is a one-to-one correspondence between zeros of Q and zeros of f_Q, independently of the basis choice. We remark that the rank of Q can be equivalently defined as the minimal number of variables appearing in the polynomial f_Q associated to Q, where minimality is taken over all possible basis choices.

Back to the case of $K = \mathbb{F}_q$, we have the following straightforward consequence of the classification theorems.

Corollary A.8. *Assume that $r \ge 3$. Then the polynomial f_Q associated to Q in some suitable basis can be written as*

$$f_Q = g_Q + X_{k-1} X_k, \qquad \textit{with} \qquad g_Q \in \mathbb{F}_q[X_1, \dots, X_{k-2}].$$

Proof. As $r \ge 3$, the classification theorems give an $\mathbb{F}_q$-basis $\{v_1, \dots, v_k\}$ of V such that $\tilde{B}_Q(v_{k-1}, v_k) = 1$, $Q(v_{k-1}) = Q(v_k) = 0$ and $\langle v_1, \dots, v_{k-2} \rangle \perp \langle v_{k-1}, v_k \rangle$. The polynomial f_Q associated to Q with respect to this basis has the desired form. $\triangle$

We are ready to proceed. We start with the case of full-rank forms, and then we show how the general case easily follows.

Theorem A.9. *Assume that $r = k$, i.e. that Q has full rank. Then the number of vectors $x \in V$ such that $Q(x) = 0$ is*

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

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

Proof. Denote by $Z_k(f)$ the number of zeros in $\mathbb{F}_q^k$ of a polynomial $f \in \mathbb{F}_q[X_1, \dots, X_k]$. The proof is by induction on k. If $k = 1$ (case a) then in some basis $f_Q = \alpha X_1^2$ and its only zero is the zero vector. If $k = 2$ (case b) then, by classification theorems, we have two possible situations: either the only zero of f_Q is the zero vector or $f_Q = X_1 X_2$ has $2q - 1$ zeros.

Now let $k \ge 3$. By Corollary A.8 we can write

$$f_Q = g_Q + X_{k-1} X_k, \qquad \text{with} \qquad g_Q \in \mathbb{F}_q[X_1, \dots, X_{k-2}].$$

Note that the zeros of f_Q are exactly all k-tuples (x, α_1, α_2) with $x \in \mathbb{F}_q^{k-2}, \alpha_1, \alpha_2 \in \mathbb{F}_q$ such that

- x is a zero of g_Q and $\alpha_1 \alpha_2 = 0$ or
- x is not a zero of g_Q, $\alpha_1 \neq 0$ and $\alpha_2 = -\alpha_1^{-1} g_Q(x)$.

Hence we get the recursion formula

$$Z_k(f_Q) = (2q-1)Z_{k-2}(g_Q) + (q-1)(q^{k-2} - Z_{k-2}(g_Q)) = q^{k-1} - q^{k-2} + qZ_{k-2}(g_Q)$$

for $k \geq 3$. This gives the result. △

Proof of Theorem A.6. In a suitable basis, the polynomial associated to Q is r-variate, i.e. $f_Q \in \mathbb{F}_q[X_1, \ldots, X_r]$. This defines a full-rank quadratic form on $\mathbb{F}_q^r$, hence Theorem A.9 applies. The conclusion now follows as any zero of f_Q in $\mathbb{F}_q^r$ gives q^{k-r} zeros of f_Q in $\mathbb{F}_q^k$ by padding. △

A.2 Number of quadratic forms of given rank

In this section we compute the number $N(k,r)$ of rank r quadratic forms on any $\mathbb{F}_q$-vector space of dimension k, where k, r are non-negative integers with $k \geq r$. First we deal with the case $k = r$, i.e. of full-rank quadratic forms, then we address the general case. In the full-rank case we write $N(k)$ instead of $N(k,k)$, as a shorthand. We now state the results: Theorem A.10 for the first case, Theorem A.11 for the latter.

Theorem A.10. *For all non-negative integers k, the number of full-rank quadratic forms on an $\mathbb{F}_q$-vector space of dimension k is*

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

Theorem A.11. *For all non-negative integers $k \geq r$, the number of rank r quadratic forms on an $\mathbb{F}_q$-vector space of dimension k is*

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

where $\left[\begin{smallmatrix} k \\ r \end{smallmatrix}\right]$ denotes the q-ary Gaussian binomial coefficient (see Definition 3.1).

Remark A.12. *Recall that $\left[\begin{smallmatrix} k \\ r \end{smallmatrix}\right]$ equals the number of r-dimensional subspaces of any $\mathbb{F}_q$-vector space of dimension k.*

Our proofs of Theorems A.10 and A.11 follow. Our strategy consists of constructing all quadratic forms on a given space as "combinations" (in the sense of Definition A.13 and Construction A.14 below) of quadratic forms on subspaces. Counting recursively the number of forms constructed in this way and dividing by the number of repetitions will give the required quantity.

Towards a proof of Theorem A.10, we fix a non-negative integer k and an $\mathbb{F}_q$-vector space V of dimension k. We define the following "sum" of quadratic forms.

Definition A.13. *Let $V_1, V_2 \leq V$ be subspaces such that $V_1 \cap V_2 = 0$, let Q_1 be a quadratic form on V_1 and Q_2 a quadratic form on V_2. We define $Q := Q_1 \oplus Q_2$ to be the unique quadratic form on $V_1 \oplus V_2$ defined by the conditions $Q|_{V_1} = Q_1$, $Q|_{V_2} = Q_2$ and $V_1 \perp V_2$.*

In other words, for $v \in V_1 \oplus V_2$, we define $Q(v) := Q_1(v_1) + Q_2(v_2)$, where $v_1 \in V_1$ and $v_2 \in V_2$ are the unique vectors such that $v_1 + v_2 = v$. Also note that $\mathrm{Rad}(V_1 \oplus V_2) = \mathrm{Rad}\, V_1 \oplus \mathrm{Rad}\, V_2$. So we construct quadratic forms on V as follows.

Construction A.14. *Let $h \leq k$ be a non-negative integer. Let (V_1, V_2, Q_1, Q_2) be a 4-tuple consisting of a subspace $V_1 \leq V$ of dimension h, a complement $V_2 \leq V$ of V_1, a full-rank quadratic form Q_1 on V_1 and a full-rank quadratic form Q_2 on V_2. Define $Q := Q_{(V_1,V_2,Q_1,Q_2)} := Q_1 \oplus Q_2 \in \mathrm{Quad}(V)$.*

The choice of the parameter h is determined by the characteristic of $\mathbb{F}_q$ and the parity of the dimension k of V, as follows:

1. $h = 1$ if k is odd and $\operatorname{char} \mathbb{F}_q \neq 2$,
2. $h = 2$ if k is even and $\operatorname{char} \mathbb{F}_q \neq 2$,
3. $h = 2$ if $\operatorname{char} \mathbb{F}_q = 2$.

We prove that, with this choice of h, all full-rank quadratic forms on V are obtained by Construction A.14 and, conversely, all forms defined using Construction A.14 have full rank.

Lemma A.15. *Any full-rank quadratic form on V is an instance of Construction A.14 with h chosen as above.*

Proof. First assume that $\operatorname{char} \mathbb{F}_q \neq 2$. If Q is a full-rank quadratic form on V then by Theorem A.2 we have an orthogonal decomposition

$$V = \bigoplus_{i=1}^{m} H_i \oplus W,$$

with $\dim H_i = 2$ for all $i = 1, \ldots, m$ and $\dim W \leq 2$. If k is odd then $\dim W$ is also odd, hence it must equal 1. Let $V_1 := W$, $V_2 := \bigoplus_{i=1}^{m} H_i$, $Q_1 := Q|_{V_1}$ and $Q_2 := Q|_{V_2}$, then $Q = Q_{(V_1,V_2,Q_1,Q_2)}$ with $h = \dim W = 1$. If k is even, let $V_1 := H_1, V_2 := \bigoplus_{i=2}^{m} H_i \oplus W, Q_1 := Q|_{V_1}, Q_2 := Q|_{V_2}$, then $Q = Q_{(V_1,V_2,Q_1,Q_2)}$ with $h = \dim H_1 = 2$.

Now assume $\operatorname{char} \mathbb{F}_q = 2$. If Q is a full-rank quadratic form on V then by Theorem A.4 we have an orthogonal decomposition

$$V = \operatorname{Rad} V \oplus \bigoplus_{i=1}^{m} S_i$$

with $\dim \operatorname{Rad} V = 0$ or 1. Let $V_1 := S_1, V_2 := \operatorname{Rad} V \oplus \bigoplus_{i=2}^{m} S_i, Q_1 := Q|_{V_1}, Q_2 := Q|_{V_2}$, then $Q = Q_{(V_1,V_2,Q_1,Q_2)}$ with $h = \dim S_1 = 2$. △

Lemma A.16. *Any instance of Construction A.14, with h chosen as above, is a full-rank quadratic form on V.*

Proof. Let V_1, V_2, Q_1, Q_2 be as in Construction A.14, and let $Q := Q_{(V_1,V_2,Q_1,Q_2)}$. The statement is obvious if $\operatorname{char} \mathbb{F}_q$ is odd: in this case both $\operatorname{Rad} V_1 = \operatorname{Rad} V_2 = 0$, hence $\operatorname{Rad}(V_1 \oplus V_2) = 0$ as well. The same happens in the characteristic 2 case if both h and k are even.

The only non trivial case is the one of $\operatorname{char} \mathbb{F}_q = 2$ and k odd. We have chosen h to be even, hence $\operatorname{Rad} V_1 = 0$ while $\operatorname{Rad} V_2 = \langle w \rangle$ for some $w \in V_2$ such that $Q(w) \neq 0$. Then $\operatorname{Rad}(V_1 \oplus V_2) = \langle w \rangle$ and $Q(w) = Q_2(w) \neq 0$, hence Q has full rank. △

It follows that the number of full-rank quadratic forms on V is given by the number of suitable 4-tuples (V_1, V_2, Q_1, Q_2) divided by the number of repetitions. The number of possible choices for V_1 is given by a Gaussian binomial coefficient. The following combinatorial lemma computes the number of possible choices for V_2.

Lemma A.17. *Let $h \leq k$ be a non-negative integer. The number of complements of an h-dimensional subspace of V is $q^{h(k-h)}$.*

Proof. Let W be an h-dimensional subspace of V, with basis $\{v_1, \dots, v_h\}$. This can be completed to a basis of V in $(q^k - q^h)(q^k - q^{h+1}) \cdots (q^k - q^{k-1})$ ways. Any complement of W has dimension $k-h$, hence $(q^{k-h} - 1)(q^{k-h} - q) \cdots (q^{k-h} - q^{k-h-1})$ different bases. Hence the number of complements of W is

$$\frac{q^k - q^h}{q^{k-h} - 1} \cdot \frac{q^k - q^{h+1}}{q^{k-h} - q} \cdots \frac{q^k - q^{k-1}}{q^{k-h} - q^{k-h-1}} = q^h \cdot q^h \cdots q^h = q^{h(k-h)}.$$

△

Finally, we count how many times a quadratic form is repeated.

Lemma A.18. *Let Q be a full-rank quadratic form on V. For any non-degenerate h-dimensional subspace V_1 of V, with h chosen as above, we have a unique complement V_2 of V_1 and unique full-rank quadratic forms Q_1 and Q_2 on V_1 and V_2 respectively such that $Q = Q_{(V_1,V_2,Q_1,Q_2)}$.*

Proof. Let V_1 be a non-degenerate h-dimensional subspace of V. We want to define V_2, Q_1, Q_2 such that $Q_{(V_1,V_2,Q_1,Q_2)} = Q$. Clearly we have to take $Q_1 := Q|_{V_1}$. The choice of h implies that $\operatorname{Rad} V_1 = 0$, hence V_1 has an orthogonal complement. So take $V_2 := V_1^{\perp}$ and $Q_2 := Q|_{V_2}$. Note that these are the only possible choices, hence this proves the lemma. △

For all full-rank quadratic forms Q on V and all non-negative integers h we denote by $R(Q,h)$ the number of non-degenerate h-dimensional subspaces of V. A priori, this number depends on Q, but we will see that under our choice of h it only depends on k and h. In those cases we denote it by $R(k,h)$.

All lemmas above together prove the following.

Lemma A.19. *Let h be chosen as above, assume that $R(k,h) = R(Q,h)$ is independent of the choice of a quadratic form Q. Then*

$$N(k) = \frac{\begin{bmatrix} k \\ h \end{bmatrix} q^{h(k-h)}}{R(k,h)} N(h) N(k-h).$$

Remark A.20. *By classification theorems, any quadratic form can be obtained by Construction A.14 with $h = 2$, independently of the rank parity. So it is natural to ask why, in the odd characteristic case, we are dealing separately with odd rank and even rank quadratic forms, using $h = 1$ in the first case and $h = 2$ in the second. The reason is that if $\operatorname{rk} Q$ is odd then $R(Q,2)$ depends on Q, yielding a formula more complicated than the one given by Lemma A.19, involving terms which also depend on Q. So our strategy allows a simpler proof.*

Computing the number $R(k,h)$ is the last non trivial step towards the computation of $N(k)$. We are going to do that in the next two sections, obtaining the following recursion formula.

Theorem A.21. *For $k \geq 1$,*

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

Theorem A.21 will be proved in the next two sections, dealing with the odd characteristic case and with the characteristic 2 case separately. We now use it to prove the closed-form expression for $N(k)$ stated by Theorem A.10. Then we will conclude this section with the proof of Theorem A.11.

Proof of Theorem A.10. We argue by induction on k. First note that $N(0) = 1$ and $N(1) = q - 1$. Now let $k > 1$ and assume that the statement is true for $k - 1$. We use the recursion formula given by Theorem A.21. If k is odd then

$$N(k) = (q^k - 1)N(k-1) = (q^k - 1)q^{\frac{k-1}{2}\left(\frac{k-1}{2}+1\right)} \prod_{i=1}^{\frac{k-1}{2}} (q^{2i-1} - 1) = q^{\frac{k-1}{2}\frac{k+1}{2}} \prod_{i=1}^{\frac{k+1}{2}} (q^{2i-1} - 1).$$

If k is even then

$$N(k) = q^k N(k-1) = q^k q^{\frac{k}{2}\left(\frac{k}{2}-1\right)} \prod_{i=1}^{\frac{k}{2}} (q^{2i-1} - 1) = q^{\frac{k}{2}\left(\frac{k}{2}+1\right)} \prod_{i=1}^{\frac{k}{2}} (q^{2i-1} - 1).$$

△

Proof of Theorem A.11. Consider the following construction. For any choice of a subspace V_0 of dimension r, a full-rank quadratic form Q_0 on V_0 and a direct complement R of V_0 we can define the quadratic form $Q := Q_{(V_0,Q_0,R)} := Q_0 \oplus 0 \in \mathrm{Quad}(V)$ of rank r, i.e. the unique quadratic form on V defined by the conditions $Q|_{V_0} = Q_0, Q|_R = 0$ and $V_0 \perp R$. By classification of quadratic forms, any rank r quadratic form is given by $Q_{(V_0,Q_0,R)}$ for some triple (V_0, Q_0, R).

So we only need to compute the number of times each form is repeated, i.e. the number of triples (V_0', Q_0', R') such that $Q_{(V_0',Q_0',R')} = Q_{(V_0,Q_0,R)} =: Q$, where (V_0, Q_0, R) is a fixed triple. First note that

$$R' = \{x \in \mathrm{Rad}\, V : Q(x) = 0\} = R,$$

hence V_0' has to be a direct complement of R. But for any direct complement V_0' of R we have that the triple $(V_0', Q|_{V_0'}, R)$ defines the form Q. So, for any triple (V_0, Q_0, R), the number of triples (V_0', Q_0', R') such that $Q_{(V_0',Q_0',R')} = Q_{(V_0,Q_0,R)}$ is equal to the number of direct complements of R.

We are ready to conclude. We have $\begin{bmatrix} k \\ r \end{bmatrix}$ choices for V_0, $N(r)$ choices for Q_0 by definition, $q^{r(k-r)}$ choices for R by Lemma A.17 and any form occurs $q^{r(k-r)}$ times. Hence $N(k, r) = \begin{bmatrix} k \\ r \end{bmatrix} N(r)$, as claimed. △

The next two sections constitute the proof of Theorem A.21. They share a similar structure: first we compute $R(k, h)$ in some interesting cases, then we use it, together with Lemma A.19, to prove Theorem A.21. Section A.2.1 deals with the odd characteristic case, Section A.2.2 deals with the characteristic 2 case.

A.2.1 Odd characteristic case

In this section, assume that $\mathrm{char}\, \mathbb{F}_q$ *is odd.*

Lemma A.22. *We have that*

1. $R(k, 1) = q^{k-1}$ *if* k *is odd,*
2. $R(k, 2) = q^{k-2}\frac{q^k-1}{q^2-1}$ *if* k *is even.*

In particular, these numbers are independent of the choice of a full-rank quadratic form Q.

Proof. Let Q be a full-rank quadratic form on V. All 1-dimensional subspaces $V_1 \leq V$ such that $Q|_{V_1}$ has full rank are given by $V_1 = \langle v_1 \rangle$ for some vector $v_1 \in V$ such that $Q(v_1) \neq 0$. As Q has odd rank, it has q^{k-1} zeros, hence we have $q^k - q^{k-1}$ possible choices for v_1. But $\langle \lambda v_1 \rangle = \langle v_1 \rangle$ for any $\lambda \in \mathbb{F}_q, \lambda \neq 0$, hence each subspace is counted $q-1$ times. So $R(k,1) = \frac{q^k - q^{k-1}}{q-1} = q^{k-1}$, and this proves the first claim.

We now prove the second claim. We can choose any non zero $v_1 \in V$ as first basis vector of V_1 and we want to count the number of vectors $v_2 \in V \setminus \langle v \rangle$ such that $Q|_{\langle v_1, v_2 \rangle}$ has full rank. This holds if and only if

$$\det \begin{pmatrix} \tilde{B}_Q(v_1,v_1) & \tilde{B}_Q(v_1,v_2) \\ \tilde{B}_Q(v_1,v_2) & \tilde{B}_Q(v_2,v_2) \end{pmatrix} = \tilde{B}_Q(v_1,v_1)\tilde{B}_Q(v_2,v_2) - \tilde{B}_Q(v_1,v_2)^2 \neq 0,$$

i.e. if and only if v_2 is not a zero of the quadratic form on V defined by

$$Q'(x) := \tilde{B}_Q(v_1,v_1)\tilde{B}_Q(x,x) - \tilde{B}_Q(v_1,x)^2$$

for $x \in V$. One can easily verify that this is indeed a quadratic form and that the associated bilinear form is defined by

$$\tilde{B}_{Q'}(x,y) = 2\tilde{B}_Q(v_1,v_1)\tilde{B}_Q(x,y) - 2\tilde{B}_Q(v_1,x)\tilde{B}_Q(v_1,y)$$

for $x, y \in V$. We distinguish two cases. If $\tilde{B}_Q(v_1,v_1) = 0$ then $Q'(x) = -\tilde{B}_Q(v_1,x)^2$ is the square of a non zero linear form, hence it has rank 1. If $\tilde{B}_Q(v_1,v_1) \neq 0$ then the radical of V with respect to $\tilde{B}_{Q'}$ is exactly the span of v_1, hence $\operatorname{rk} Q' = \operatorname{rk} Q - 1$ is odd as $\operatorname{rk} Q$ is even. In order to prove this, let $w \in \operatorname{Rad} V$ (with respect to $\tilde{B}_{Q'}$), i.e. $\tilde{B}_{Q'}(w,y) = 0$ for all $y \in V$. Then

$$\begin{aligned} \tilde{B}_{Q'}(w,y) &= 2\tilde{B}_Q(v_1,v_1)\tilde{B}_Q(w,y) - 2\tilde{B}_Q(v_1,w)\tilde{B}_Q(v_1,y) = \\ &= 2\tilde{B}_Q(\tilde{B}_Q(v_1,v_1)w - \tilde{B}_Q(v_1,w)v_1, y) = 0 \end{aligned}$$

for all $y \in V$. But $\tilde{B}_Q$ is non-degenerate, hence this implies that $\tilde{B}_Q(v_1,v_1)w = \tilde{B}_Q(v_1,w)v_1$, therefore $w \in \langle v_1 \rangle$ as $\tilde{B}_Q(v_1,v_1) \neq 0$. This proves that $\operatorname{Rad} V \subseteq \langle v_1 \rangle$, and the converse inclusion is obvious. So in any case $\operatorname{rk} Q'$ is odd, hence Q' has q^{k-1} zeros. We can finally conclude. We have $q^k - 1$ choices for v_1 and $q^k - q^{k-1}$ choices for v_2, and any subspace is given by $(q^2-1)(q^2-q)$ different choices of v_1, v_2 (corresponding to the number of bases of $\langle v_1, v_2 \rangle$). So we have $R(k,2) = \frac{(q^k-1)(q^k-q^{k-1})}{(q^2-1)(q^2-q)} = q^{k-2}\frac{q^k-1}{q^2-1}$. This concludes the proof. $\triangle$

The following theorem implies Theorem A.21 in the odd characteristic case. First we need two remarks. Full-rank quadratic forms on $\mathbb{F}_q$ correspond to non zero elements of $\mathbb{F}_q$, hence $N(1) = q-1$. Full-rank quadratic forms on $\mathbb{F}_q^2$ correspond to triples $(x,y,z) \subseteq \mathbb{F}_q^3$ such that $xy - z^2 \neq 0$, which is a quadratic form of rank 3, hence $N(2) = q^3 - q^2 = q^2(q-1)$.

Theorem A.23. *For $k \geq 1$,*

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

Proof. If k is odd then we apply Construction A.14 with $h = 1$. By Lemma A.19 and the first claim of Lemma A.22 we have

$$N(k) = \frac{\begin{bmatrix} k \\ 1 \end{bmatrix} q^{k-1}}{R(k,1)} N(1)N(k-1) = \frac{q^k-1}{q-1}\frac{q^{k-1}}{q^{k-1}}(q-1)N(k-1) = (q^k-1)N(k-1).$$

If k is even then we apply Construction A.14 with $h = 2$. By Lemma A.19 and the second claim of Lemma A.22 we have

$$\begin{aligned} N(k) &= \frac{\begin{bmatrix}k\\2\end{bmatrix} q^{2(k-2)}}{R(k,2)} N(2)N(k-2) = \\ &= \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)} q^{2(k-2)} \frac{1}{q^{k-2}} \frac{q^2-1}{q^k-1} q^2(q-1)N(k-2) = \\ &= q^k(q^{k-1}-1)N(k-2). \end{aligned}$$

△

A.2.2 Characteristic 2 case

In this section, assume that $\operatorname{char} \mathbb{F}_q = 2$.

Lemma A.24. *We have that*

1. $R(k,2) = q^{k-2}\frac{q^k-q}{q^2-1}$ *if k is odd,*
2. $R(k,2) = q^{k-2}\frac{q^k-1}{q^2-1}$ *if k is even.*

In particular, these numbers are independent of the choice of a full-rank quadratic form Q.

Proof. The proof is similar to the proof of the second claim of Lemma A.22. Let Q be a full-rank quadratic form on V. In order to obtain a plane $\langle v_1, v_2\rangle \leq V$ such that $Q|_{\langle v_1,v_2\rangle}$ has full rank, we can choose any $v_1 \in V \setminus \operatorname{Rad} V$ and any $v_2 \in V \setminus \langle v_1\rangle$ which is not a zero of the quadratic form defined by

$$Q'(x) := \tilde{B}_Q(v_1,v_1)\tilde{B}_Q(x,x) - \tilde{B}_Q(v_1,x)^2 = \tilde{B}_Q(v_1,x)^2$$

for $x \in V$. In the characteristic 2 case this form always has rank 1, hence it has q^{k-1} zeros. So we have $q^k - |\operatorname{Rad} V|$ choices for v_1 and $q^k - q^{k-1}$ choices for v_2, and any subspace is given by $(q^2-1)(q^2-q)$ different choices of v_1, v_2, hence $R(k,2) = \frac{(q^k-|\operatorname{Rad} V|)(q^k-q^{k-1})}{(q^2-1)(q^2-q)} = q^{k-2}\frac{q^k-|\operatorname{Rad} V|}{q^2-1}$. Now note that $|\operatorname{Rad} V| = q$ if k is odd and $|\operatorname{Rad} V| = 1$ if k is even, hence both claims follow at once. △

We are going to conclude the proof of Theorem A.21. Again, we use the fact that $N(2) = q^2(q-1)$.

Theorem A.25. *For $k \geq 1$,*

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

Proof. Recall that in this case we use Construction A.14 with $h = 2$. By Lemma A.19 we have

$$N(k) = \frac{\begin{bmatrix}k\\2\end{bmatrix} q^{2(k-2)}}{R(k,2)} N(2)N(k-2) = \frac{1}{R(k,2)} q^{2(k-2)} q^2(q-1) \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)} N(k-2).$$

If k is odd then by claim *1* of Lemma A.24 we have

$$N(k) = \frac{q^2-1}{q^k-q} \frac{1}{q^{k-2}} q^{2(k-2)} q^2(q-1) \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)} N(k-2) = q^{k-1}(q^k-1)N(k-2).$$

If k is even then by claim *2* of Lemma A.24 we have

$$N(k) = \frac{q^2-1}{q^k-1} \frac{1}{q^{k-2}} q^{2(k-2)} q^2(q-1) \frac{(q^k-1)(q^{k-1}-1)}{(q^2-1)(q-1)} N(k-2) = q^k(q^{k-1}-1)N(k-2).$$

△