Maximum-Likelihood Decoding of Gabidulin Codes Is NP-Hard Even in Dimension One

Philippe Gaborit
XLIM, Université de Limoges, France
gaborit@unilim.fr

Abstract

Fix a prime power q. We prove that deciding whether a received word $y \in \mathbb{F}_{q^m}^n$ lies at rank distance at most $n-2$ from the one-dimensional Gabidulin code $\{\lambda g : \lambda \in \mathbb{F}_{q^m}\}$ is NP-complete. Thus maximum-likelihood decoding of Gabidulin codes is NP-hard even for $k = 1$, an analogue of the Guruswami–Vardy theorem for Reed–Solomon codes. In the Hamming metric, by contrast, hardness at this radius requires the dimension to grow with the length, as in the Guruswami–Vardy theorem. The reduction is deterministic; consequently Rank Syndrome Decoding (RSD) and Rank Minimum Distance (RMD) for $\mathbb{F}_{q^m}$-linear codes are NP-complete under deterministic polynomial reductions, whereas the previously known reduction was randomized. The proof goes through a pivot problem that we introduce, Twisted Square Membership (TSM): given $\mathbb{F}_q$-subspaces $U, W \subset \mathbb{F}_{q^N}$, decide whether some non-zero $a \in U$ satisfies $a^{q+1} \in W$. Quadratic systems in d unknowns are encoded into TSM, then TSM into Gabidulin decoding. The last step views the received word as an $\mathbb{F}_q$-linear map and decoding at radius $n-2$ as the search for an $\mathbb{F}_q$-plane on which it acts as a scalar. With support $U \oplus \tau W$ in a cubic extension and map $a + \tau b \mapsto a^{q^2} + \tau b^q$, two Frobenius twists force solution planes to encode the relation $a^{q+1} \in W$. All constructions are explicit and polynomial, with $N = O(qd^2)$, $n \le N + d$, and $m = 3N$.

Keywords: Rank metric · Gabidulin codes · NP-completeness · maximum-likelihood decoding · MinRank

1 Introduction

1.1 Context and motivation

Gabidulin codes [11, 16] are the rank-metric analogues of Reed–Solomon codes. They are maximum rank distance codes and can be decoded in polynomial time up to $\lfloor (n-k)/2 \rfloor$ errors. Beyond half the minimum distance, however, the picture changes sharply: no analogue of the Guruswami–Sudan algorithm is known, and for many parameters no efficient worst-case list decoder can exist because some received words have exponentially many nearby codewords [36, 32]. The complexity of maximum-likelihood decoding for Gabidulin codes themselves has remained open, to the best of our knowledge. Our main result closes this gap in a particularly rigid case: for every fixed prime power q, decoding is NP-complete already for dimension-one Gabidulin codes at radius $n-2$ (Theorem 13).

This result fits into a longer line of hardness results for decoding. In the Hamming metric, Berlekamp, McEliece and van Tilborg proved that decoding a general linear code is NP-complete [5]; Vardy settled the corresponding minimum-distance problem [35], and Dumer, Micciancio and Sudan proved hardness of approximation [12]. Structured algebraic codes require separate arguments. Reed–Solomon codes admit polynomial-time decoding up to half the minimum distance, and the Guruswami–Sudan algorithm reaches the Johnson radius [23]; nevertheless, Guruswami and Vardy proved maximum-likelihood decoding NP-hard at radius $n-k-1$ over fields of exponential size [26]. Further hardness results connect bounded-distance decoding to discrete logarithms [8], cover algebraic-geometry codes under randomized reductions [7], and lower the NP-hard radius for Reed–Solomon codes to $n-k-c\log n/\log\log n$ [20].

In the rank metric, a vector in $\mathbb{F}_{q^m}^n$ is weighted by the $\mathbb{F}_q$-dimension of the space spanned by its coordinates rather than by the number of non-zero coordinates. Besides their coding-theoretic role, Gabidulin codes underlie error control in random linear network coding [27, 34] and have found applications in theoretical computer science, from explicit hitting sets for low-rank matrices [14] to list decoding via subspace designs [24, 22]; random Gabidulin codes achieve list decoding capacity [25]. On the complexity side, MinRank is NP-complete [6], and decoding an $\mathbb{F}_q$-linear code is an instance of MinRank. The $\mathbb{F}_{q^m}$-linear case is substantially more rigid. Gaborit and Zémor proved hardness for such rank-metric decoding problems through a randomized reduction from Hamming decoding [19], but no hardness result was known for maximum-likelihood decoding of Gabidulin codes themselves, to the best of our knowledge.

The question also matters in rank-based cryptography. The first rank-metric encryption scheme, due to Gabidulin, Paramonov and Tretjakov [18], is a McEliece-type construction based on a disguised Gabidulin code; Overbeck's structural attacks [30] motivated repaired variants, including Loidreau's scheme [29] and its subsequent cryptanalysis [9]. More directly related to this work, the Faure–Loidreau scheme [13] and its repaired version LIGA [31] rely on decoding Gabidulin codes beyond the unique-decoding radius. Our result concerns worst-case complexity only and does not address the particular parameters or instance distributions used by these cryptosystems; it places the underlying worst-case decoding problem on a firmer complexity-theoretic footing. Other rank-based constructions rely on rank syndrome decoding for random or quasi-cyclic $\mathbb{F}_{q^m}$-linear codes, including LRPC-based schemes [17, 1], the ROLLO and RQC candidates to the NIST post-quantum standardization process [3, 4], and rank-based signatures such as Durandal [2].

1.2 The idea of the method

The proof rests on three elementary observations whose combination is the key.

First, decoding becomes an eigenplane problem. For a dimension-one Gabidulin code $\{\lambda g\}$, the received word y can be viewed as an $\mathbb{F}_q$-linear map $\tilde{y}$ on the $\mathbb{F}_q$-space spanned by the coordinates of g, while the codeword λg corresponds to multiplication by λ. Decoding at radius $n-2$ is therefore equivalent to finding an $\mathbb{F}_q$-plane on which $\tilde{y}$ acts as a scalar, which we call an *eigenplane*.

Second, the eigenplane equation produces a twisted square. Because the received word is part of the constructed instance, we let $\tilde{y}$ act by different Frobenius twists on different parts of the support. Comparing $a \mapsto a^{q^2}$ and $b \mapsto b^q$ along an eigenplane yields $b \in \mathbb{F}_q^*\, a^{q+1}$. Thus the

only non-linearity that must be encoded is the map $a \mapsto a^{q+1} = a \cdot a^q$. This leads to the pivot problem Twisted Square Membership (TSM): given subspaces $U, W \subset \mathbb{F}_{q^N}$, decide whether there exists a non-zero $a \in U$ with $a^{q+1} \in W$. The linear membership constraints are built into the support, while the eigenplane equation supplies the non-linear relation.

Third, twisted squares encode homogeneous quadratic systems. The element $a \cdot a^q$ is quadratic in the $\mathbb{F}_q$-coordinates of a. With a suitable basis of U, every homogeneous quadratic system can be represented by linear conditions on a^{q+1}. Since such systems encode 3-SAT, TSM is NP-complete.

The complete reduction is therefore

$$\text{3-SAT} \longrightarrow \text{HomMQ} \longrightarrow \text{TSM} \longrightarrow \text{GabDec}_1,$$

with TSM separating the finite-field encoding of quadratic forms from the Gabidulin decoding construction.

1.3 Contributions and organization

Theorem 13 proves that, for every fixed prime power q, deciding whether a received word lies at rank distance at most $n-2$ from a dimension-one Gabidulin code is NP-complete. Radius $n-1$ is always reachable, so $n-2$ is the first nontrivial radius. Maximum-likelihood decoding is therefore NP-hard as soon as the problem ceases to be trivial, already for $k = 1$. This is a rank-metric analogue of the Guruswami–Vardy theorem, with the notable difference that its Hamming-metric counterpart requires growing dimension; see Section 7.

The reduction is deterministic. As a consequence, rank syndrome decoding and rank minimum distance for general $\mathbb{F}_{q^m}$-linear codes are NP-complete under deterministic polynomial reductions, with rank minimum distance already hard for dimension-two codes (Corollaries 26 and 27). The previously known reduction for these problems was randomized [19].

A further contribution is the pivot problem TSM, a compact NP-complete problem over finite fields that may be of independent interest. The construction is fully explicit: the encoding exponents are given by a closed formula obtained by interleaving base-q expansions, and a quadratic system in d unknowns leads to parameters $N = O(qd^2)$, $n \leq N + d$, and $m = 3N$.

Organization. Section 2 recalls the necessary background and develops the eigenplane formulation and TSM. Section 3 states the main theorem and gives the complete reduction at a high level. Sections 4–6 prove its three steps. Section 7 derives the complexity consequences, and Section 8 discusses open questions and suggests some directions.

2 Background and preliminaries

This section gathers what the reduction needs. The first part recalls standard material: the rank metric, Gabidulin codes, the two decoding problems of rank-metric coding theory, and the two classical NP-complete problems, 3-SAT and homogeneous quadratic systems, from which we start. The second part contains the two ingredients specific to this paper: the reformulation of decoding in dimension one as the search for an eigenplane, and the pivot problem TSM.

2.1 Background: known problems

Throughout, q is a fixed prime power. For $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$, the rank $\mathrm{rk}(v)$ is the dimension over $\mathbb{F}_q$ of $\langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q}$; equivalently it is the rank of the $m \times n$ matrix over $\mathbb{F}_q$ whose j-th column is the vector of coordinates of v_j in a fixed basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. The rank distance is $d(u, v) = \mathrm{rk}(u - v)$. For instance, with $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$, the vector $(\alpha, \alpha, \alpha + 1)$ has Hamming weight 3 but rank 2, its coordinates spanning $\langle 1, \alpha \rangle$: vanishing coordinates in the Hamming metric are replaced by $\mathbb{F}_q$-linear dependencies in the rank metric.

An $\mathbb{F}_{q^m}$-linear code of length $n \leq m$ and dimension k has minimum rank distance at most $n - k + 1$; this is the Singleton bound for the rank metric [11, 16], and codes meeting it are called maximum rank distance (MRD) codes. Let $g \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(g) = n$. The Gabidulin code of dimension k is $\mathrm{Gab}(g, k) = \{(f(g_1), \ldots, f(g_n))\}$ where f runs over the q-polynomials $\sum_{i<k} f_i X^{q^i}$ with $f_i \in \mathbb{F}_{q^m}$; it is MRD, with minimum rank distance $n - k + 1$. For $k = 1$ one has $f(X) = \lambda X$, so $\mathrm{Gab}(g, 1) = \{\lambda g : \lambda \in \mathbb{F}_{q^m}\}$ has minimum distance n and unique decoding radius $\lfloor (n-1)/2 \rfloor$. At the other end, decoding $\mathrm{Gab}(g, 1)$ at radius $n-1$ is easy: every received word lies at rank distance at most $n - 1$ from the code, since for any coordinate y_j the scalar $\lambda = y_j/g_j$ makes the j-th coordinate of $y - \lambda g$ vanish, so that its coordinates span a space of dimension at most $n - 1$. The first radius at which decoding is a non-trivial question is therefore $n - 2$.

We shall decode this code, but our conclusions concern the two general problems of rank-metric coding theory, which we recall now. An $\mathbb{F}_{q^m}$-linear code of length n and dimension k is given by a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ or by a parity-check matrix $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$. Both problems below are in NP, with e or the codeword as certificate.

Definition 1 (rank syndrome decoding, RSD)**.** Given $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$, a syndrome $s \in \mathbb{F}_{q^m}^{n-k}$ and an integer t, decide whether there exists $e \in \mathbb{F}_{q^m}^n$ with $He^\top = s$ and $\mathrm{rk}(e) \leq t$.

Definition 2 (rank minimum distance, RMD)**.** Given $G \in \mathbb{F}_{q^m}^{k \times n}$ and an integer w, decide whether the code generated by G contains a non-zero codeword of rank at most w.

RSD is equivalent to bounded-distance decoding, with input (G, y, t) and question whether some codeword lies at rank distance at most t from y, since $e = y - c$ and H, $s = Hy^\top$ are computed from G and y in polynomial time.

Remark 3 (relation with MinRank). Identifying a vector of $\mathbb{F}_{q^m}^n$ with its $m \times n$ matrix of coordinates over $\mathbb{F}_q$, the codewords of an $\mathbb{F}_{q^m}$-linear code form an $\mathbb{F}_q$-space of matrices, and RSD asks for a matrix of rank at most t in an affine space of matrices: this is an instance of MinRank. It is a structured one, since the matrix space is stable under multiplication by $\mathbb{F}_{q^m}$; for the code $\{\lambda g\}$, for instance, every non-zero matrix of the space has full rank n. This gives RSD $\leq$ MinRank and not the converse, so the hardness of MinRank [6] does not transfer and a dedicated reduction is needed.

The source of our reduction is the satisfiability problem for formulas in 3-conjunctive normal form.

Definition 4 (3-SAT)**.** An instance consists of Boolean variables $b_1, \ldots, b_v$ and a formula $\Phi = C_1 \wedge \cdots \wedge C_c$. Each clause C_j is a disjunction $\ell_{j,1} \vee \ell_{j,2} \vee \ell_{j,3}$ of three *literals*, a literal being either a variable b_i or its negation $\neg b_i$. An *assignment* is a map $\sigma : \{b_1, \ldots, b_v\} \to \{\mathrm{true}, \mathrm{false}\}$; it makes the literal b_i true if $\sigma(b_i) = \mathrm{true}$, the literal $\neg b_i$ true if $\sigma(b_i) = \mathrm{false}$, a clause true

if at least one of its three literals is true, and Φ true if all clauses are true. The question is whether there exists an assignment making Φ true, in which case Φ is *satisfiable*.

For instance $\Phi = (b_1 \vee \neg b_2 \vee b_3) \wedge (\neg b_1 \vee b_2 \vee b_3)$ is satisfiable, by $\sigma(b_3) = \text{true}$, whatever the values of b_1 and b_2. 3-SAT is the NP-complete problem of Cook and Levin [21]; the size of an instance is polynomial in $v + c$. Its first translation is into quadratic systems, whose NP-completeness is classical as well [15, 21]; we use the homogeneous version.

Definition 5 (HomMQ)**.** Given homogeneous quadratic forms $Q_1, \ldots, Q_s$ in d unknowns over $\mathbb{F}_q$, decide whether there exists $x = (x_1, \ldots, x_d) \in \mathbb{F}_q^d$, $x \neq 0$, with $Q_1(x) = \cdots = Q_s(x) = 0$.

2.2 Preliminaries: the eigenplane formulation and the TSM pivot problem

We next specialize to the problem studied in this paper: decoding dimension-one Gabidulin codes at the first nontrivial radius.

Definition 6 (GabDec_1)**.** Given $g, y \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(g) = n$, decide whether there exists $\lambda \in \mathbb{F}_{q^m}$ such that $\mathrm{rk}(y - \lambda g) \leq n - 2$.

This is RSD for $k = 1$, $G = g$ and $t = n - 2$; it is in NP with λ as certificate. Radius $n - 1$ is always reachable, as shown below, so $n - 2$ is the first non-trivial radius.

The key to everything that follows is to read vectors as linear maps. Throughout the paper, $g = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ has $\mathbb{F}_q$-linearly independent coordinates, and we call

$$G = \langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_{q^m}$$

the *support* of the code $\mathrm{Gab}(g, 1)$; it is an $\mathbb{F}_q$-space of dimension n, of which g is a basis.

Definition 7 (the map $\tilde{y}$)**.** For $y = (y_1, \ldots, y_n) \in \mathbb{F}_{q^m}^n$, we denote by $\tilde{y} : G \to \mathbb{F}_{q^m}$ the unique $\mathbb{F}_q$-linear map such that $\tilde{y}(g_j) = y_j$ for $j = 1, \ldots, n$, that is,

$$\tilde{y}\Big(\sum_{j=1}^{n} c_j g_j\Big) = \sum_{j=1}^{n} c_j y_j \qquad (c_j \in \mathbb{F}_q).$$

Lemma 8 (vectors as linear maps)**.** *The map $y \mapsto \tilde{y}$ is a bijection between $\mathbb{F}_{q^m}^n$ and the set of $\mathbb{F}_q$-linear maps $G \to \mathbb{F}_{q^m}$, whose inverse is $\tilde{y} \mapsto (\tilde{y}(g_1), \ldots, \tilde{y}(g_n))$. Under this bijection, the codeword λg corresponds to the multiplication by λ on G, and $y - \lambda g$ corresponds to $\tilde{y} - \lambda$.*

Proof. An $\mathbb{F}_q$-linear map on G is determined by the images of the basis g, and these images can be prescribed arbitrarily. The map attached to λg sends g_j to λg_j, hence is $x \mapsto \lambda x$ by linearity; the last assertion follows since $y \mapsto \tilde{y}$ is $\mathbb{F}_q$-linear. □

In particular, choosing a received word is the same as choosing an $\mathbb{F}_q$-linear map on the support; this is how received words will be constructed in Section 6.

Lemma 9. $\mathrm{rk}(y - \lambda g) = n - \dim_{\mathbb{F}_q} \mathrm{Ker}(\tilde{y} - \lambda)$.

Proof. The coordinates of $y - \lambda g$ are the images $(\tilde{y} - \lambda)(g_j)$ of a basis of G, so they span $\mathrm{Im}(\tilde{y} - \lambda)$; conclude with the rank theorem. □

Lemma 10 (eigenplane)**.** *There exists λ with $\mathrm{rk}(y-\lambda g) \le n-2$ if and only if there exist $\mathbb{F}_q$-linearly independent $x_1, x_2 \in G$ with $\tilde{y}(x_1)\,x_2 = \tilde{y}(x_2)\,x_1$.*

Proof. If $\dim \mathrm{Ker}(\tilde{y}-\lambda) \ge 2$, two independent vectors x_1, x_2 of this kernel satisfy $\tilde{y}(x_i) = \lambda x_i$, whence $\tilde{y}(x_1)x_2 = \lambda x_1 x_2 = \tilde{y}(x_2)x_1$. Conversely put $\lambda = \tilde{y}(x_1)/x_1$; the equation gives $\tilde{y}(x_2) = \lambda x_2$, and since $\tilde{y}-\lambda$ is $\mathbb{F}_q$-linear the whole plane $\langle x_1, x_2\rangle$ lies in its kernel. □

For a single vector the condition is empty: any $x \neq 0$ gives $\lambda = \tilde{y}(x)/x$, which is why radius $n-1$ is trivial. In Lemma 10 the equation is written for one basis (x_1, x_2) of the plane; in Section 6 we shall apply it to other pairs of vectors of the same plane, which the following lemma allows.

Lemma 11 (eigenplane equation for all pairs)**.** *Let $L \subset G$ be an $\mathbb{F}_q$-plane. The following are equivalent: (i) $\tilde{y}(x_1)x_2 = \tilde{y}(x_2)x_1$ for one basis (x_1, x_2) of L; (ii) $L \subset \mathrm{Ker}(\tilde{y}-\lambda)$ for some $\lambda \in \mathbb{F}_{q^m}$; (iii) $\tilde{y}(x)\,x' = \tilde{y}(x')\,x$ for all $x, x' \in L$.*

Proof. (i)⇒(ii) is the second half of the proof of Lemma 10, with $\lambda = \tilde{y}(x_1)/x_1$. (ii)⇒(iii): every $x \in L$ satisfies $\tilde{y}(x) = \lambda x$, hence for $x, x' \in L$, $\tilde{y}(x)x' = \lambda x x' = \tilde{y}(x')x$. (iii)⇒(i) is a special case. □

We call a plane satisfying these conditions a *solution plane*; by Lemma 9, the decoding instance is a yes-instance if and only if a solution plane exists.

The eigenplane formulation tells us what has to be encoded: a plane on which $\tilde{y}$ acts as a scalar. The reduction will be organized around an intermediate problem tailored to this, which we introduce now. Let $E = \mathbb{F}_{q^N}$. For $a \in E$ we call $a^{q+1} = a \cdot a^q$ the *twisted square* of a: it is a square twisted by the Frobenius, and for $a \in \mathbb{F}_{q^2}$ it would be the norm to $\mathbb{F}_q$, but here N will be odd.

Definition 12 (Twisted Square Membership, TSM)**.** Given an integer $N \equiv \pm 1 \pmod 6$ and two $\mathbb{F}_q$-subspaces U, W of $E = \mathbb{F}_{q^N}$ by bases, decide whether there exists $a \in U \setminus \{0\}$ whose twisted square a^{q+1} lies in W.

The problem is in NP, with a as certificate. Since $a \mapsto a^q$ is $\mathbb{F}_q$-linear, the twisted square is a quadratic form in the coordinates of a, which is what allows TSM to encode HomMQ (Section 5); and it is the non-linear operation computed by an eigenplane equation, which is what allows TSM to embed into GabDec_1 (Section 6). The condition on N combines two constraints of the latter step: N odd, so that $\mathbb{F}_{q^2} \cap \mathbb{F}_{q^N} = \mathbb{F}_q$, and N prime to 3, so that a cubic extension of $\mathbb{F}_q$ stays cubic over $\mathbb{F}_{q^N}$. We are not aware of TSM having been studied before.

3 Main result and overview of the reduction

We can now state the main result. It concerns the simplest Gabidulin codes, those of dimension one, at the first radius beyond which decoding is not trivial, $n-2$; in particular it does not depend on any special structure of the received word, which is part of the input. The field size q is fixed, while the length n and the extension degree m are part of the input and are polynomial in the size of the source formula.

Theorem 13. *For every fixed prime power q,* GabDec_1 *is NP-complete. More precisely, a 3-SAT formula with v variables and c clauses is mapped in deterministic polynomial time to an instance with $m = 3N$ and $n \leq N + d$, where $d = 1 + v + c$, $N \equiv \pm 1 \pmod 6$ and $N = O(q\, d^2)$.*

Membership in NP was noted in Section 2. NP-hardness is proved by a reduction from 3-SAT in three steps,

$$\mathsf{3\text{-}SAT} \xrightarrow{\S 4} \mathsf{HomMQ} \xrightarrow{\S 5} \mathsf{TSM} \xrightarrow{\S 6} \mathsf{GabDec}_1,$$

each step being an equivalence between a yes-instance of one problem and a yes-instance of the next (Propositions 14, 17 and 23). Before giving the details, we describe the three steps once in a row, following the same object along the chain: a satisfying assignment of the formula becomes a non-zero solution x of a quadratic system, then a field element a, and finally a plane $\langle a, \tau a^{q+1} \rangle$ on which the received word acts as a scalar.

From 3-SAT to HomMQ. Given a formula Φ with variables $b_1, \ldots, b_v$ and clauses C, we write a system of quadratic equations in $d = 1+v+c$ unknowns over $\mathbb{F}_q$: an unknown h which stands for the constant 1, one unknown z_i per variable, which stands for its truth value, and one auxiliary unknown w_C per clause. The equations say that $z_i \in \{0, 1\}$ and that at least one literal of each clause is true. The unknown h is there to make all equations homogeneous: a satisfying assignment gives a solution with $h = 1$, and conversely homogeneity and the equations $z_i^2 = h z_i$ force any non-zero solution to have $h \neq 0$, hence to come from a satisfying assignment. This yields homogeneous quadratic forms $Q_1, \ldots, Q_s$ such that Φ is satisfiable if and only if the Q_k have a common zero $x \neq 0$.

From HomMQ to TSM. We encode the d coordinates of x into a single field element so that all the quadratic forms become linear conditions on its twisted square. We take $E = \mathbb{F}_{q^N}$ with a generator α, choose exponents $e_1 < \cdots < e_d$, and encode x as $a = \phi(x) = x_1 \alpha^{e_1} + \cdots + x_d \alpha^{e_d}$; this identifies $\mathbb{F}_q^d$ with the subspace $U = \langle \alpha^{e_1}, \ldots, \alpha^{e_d} \rangle$, and $x \neq 0$ with $a \neq 0$. Expanding $a^{q+1} = a \cdot a^q$ gives $\sum_{i \leq j} x_i x_j \mu_{ij}$ with $\mu_{ij} \in E$; the exponents are chosen so that the μ_{ij} are linearly independent, which means that a^{q+1} "remembers" every monomial $x_i x_j$ separately. Trace duality then provides, for each k, an element $t_k \in E$ with $\mathrm{Tr}(t_k a^{q+1}) = Q_k(x)$ for all x. Putting $W = \{z \in E : \mathrm{Tr}(t_k z) = 0 \text{ for all } k\}$, the conditions $Q_k(x) = 0$ become $a^{q+1} \in W$. This gives an instance (U, W) of TSM that is a yes-instance if and only if the system has a non-zero solution.

From TSM to GabDec_1. From (U, W) we build a code and a received word, i.e. a support G and an $\mathbb{F}_q$-linear map $\tilde{y}$ on it, so that the eigenplanes of $\tilde{y}$ are exactly the planes $\langle a, \tau a^{q+1} \rangle$ with a a solution of TSM. Three things must be imposed on a plane: its shape, and the two conditions of TSM. The linear conditions are placed in the support: $G = U \oplus \tau W$ inside a cubic extension $K = E(\tau)$, so that every vector of G is $a + \tau b$ with $a \in U$, $b \in W$. The eigenplane equation, one equality in K, is then three equalities in E, one per coefficient on $1, \tau, \tau^2$, and this is what the cubic extension is for. We take $\tilde{y}(a + \tau b) = a^{q^2} + \tau b^q$, two Frobenius twists with different exponents. Two of the three equalities force the plane to be $\langle a, \tau b \rangle$; the third compares the two twists and forces b to be the twisted square a^{q+1}, up to a scalar of $\mathbb{F}_q$, so

that $a^{q+1} \in W$. Conversely a solution a of TSM gives the eigenplane $\langle a, \tau a^{q+1} \rangle$. Thus (g, y) is a yes-instance exactly when (U, W) is; the details are in Section 6.

The sizes are summarized in Table 1 at the end of Section 6. The three steps are now treated in turn, each in a self-contained section.

4 From 3-SAT to HomMQ

This first step is classical, and we include it because its two features, homogeneity and the special unknown h, are used later. We start from a 3-SAT instance as in Section 2, with variables $b_1, \ldots, b_v$ and c clauses $C = \ell_1 \vee \ell_2 \vee \ell_3$. We may assume $v + c \geq 1$, so that $d = 1 + v + c \geq 2$; the trivial formula with no variable and no clause is satisfiable and is mapped to a fixed yes-instance. From such an instance we construct an instance of HomMQ: homogeneous quadratic forms $Q_1, \ldots, Q_s$ in d unknowns over $\mathbb{F}_q$ such that the formula is satisfiable if and only if the forms have a common zero $x \neq 0$.

The translation is the natural one. A truth value becomes an element of $\{0, 1\} \subset \mathbb{F}_q$, encoded by the equation $z^2 = z$. A literal is represented by a linear expression which vanishes exactly when the literal is true, and a clause is true when the product of the three expressions of its literals vanishes; since this product has degree three, an auxiliary unknown is introduced per clause to split it into equations of degree two. Finally, the constant 1 is replaced by an unknown h, for the reason explained below.

The role of the unknown h for homogenization. We recall here the standard technique of homogenization [10], and explain why it is needed. The unknown h is imposed by the pivot problem TSM (Twisted Square Membership) to which the quadratic system will be reduced in Section 5. The twisted square $a^{q+1} = a \cdot a^q$ is a homogeneous quadratic form in the coordinates of a: every monomial is a product $x_i x_j$, with no constant and no linear term. Through trace duality, only homogeneous equations of degree two can therefore be encoded into TSM. The natural equations are not homogeneous: a Boolean value z satisfies $z^2 - z = 0$, which has a linear term, and a clause involves the constant 1. We therefore homogenize: the constant 1 is replaced by a new unknown h and every linear term z by hz, which turns an equation $f(z) = 0$ of degree at most two into the homogeneous equation $h^2 f(z/h) = 0$; geometrically, this passes from an affine variety to its projective closure [10, Ch. 8]. Its effect on solutions is the following. If $h \neq 0$, every equation can be divided by h^2, and the solution divided by h is a solution of the original system with $h = 1$. If $h = 0$, the equations $z_i^2 - hz_i = 0$ become $z_i^2 = 0$, so $z_i = 0$, and likewise for the auxiliary unknowns, so that the solution is zero. Thus the homogenization creates no spurious solution, provided one asks for a *non-zero* solution, which is exactly what HomMQ does.

For instance, consider the single clause $b_1 \vee \neg b_2 \vee b_3$. Without h, it is encoded by the equations $z_i^2 - z_i = 0$ and $(1 - z_1)z_2(1 - z_3) = 0$, which cannot be fed to TSM. With h, the equations become $z_i^2 - hz_i = 0$, $w^2 - hw = 0$, $hw - (h - z_1)z_2 = 0$ and $w(h - z_3) = 0$, all homogeneous of degree two. The assignment $b_1 =$ true, $b_2 = b_3 =$ false gives the solution $(h, z_1, z_2, z_3, w) = (1, 1, 0, 0, 0)$. Over $\mathbb{F}_3$, the vector $(2, 2, 0, 0, 0) = 2 \cdot (1, 1, 0, 0, 0)$ is also a solution; it describes the same assignment, recovered by dividing by $h = 2$. Setting $h = 0$ forces $z_1 = z_2 = z_3 = w = 0$.

Concretely, the unknowns are h, one unknown z_i per variable b_i, and one auxiliary unknown

w_C per clause C, so that $d = 1 + v + c$. To a literal we associate the linear form

$$u(b_i) = h - z_i, \qquad u(\neg b_i) = z_i,$$

which, for $h = 1$, vanishes exactly when the literal is true. For a clause $C = \ell_1 \vee \ell_2 \vee \ell_3$ we write $u_j = u(\ell_j)$. The system consists of the following equations, v of the first kind and $3c$ of the other three, so that $s = v + 3c$:

$$z_i^2 - hz_i = 0, \qquad w_C^2 - hw_C = 0, \qquad hw_C - u_1u_2 = 0, \qquad w_Cu_3 = 0.$$

The first family says that z_i is a truth value, the third defines w_C as u_1u_2, and the last one then says $u_1u_2u_3 = 0$, i.e. that one literal of C is true; the second family only normalizes w_C.

Before proving that this system does what we want, let us see it on a small case. As a running example, take the formula consisting of the single clause $C = b_1 \vee \neg b_2 \vee b_3$, so that $v = 3$, $c = 1$ and $d = 5$. The unknowns are h, z_1, z_2, z_3, w_C, the literal forms are $u_1 = h - z_1$, $u_2 = z_2$, $u_3 = h - z_3$, and the system consists of the $s = v + 3c = 6$ equations

$$z_1^2 - hz_1, \quad z_2^2 - hz_2, \quad z_3^2 - hz_3, \quad w_C^2 - hw_C, \quad hw_C - (h - z_1)z_2, \quad w_C(h - z_3).$$

The assignment $b_1 = \text{true}$, $b_2 = b_3 = \text{false}$ gives the solution $(h, z_1, z_2, z_3, w_C) = (1, 1, 0, 0, 0)$, and indeed $u_1 = 0$. In the notation of Section 5, where the unknowns are numbered $x_1 = h$, $x_2 = z_1$, $x_3 = z_2$, $x_4 = z_3$, $x_5 = w_C$, the fifth equation reads $x_1x_5 - x_1x_3 + x_2x_3$, with coefficients $c_{15} = 1$, $c_{13} = -1$, $c_{23} = 1$ and all others zero.

It remains to verify that satisfying assignments correspond exactly to non-zero solutions. The only point requiring care is that a non-zero solution must have $h \neq 0$.

Proposition 14. *The formula is satisfiable if and only if the system has a non-zero solution in $\mathbb{F}_q^d$.*

Proof. Given a satisfying assignment, set $h = 1$, $z_i \in \{0, 1\}$ its value and $w_C = u_1u_2$; the last equation holds since one literal of C is true, so $u_1u_2u_3 = 0$. Conversely let x be a non-zero solution. If $h = 0$ the first two equations give $z_i = w_C = 0$, hence $x = 0$; so $h \neq 0$, and by homogeneity we may take $h = 1$. Then $z_i \in \{0, 1\}$ defines an assignment, $w_C = u_1u_2$, and $u_1u_2u_3 = 0$ says that a literal of each clause is true. □

The output of this step, the list $Q_1, \ldots, Q_s$ of the left-hand sides above, read as forms in the d unknowns $h, z_1, \ldots, z_v, (w_C)_C$, is the input of Section 5.

5 From HomMQ to TSM

We start from an instance of HomMQ, that is, homogeneous quadratic forms $Q_1, \ldots, Q_s$ in d unknowns over $\mathbb{F}_q$, for instance those produced in Section 4, and we construct an instance (N, U, W) of TSM, that is, a field $E = \mathbb{F}_{q^N}$ with $N \equiv \pm 1 \pmod 6$ and two subspaces $U, W \subset E$ given by bases, such that the forms have a common zero $x \neq 0$ if and only if some $a \in U \setminus \{0\}$ has $a^{q+1} \in W$ (Proposition 17). The plan is to encode the unknown vector $x \in \mathbb{F}_q^d$ by a single element a of a field $E = \mathbb{F}_{q^N}$, chosen so that every form $Q_k(x)$ can be read off a^{q+1} by a linear operation. Two tools make this possible. Trace duality (Section 5.1) expresses every $\mathbb{F}_q$-linear form on E as $z \mapsto \mathrm{Tr}(tz)$ and lets us prescribe the values of such a form on independent

elements. An explicit choice of exponents (Section 5.2) ensures that, when $a = \sum_i x_i \alpha^{e_i}$ is raised to the power $q+1$, each monomial $x_i x_j$ comes with its own independent coefficient in E, so that the forms can be prescribed freely. The encoding itself and the proof of the equivalence are in Section 5.3.

5.1 Trace duality

Let $E = \mathbb{F}_{q^N}$ and $\mathrm{Tr}(z) = z + z^q + \cdots + z^{q^{N-1}}$, an $\mathbb{F}_q$-linear map $E \to \mathbb{F}_q$ which is not identically zero, being a polynomial of degree $q^{N-1} < |E|$.

Lemma 15. *Every $\mathbb{F}_q$-linear form on E is $z \mapsto \mathrm{Tr}(tz)$ for a unique $t \in E$. Consequently, if $\mu_1, \ldots, \mu_r \in E$ are $\mathbb{F}_q$-linearly independent and $c_1, \ldots, c_r \in \mathbb{F}_q$, there exists $t \in E$ with $\mathrm{Tr}(t\mu_j) = c_j$ for all j, computable by linear algebra.*

Proof. If $t \neq 0$, $z \mapsto tz$ is a bijection of E, so $z \mapsto \mathrm{Tr}(tz)$ is not zero. Hence $t \mapsto \mathrm{Tr}(t\,\cdot)$ is an injective linear map between two spaces of dimension N, thus bijective. For the second claim, complete the μ_j into a basis and prescribe a linear form on it. □

5.2 Choice of exponents

Let us first see what is needed. The unknown $x \in \mathbb{F}_q^d$ will be encoded as $a = \sum_{i=1}^{d} x_i \alpha^{e_i}$, where α generates E over $\mathbb{F}_q$ and $e_1 < \cdots < e_d$ are integers to be chosen. Since $x_i^q = x_i$ for $x_i \in \mathbb{F}_q$, the twisted square expands as

$$a^{q+1} = a \cdot a^q = \Big(\sum_i x_i \alpha^{e_i}\Big)\Big(\sum_j x_j \alpha^{q e_j}\Big) = \sum_{i,j} x_i x_j \, \alpha^{e_i + q e_j}.$$

So the twisted square is the sum, over all ordered pairs (i, j), of the monomial $x_i x_j$ times the power $\alpha^{e_i + q e_j}$. We want to recover each monomial from a^{q+1} by a linear operation, and this is possible as soon as the powers $\alpha^{e_i + q e_j}$ are linearly independent over $\mathbb{F}_q$, which holds when the exponents $e_i + q e_j$ are pairwise distinct and smaller than N, since $1, \alpha, \ldots, \alpha^{N-1}$ is a basis. The condition on the exponents is thus

$$(\star) \qquad \text{the } d^2 \text{ integers } e_i + q e_j \ (1 \le i, j \le d) \ \text{ are pairwise distinct,}$$

the case $i = j$ giving $(q+1)e_i$; and the size of the largest of them will dictate N, hence the size of the whole construction. We therefore want integers satisfying $(\star)$ which are as small as possible.

The idea of the construction is that $e_i + q e_j$ should display i and j side by side, without interference. Write $i - 1$ in base q and dilate its expansion, placing its coefficients on the even positions; the odd positions are then free, and multiplying by q shifts a number by one position. Thus e_i occupies the even positions and $q e_j$ the odd ones, and the sum $e_i + q e_j$ is simply the interleaving of the two base-q expansions, from which i and j are read off. Formally, for an integer $t \ge 0$ with base-q expansion $t = \sum_k t_k q^k$, with coefficients $0 \le t_k < q$, put

$$\delta_q(t) = \sum_k t_k q^{2k},$$

and set $e_i = \delta_q(i-1)$. For $q = 2$, $t = 5 = \mathtt{101}_2$ gives $\delta_2(5) = \mathtt{10001}_2 = 17$, and the first exponents are $0, 1, 4, 5, 16$.

Lemma 16. *The integers $e_i = \delta_q(i-1)$ are strictly increasing, satisfy $(\star)$, and $e_d \le (d-1)^2$. Hence all integers of $(\star)$ are at most $(q+1)(d-1)^2$.*

Proof. δ_q is strictly increasing, since it preserves the lexicographic comparison of coefficients. Let (t_k) and (s_k) be the base-q coefficients of $i-1$ and $j-1$. Then $e_i + qe_j = \sum_k t_k q^{2k} + \sum_k s_k q^{2k+1}$: the coefficients of e_i sit on even positions, those of qe_j on odd positions, and all are smaller than q, so the two expansions interleave and this is the base-q expansion of the sum, with coefficients $t_0, s_0, t_1, s_1, \ldots$ By uniqueness of the expansion, the even positions give back $i-1$ and the odd positions $j-1$, so the ordered pair (i,j) is recovered and $(\star)$ holds. For instance, for $q=2$ and $(i,j)=(2,3)$, $e_2 + 2e_3 = 1+8 = 9 = \mathtt{1001}_2$, whose even positions read $1 = i-1$ and odd positions read $2 = j-1$. Finally $t_k^2 \ge t_k$ gives $\delta_q(t) \le \sum_k t_k^2 q^{2k} \le (\sum_k t_k q^k)^2 = t^2$, whence $e_d \le (d-1)^2$. □

5.3 The encoding and the reduction

We now fix the field and encode the unknown. Let N be the smallest integer with $N \equiv \pm 1 \pmod 6$ and $N > (q+1)(d-1)^2$, so $N = O(qd^2)$; the congruence will be used in Section 6. We build $E = \mathbb{F}_q[X]/(P)$ with P irreducible of degree N, found in deterministic polynomial time by Shoup's algorithm [33], and let α be the class of X. Since P is the minimal polynomial of α, the powers $1, \alpha, \ldots, \alpha^{N-1}$ form an $\mathbb{F}_q$-basis of E: a non-trivial relation would give a non-zero polynomial of degree less than N vanishing at α.

The quadratic-system unknown is encoded as follows. The unknown is a single vector $x = (x_1, \ldots, x_d) \in \mathbb{F}_q^d$: its coordinate $x_i \in \mathbb{F}_q$ is the value given to the i-th unknown of the system, with the numbering $x_1 = h$, $x_2, \ldots, x_{v+1}$ the values of $z_1, \ldots, z_v$ and the last c coordinates the values of the w_C, as in the example of Section 4; $Q_k(x) \in \mathbb{F}_q$ is the value of the k-th equation at this point, and we look for $x \neq 0$ with $Q_k(x) = 0$ for all k. The aim of this step is to replace the d coordinates of x by one element of the field E. Let $U = \langle \alpha^{e_1}, \ldots, \alpha^{e_d} \rangle_{\mathbb{F}_q}$, a subspace of dimension d since the α^{e_i} are distinct elements of a basis, and define

$$\phi : \mathbb{F}_q^d \longrightarrow U, \qquad x = (x_1, \ldots, x_d) \longmapsto a = x_1\alpha^{e_1} + \cdots + x_d\alpha^{e_d}.$$

Thus the x_i are the coordinates of a in the basis (α^{e_i}) of U, and ϕ is an $\mathbb{F}_q$-linear bijection: looking for x or looking for $a \in U$ is the same thing, and $a \neq 0$ if and only if $x \neq 0$. For $q=2$ and $d=2$ one has $a = x_1 + x_2\alpha$, and $a^3 = a \cdot a^2 = (x_1 + x_2\alpha)(x_1 + x_2\alpha^2) = x_1^2 + x_1x_2(\alpha + \alpha^2) + x_2^2\alpha^3$: each monomial of the system comes out with its own coefficient in E, which is the point of the encoding. In general, since $x_i^q = x_i$,

$$a^{q+1} = a \cdot a^q = \sum_{i \le j} x_i x_j \, \mu_{ij}, \qquad \mu_{ii} = \alpha^{(q+1)e_i}, \quad \mu_{ij} = \alpha^{e_i + qe_j} + \alpha^{e_j + qe_i} \ (i < j).$$

By Lemma 16 and $N > (q+1)(d-1)^2$, the elements μ_{ij} involve pairwise disjoint sets of basis vectors α^e, $e < N$, and are therefore linearly independent over $\mathbb{F}_q$.

Write $Q_k(x) = \sum_{i \le j} c_{ij}^{(k)} x_i x_j$, where $c_{ij}^{(k)} \in \mathbb{F}_q$ is the coefficient of the monomial x_ix_j in the k-th equation; the coordinates of x are the values of h, of the z_i and of the w_C, in this order, as in the example of Section 4. For instance the equation $z_1^2 - hz_1$ reads $x_2^2 - x_1x_2$, so that $c_{22} = 1$, $c_{12} = -1$ and all other coefficients vanish. Since the μ_{ij} are independent, Lemma 15

lets us prescribe a linear form on them: we choose $t_k \in E$ with $\mathrm{Tr}(t_k \mu_{ij}) = c_{ij}^{(k)}$ for all $i \le j$. Since $x_i x_j \in \mathbb{F}_q$ and the trace is $\mathbb{F}_q$-linear,

$$\mathrm{Tr}(t_k\, a^{q+1}) = \sum_{i \le j} x_i x_j \,\mathrm{Tr}(t_k \mu_{ij}) = Q_k(x) \qquad \text{for all } x \in \mathbb{F}_q^d.$$

Finally put $W = \{z \in E : \mathrm{Tr}(t_k z) = 0,\ k = 1, \dots, s\}$, a subspace computed by linear algebra.

Proposition 17. *The quadratic system has a non-zero solution if and only if (U, W) is a yes-instance of* TSM.

Proof. Let $x \in \mathbb{F}_q^d$ and $a = \phi(x) \in U$. Since ϕ is a linear bijection, $a \neq 0$ if and only if $x \neq 0$. By definition of W, $a^{q+1} \in W$ if and only if $\mathrm{Tr}(t_k a^{q+1}) = 0$ for all k, and by the choice of the t_k this reads $Q_k(x) = 0$ for all k. Hence if $x \neq 0$ is a common zero of the Q_k, then $a = \phi(x)$ is a non-zero element of U with $a^{q+1} \in W$; conversely, if $a \in U \setminus \{0\}$ satisfies $a^{q+1} \in W$, then $x = \phi^{-1}(a)$ is non-zero and $Q_k(x) = \mathrm{Tr}(t_k a^{q+1}) = 0$ for all k. □

Corollary 18. *For every fixed prime power q,* TSM *is NP-complete under deterministic polynomial-time reductions.*

Proof. TSM is in NP: a certificate is a, and the conditions $a \in U \setminus \{0\}$ and $a^{q+1} \in W$ are checked by linear algebra over $\mathbb{F}_q$. NP-hardness follows from Propositions 14 and 17, whose composition is a deterministic polynomial-time reduction from 3-SAT to TSM. □

This completes the second step. Its output is the instance (N, U, W) of TSM, with U given by the basis $\alpha^{e_1}, \dots, \alpha^{e_d}$ and W by a basis computed from the t_k; all the non-linearity of the quadratic system is now carried by the single operation $a \mapsto a^{q+1}$, and the two remaining conditions, $a \in U$ and $a^{q+1} \in W$, are linear. The next section shows how a Gabidulin decoding instance can impose exactly these three things.

6 From TSM to GabDec_1

6.1 What has to be shown

Section 5 turned a homogeneous quadratic system into an instance (N, U, W) of TSM: a field $E = \mathbb{F}_{q^N}$ with $N \equiv \pm 1 \pmod 6$, and two subspaces $U, W \subset E$ given by bases, such that the system has a non-zero solution if and only if some $a \in U \setminus \{0\}$ has $a^{q+1} \in W$. All the non-linearity of the original problem is now carried by the twisted square $a \mapsto a^{q+1}$, while the conditions $a \in U$ and $a^{q+1} \in W$ are linear. In this last step we start from such an instance and construct an instance (g, y) of GabDec_1, that is, a field $K = \mathbb{F}_{q^m}$, a vector $g \in K^n$ of rank n and a received word $y \in K^n$, such that some $\lambda \in K$ satisfies $\mathrm{rk}(y - \lambda g) \le n - 2$ if and only if some $a \in U \setminus \{0\}$ has $a^{q+1} \in W$. The received word is not given, it is designed.

By Lemma 10, the decoding instance is a yes-instance exactly when some plane of the support satisfies the eigenplane equation. One direction consists in exhibiting such a plane from a solution of TSM. The converse is the heart of the proof: we show that every solution plane is necessarily of the form $\langle a, \tau a^{q+1} \rangle$ with $a \in U \setminus \{0\}$ and $a^{q+1} \in W$. The construction and the proof are organized as follows. In Section 6.2 we build a cubic extension $K = E(\tau)$ of E, in which one equality splits into three independent equalities in E, one per coefficient

on $1, \tau, \tau^2$; this is what allows a single eigenplane equation to impose several conditions. In Section 6.3 we choose the code, through its support $G = U \oplus \tau W$, so that the two linear conditions of TSM are built into the code itself. In Section 6.4 we choose the received word, $\tilde{y}(a + \tau b) = a^{q^2} + \tau b^q$, made of two Frobenius twists with different exponents, and check that it is a legitimate received word. Finally, in Section 6.5, we read the eigenplane equation coefficient by coefficient: the coefficients on 1 and τ^2 force the shape $\langle a, \tau b\rangle$, the coefficient on τ forces $b \in \mathbb{F}_q^* a^{q+1}$, and this proves the equivalence (Proposition 23) and the main theorem.

6.2 The field K

We first build the field in which the code will live. Fix once and for all an irreducible polynomial $R \in \mathbb{F}_q[Y]$ of degree 3; it depends only on q, and it exists since the field $\mathbb{F}_{q^3}$ exists and the minimal polynomial over $\mathbb{F}_q$ of a generator of its cyclic multiplicative group is irreducible of degree 3 (for $q = 2$, $Y^3 + Y + 1$); it is found by exhaustive search in constant time. Put $K = E[Y]/(R)$ and let τ be the class of Y.

Lemma 19. *K is a field, $K = \mathbb{F}_{q^{3N}}$, and $1, \tau, \tau^2$ is a basis of K over E.*

Proof. An irreducible polynomial of degree 3 over $\mathbb{F}_q$ factors over $\mathbb{F}_{q^N}$ into $\gcd(3, N)$ irreducible factors of equal degree, and $\gcd(3, N) = 1$ since $N \equiv \pm 1 \pmod 6$. Hence R stays irreducible over E, $[K : E] = 3$, and $1, \tau, \tau^2$ is a basis by the argument used for α. □

Every $z \in K$ is thus written uniquely $z = z_0 + z_1\tau + z_2\tau^2$ with $z_i \in E$, and an equality in K is equivalent to three equalities in E, one for each power of τ; we call z_i the component of z on τ^i.

6.3 The code

With K in hand we choose the code, that is, its support. Recall from Section 2 that a code $\mathrm{Gab}(g, 1)$ is determined by the vector $g = (g_1, \ldots, g_n)$, whose coordinates are $\mathbb{F}_q$-linearly independent, and that its *support* is the $\mathbb{F}_q$-space $G = \langle g_1, \ldots, g_n\rangle_{\mathbb{F}_q} \subset \mathbb{F}_{q^m}$ of dimension n spanned by these coordinates: g is a basis of G, a received word is an $\mathbb{F}_q$-linear map $\tilde{y} : G \to \mathbb{F}_{q^m}$, and decoding asks for a plane of G on which $\tilde{y}$ acts as a scalar. Choosing the code thus amounts to choosing G together with a basis. Since the expected plane contains a vector $a \in U$ and a vector τb with $b \in W$, we take

$$G = U \oplus \tau W = \{a + \tau b : a \in U,\ b \in W\} \subset K.$$

The sum is direct, because 1 and τ are linearly independent over E, so, writing $r = \dim W$ (with $N - s \le r \le N$, since W is cut out by s linear conditions), $n := \dim_{\mathbb{F}_q} G = \dim U + \dim W = d + r \le d + N$. We choose the extension field $\mathbb{F}_{q^m} = K$ with $m = 3N$, and for $g \in K^n$ the concatenation of the basis $\alpha^{e_1}, \ldots, \alpha^{e_d}$ of U and of $\tau w_1, \ldots, \tau w_r$ for a basis $w_1, \ldots, w_r$ of W (computed by linear algebra from the t_k); this is an $\mathbb{F}_q$-basis of G, so $\mathrm{rk}(g) = n$. Note that $n \ge d \ge 2$, so that radius $n - 2$ makes sense. Moreover $N > (q + 1)(d - 1)^2 \ge d$ since $d \ge 2$, hence

$$n \le d + N \le 2N < 3N = m,$$

so that the code satisfies the length constraint $n \le m$ of Gabidulin codes.

6.4 The received word

The code being fixed, it remains to choose the received word; this is where the twisted square is produced. Since (g, y) is ours to choose, and since by Section 2 received words correspond exactly to $\mathbb{F}_q$-linear maps $G \to K$, we define the map $\tilde{y}$ and deduce y from it. Every element of G is uniquely $a + \tau b$ with $a \in U$, $b \in W$, so it suffices to give $\tilde{y}(a + \tau b)$. We set

$$(*) \qquad \tilde{y}(a + \tau b) = a^{q^2} + \tau\, b^q.$$

Lemma 20. *The map $(*)$ is $\mathbb{F}_q$-linear. The corresponding received word $y_j = \tilde{y}(g_j)$ is $y_j = \alpha^{e_i q^2}$ for $g_j = \alpha^{e_i}$ and $y_j = \tau w_l^q$ for $g_j = \tau w_l$, and is computed in polynomial time.*

Proof. The map $a + \tau b \mapsto (a, b)$ is linear; $a \mapsto a^{q^2}$ and $b \mapsto b^q$ are additive and satisfy $(\lambda a)^{q^2} = \lambda a^{q^2}$ for $\lambda \in \mathbb{F}_q$; the multiplication by τ is linear. □

The two Frobenius twists have distinct exponents on purpose: equal exponents on a and b would force the plane to be $\langle a, \tau b\rangle$ as well, but would only give $b \in \mathbb{F}_q^* a$, whereas the exponents q^2 and q produce $b \in \mathbb{F}_q^* a^{q+1}$. For $x = a + \tau b$ and $x' = a' + \tau b'$ in G, the components of $\tilde{y}(x)x'$ on $1, \tau, \tau^2$ are

$$a^{q^2} a', \qquad a^{q^2} b' + b^q a', \qquad b^q b',$$

of degree at most 2 in τ, so no reduction modulo R occurs.

6.5 The shape of solution planes

We prove the converse direction by showing that every solution plane has the form $\langle a, \tau b\rangle$. The first lemma is the elementary fact that makes the coefficients on 1 and τ^2 useful.

Lemma 21. *Let $a, a' \in E$ be non-zero with $a^{q^2} a' = a'^{q^2} a$. Then $a' \in \mathbb{F}_q\, a$.*

Proof. Put $u = a'/a$. Dividing by $a^{q^2} a$ gives $u^{q^2} = u$. Since $u \in \mathbb{F}_{q^N}$, also $u^{q^N} = u$. Write $N = 2k + 1$; applying k times $u \mapsto u^{q^2}$ gives $u^{q^{2k}} = u$, hence $u = u^{q^N} = (u^{q^{2k}})^q = u^q$, and $u \in \mathbb{F}_q$. □

This is the only place where the parity of N is used.

Lemma 22. *If a plane $L \subset G$ satisfies $L \subset \mathrm{Ker}(\tilde{y} - \lambda)$ for some $\lambda \in K$, then $L = \langle a, \tau b\rangle$ with $a \in U \setminus \{0\}$ and $b \in W \setminus \{0\}$.*

Proof. By Lemma 11, for all $x = a + \tau b$ and $x' = a' + \tau b'$ in L we have $\tilde{y}(x)x' = \tilde{y}(x')x$, and the components on 1 and τ^2 give $a^{q^2} a' = a'^{q^2} a$ and $b^q b' = b'^q b$. Let $A = \{a \in U : \exists b,\ a + \tau b \in L\}$, the image of L under the linear map $a + \tau b \mapsto a$; it is a subspace of U. If $\dim A \geq 2$, take $a, a' \in A$ linearly independent and $x, x' \in L$ realizing them: the first relation and Lemma 21 give $a' \in \mathbb{F}_q a$, a contradiction. Hence $\dim A \leq 1$, and likewise $\dim B \leq 1$ for $B = \{b \in W : \exists a,\ a + \tau b \in L\}$, using $(b'/b)^q = b'/b$. The map $L \to A \times B$, $a + \tau b \mapsto (a, b)$, is linear and injective, so $2 = \dim L \leq \dim A + \dim B \leq 2$. Thus $A = \mathbb{F}_q a$, $B = \mathbb{F}_q b$ with $a, b \neq 0$, the map is bijective, and a and τb belong to L. □

Note that the argument never assumes that a particular basis of L has non-zero components: it works on the projections A and B of the whole plane. With the shape of solution planes in hand, the coefficient on τ finishes the job, and the converse direction is a direct computation.

Proposition 23. *There exists $\lambda \in K$ with $\mathrm{rk}(y - \lambda g) \leq n - 2$ if and only if there exists $a \in U \setminus \{0\}$ with $a^{q+1} \in W$.*

Proof. Assume the decoding instance is a yes-instance. By Lemmas 9 and 22, some plane $\langle a, \tau b\rangle$ with $a \in U \setminus \{0\}$ and $b \in W \setminus \{0\}$ lies in $\mathrm{Ker}(\tilde{y} - \lambda)$. The component on τ of the equality $\tilde{y}(a)\,\tau b = \tilde{y}(\tau b)\,a$ reads $a^{q^2} b = a b^q$. Dividing by ab gives $a^{q^2-1} = b^{q-1}$, and since $a^{q^2-1} = (a^{q+1})^{q-1}$, the element $\gamma = b/a^{q+1}$ satisfies $\gamma^{q-1} = 1$, so $\gamma \in \mathbb{F}_q^*$; this is where the exponent $q+1$ of TSM arises. Since W is an $\mathbb{F}_q$-subspace, $a^{q+1} = \gamma^{-1} b \in W$.

Conversely let $a \in U \setminus \{0\}$ with $a^{q+1} \in W$, put $b = a^{q+1}$, so that $\tau b \in G$, and $\lambda = a^{q^2-1}$. Then $\tilde{y}(a) = a^{q^2} = \lambda a$ and $\tilde{y}(\tau b) = \tau a^{q^2+q} = \lambda \tau b$. By linearity $\langle a, \tau b\rangle$, a plane since the sum $U \oplus \tau W$ is direct, lies in $\mathrm{Ker}(\tilde{y} - \lambda)$, and Lemma 9 gives $\mathrm{rk}(y - \lambda g) \leq n - 2$. □

6.6 Proof of Theorem 13

All three steps are now established, and we can prove the main theorem, which we recall.

Theorem 13. *For every fixed prime power q, GabDec_1 is NP-complete. More precisely, a 3-SAT formula with v variables and c clauses is mapped in deterministic polynomial time to an instance with $m = 3N$ and $n \leq N + d$, where $d = 1 + v + c$, $N \equiv \pm 1 \pmod 6$ and $N = O(q\,d^2)$.*

Proof. Membership in NP. Given (g, y), a certificate is $\lambda \in \mathbb{F}_{q^m}$; the rank of $y - \lambda g$ is computed by Gaussian elimination over $\mathbb{F}_q$ on its $m \times n$ matrix of coordinates, in polynomial time.

NP-hardness. Let Φ be a 3-SAT formula with v variables and c clauses, and $d = 1 + v + c$. Section 4 produces homogeneous quadratic forms $Q_1, \ldots, Q_s$ in d unknowns, with $s = v + 3c$, such that Φ is satisfiable if and only if they have a common zero $x \neq 0$ (Proposition 14). Section 5 produces from them an instance (N, U, W) of TSM, with $N \equiv \pm 1 \pmod 6$ and $N = O(qd^2)$, such that the forms have a common zero $x \neq 0$ if and only if some $a \in U \setminus \{0\}$ has $a^{q+1} \in W$ (Proposition 17). Section 6 produces from (N, U, W) an instance (g, y) of GabDec_1 over $K = \mathbb{F}_{q^{3N}}$, of length $n = \dim U + \dim W \leq d + N$, such that some λ satisfies $\mathrm{rk}(y - \lambda g) \leq n - 2$ if and only if (N, U, W) is a yes-instance (Proposition 23). Composing the three equivalences, Φ is satisfiable if and only if (g, y) is a yes-instance of GabDec_1.

Polynomial time. Each object of the construction is computed deterministically in time polynomial in $v + c$, with the sizes of Table 1: the exponents e_i are given by a closed formula (Lemma 16); the irreducible polynomial of degree N defining E is found by Shoup's algorithm [33]; the polynomial R of degree 3 defining K depends only on q; the elements t_k, the basis of W, the vector g and the received word y are obtained by linear algebra over $\mathbb{F}_q$ in dimension $O(m) = O(qd^2)$ (Lemmas 15 and 20). Since q is fixed, $m, n = O(d^2)$, and the $2n$ elements of $\mathbb{F}_{q^m}$ forming g and y have m coordinates each over $\mathbb{F}_q$, so that the output instance has size $|(g, y)| = O(nm) = O(d^4)$ symbols of $\mathbb{F}_q$, polynomial in the size of the formula. □

Remark 24 (representation of finite fields). The answer does not depend on how finite fields are represented. We take $E = \mathbb{F}_q[X]/(P)$, with P found by Shoup's deterministic algorithm

[33] in time polynomial in N for fixed q, and $K = E[Y]/(R)$. If the input must give $\mathbb{F}_{q^m}$ by a single irreducible polynomial Q of degree m, one computes Q by the same algorithm and an explicit isomorphism $\psi : K \to \mathbb{F}_q[Z]/(Q)$ by Lenstra's deterministic algorithm [28], and outputs $(\psi(g), \psi(y))$. Since ψ restricts to an automorphism of $\mathbb{F}_q$, it is semilinear over $\mathbb{F}_q$ and preserves rank weights; as $\psi(y - \lambda g) = \psi(y) - \psi(\lambda)\psi(g)$, the two instances have the same answer.

Table 1: Sizes in the reduction, for a formula with v variables and c clauses, $d = 1 + v + c$, and fixed q.

Object	Size	Construction
exponents e_i	$e_d \le (d-1)^2$	$\delta_q(i-1)$ (Lemma 16)
field $E = \mathbb{F}_{q^N}$	$N = O(qd^2)$, $N \equiv \pm 1 \pmod 6$	irreducible polynomial [33]
field $K = E(\tau)$	$m = 3N$	fixed degree-3 polynomial
t_k, W, g, y	polynomial	linear algebra
code	$n = d + r \le N + d$ with $r = \dim W$; $k = 1$; radius $n-2$	$\mathrm{Gab}(g, 1)$

7 Consequences

7.1 Complexity consequences

We first derive the consequence for Gabidulin codes, then turn to the general problems RSD and RMD from Section 2. Maximum-likelihood decoding of a code consists in finding, for a received word, a closest codeword.

Corollary 25. *For every fixed prime power q, maximum-likelihood decoding of Gabidulin codes is NP-hard under deterministic polynomial reductions, already for codes of dimension $k = 1$.*

Proof. For $k = 1$, a maximum-likelihood decoder applied to (g, y) returns some λ_0 with $\mathrm{rk}(y - \lambda_0 g) = \min_\lambda \mathrm{rk}(y - \lambda g)$. Comparing this rank with $n - 2$ decides GabDec_1, which is NP-complete by Theorem 13. □

This holds for the simplest codes of the family, which have dimension one and minimum distance n.

We next consider RSD and RMD.

Corollary 26. RSD*, the rank syndrome decoding problem for $\mathbb{F}_{q^m}$-linear codes, is NP-complete under deterministic polynomial reductions.*

Proof. From an instance (g, y) of GabDec_1, compute a parity-check matrix H of $\mathrm{Gab}(g, 1)$ and $s = Hy^\top$. The solutions e of $He^\top = s$ are exactly the vectors $y - \lambda g$, so a solution of rank at most $n - 2$ exists if and only if the instance of GabDec_1 is a yes-instance. □

Corollary 27. RMD*, the rank minimum distance problem for $\mathbb{F}_{q^m}$-linear codes, is NP-complete under deterministic polynomial reductions, already for codes of dimension* 2*.*

Proof. From (g, y) consider $C' = \{\mu y + \lambda g : \mu, \lambda \in \mathbb{F}_{q^m}\}$ and $w = n - 2$. If $y \in \mathbb{F}_{q^m} g$, which is tested by linear algebra, the instance of GabDec_1 is a yes-instance and we output any fixed yes-instance; otherwise C' has dimension 2. Multiplication by a non-zero scalar is an $\mathbb{F}_q$-linear bijection of $\mathbb{F}_{q^m}$, hence preserves rank. A codeword with $\mu = 0$ and $\lambda \neq 0$ therefore has rank $\mathrm{rk}(g) = n$, while a codeword with $\mu \neq 0$ equals $\mu(y - \lambda' g)$ with $\lambda' = -\lambda/\mu$ and has rank $\mathrm{rk}(y - \lambda' g)$. Hence C' has a non-zero codeword of rank at most $n-2$ if and only if the instance of GabDec_1 is a yes-instance. □

These problems underlie rank-based cryptography. Gaborit and Zémor [19] established their hardness through a randomized reduction from Hamming decoding; Corollaries 26 and 27 give NP-completeness under deterministic reductions. Their reduction covers constant rate and small weight, ours is restricted to dimension one or two and to large radius; the two results are complementary. The result can also be seen as the rank-metric counterpart of the Guruswami–Vardy theorem [26].

7.2 Comparison with the Hamming metric

It is instructive to compare with the Hamming metric. There, any linear code of fixed dimension k is decoded at radius $n - k - 1$ in polynomial time: a codeword at that distance agrees with the received word on $k+1$ positions, and one may enumerate the $\binom{n}{k+1}$ candidate position sets and solve a linear system for each. For $k = 1$ the Reed–Solomon code is the repetition code and the problem is trivial; this is why the Guruswami–Vardy theorem needs a growing dimension. In the rank metric the agreement set is an $\mathbb{F}_q$-subspace rather than a subset, there are $q^{\Theta(kn)}$ candidates, and Theorem 13 shows that the problem is hard already for $k = 1$. The same contrast explains why the Guruswami–Vardy reduction does not transfer: it encodes a subset-sum instance into the freedom of choosing which positions to keep, a freedom which does not exist for subspaces, so that the hard constraints must be written, as here, into the field structure of $\tilde{y}$.

Several questions remain open and are discussed in Section 8.

8 Discussion and open questions

The reduction proves hardness in a specific regime: dimension one, radius $n - 2$, and an extension degree $m \approx 3n$. Each of these three parameters raises a natural question, namely how far the radius can be lowered, whether the extension degree can be brought down to the values used in cryptography, and whether the dimension can be increased. We discuss them in turn, together with directions that seem interesting to explore.

Below radius $n - 2$. For $k = 1$, radius $n - r - 1$ asks for an eigenspace of dimension $r + 1$ instead of a plane. One might try to use $r+1$ summands in the support, $G = U \oplus \omega_1 W \oplus \cdots \oplus \omega_r W$, with $\tilde{y}(a + \sum_i \omega_i b_i) = a^{q^2} + \sum_i \omega_i b_i^q$, where the ω_i would be powers of τ whose pairwise products are linearly independent over E; a Sidon set of exponents could provide this with an extension of moderate degree. If the coefficientwise reading of the eigenplane equation were to go through as in Section 6, the same pivot problem might give hardness at radius $n-r-1$, at the price of a larger extension degree. Whether this works, down to which radius, and with which trade-off between the radius and m, remains to be investigated.

Square codes. The parameters produced by the reduction are not those most often used in practice: our instances have $m \approx 3n$, whereas rank-based cryptosystems frequently work with square or nearly square codes, $m = n$ or m close to n, which also give the smallest extension field for a given length. The complexity of decoding in this regime is open. A heuristic count suggests that radius $n-2$ may not be the right place to look for it: a random word has on average about $q^{2(n-2)-m}$ scalars λ within that distance, which is large when $m < 2(n-2)$. If yes-instances are indeed typical in this regime, which the expectation alone does not prove and which would not exclude worst-case hardness, the natural question for square codes would be at smaller radius.

Higher dimensions. Decoding $\mathrm{Gab}(g,k)$ at radius $n-k-1$ asks for a $(k+1)$-dimensional space on which $\tilde{y}$ agrees with a q-polynomial of q-degree less than k. A direction that seems promising is to compose a dimension-one instance with linearized polynomials of q-degree one, such as $P(x) = x^q - \delta^{q-1}x$: when $G \subseteq P(\mathbb{F}_{q^m})$, which requires a suitable choice of δ since $\dim P^{-1}(G) = \dim(G \cap P(\mathbb{F}_{q^m})) + 1$, replacing $(G, \tilde{y})$ by $(P^{-1}(G), \tilde{y} \circ P)$ would raise both the dimension of the agreement space and the q-degree by one, whereas merely adding coordinates cannot help. The difficulty would be to control the solutions that such a lifting may create without coming from the original instance; if they could be characterized and avoided by a suitable choice of δ, the present core could serve as the base case of an induction on k.

9 Conclusion

Decoding a Gabidulin code of dimension one at radius $n-2$, the first radius at which the question is not trivial, is NP-complete. Maximum-likelihood decoding of Gabidulin codes is therefore NP-hard already in dimension one, where its Hamming-metric counterpart is easy, and rank syndrome decoding and rank minimum distance for $\mathbb{F}_{q^m}$-linear codes are NP-complete under deterministic reductions, where only a randomized reduction was known. The proof rests on a single idea: once the received word is read as an $\mathbb{F}_q$-linear map, decoding becomes the search for an eigenplane, and two Frobenius twists on the support $U \oplus \tau W$ turn that eigenplane equation into the pivot problem TSM, which encodes 3-SAT.

Our result is a first step towards understanding the complexity of decoding Gabidulin codes beyond the unique decoding radius. It raises natural questions on how far hardness extends, in the dimension of the code, in the decoding radius, and towards the square parameters $m \approx n$ of cryptography, which will require further investigation.

Acknowledgment.

AI tools (Claude, Anthropic, and ChatGPT, OpenAI) were used during the preparation of this manuscript for language editing, LaTeX assistance, and exploratory discussions. All mathematical statements, proofs, and conclusions were independently verified by the author, who takes full responsibility for the content.

References

[1] Aragon, N., Gaborit, P., Hauteville, A., Ruatta, O., Zémor, G.: Low rank parity check codes: new decoding algorithms and applications to cryptography. IEEE Trans. Inf. Theory **65**(12), 7697–7717 (2019)

[2] Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: a rank metric based signature scheme. In: EUROCRYPT 2019, LNCS 11478, pp. 728–758 (2019)

[3] Aragon, N., Blazy, O., Deneuville, J.-C., Gaborit, P., Hauteville, A., Ruatta, O., Tillich, J.-P., Zémor, G., et al.: ROLLO – Rank-Ouroboros, LAKE and LOCKER. Submission to the NIST post-quantum cryptography standardization process (2019)

[4] Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Zémor, G., et al.: Rank Quasi-Cyclic (RQC). Submission to the NIST post-quantum cryptography standardization process (2019)

[5] Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A.: On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory **24**(3), 384–386 (1978)

[6] Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. J. Comput. Syst. Sci. **58**(3), 572–596 (1999)

[7] Cheng, Q.: Hard problems of algebraic geometry codes. IEEE Trans. Inf. Theory **54**(1), 402–406 (2008)

[8] Cheng, Q., Wan, D.: On the list and bounded distance decodability of Reed–Solomon codes. SIAM J. Comput. **37**(1), 195–209 (2007)

[9] Coggia, D., Couvreur, A.: On the security of a Loidreau rank metric code based encryption scheme. Des. Codes Cryptogr. **88**, 1941–1957 (2020)

[10] Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms, 4th edn. Undergraduate Texts in Mathematics, Springer (2015)

[11] Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. J. Combin. Theory Ser. A **25**, 226–241 (1978)

[12] Dumer, I., Micciancio, D., Sudan, M.: Hardness of approximating the minimum distance of a linear code. IEEE Trans. Inf. Theory **49**(1), 22–37 (2003)

[13] Faure, C., Loidreau, P.: A new public-key cryptosystem based on the problem of reconstructing p-polynomials. In: Coding and Cryptography, WCC 2005, LNCS 3969, pp. 304–315 (2006)

[14] Forbes, M.A., Shpilka, A.: On identity testing of tensors, low-rank recovery and compressed sensing. In: STOC 2012, pp. 163–172 (2012)

[15] Fraenkel, A.S., Yesha, Y.: Complexity of problems in games, graphs and algebraic equations. Discrete Appl. Math. **1**, 15–30 (1979)

[16] Gabidulin, E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**(1), 1–12 (1985)

[17] Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: WCC 2013 (2013)

[18] Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their application in cryptology. In: EUROCRYPT 1991, LNCS 547, pp. 482–489 (1991)

[19] Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Inf. Theory **62**(12), 7245–7252 (2016)

[20] Gandikota, V., Ghazi, B., Grigorescu, E.: NP-hardness of Reed–Solomon decoding and the Prouhet–Tarry–Escott problem. In: FOCS 2015, pp. 760–773 (2015)

[21] Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman (1979)

[22] Guruswami, V., Kopparty, S.: Explicit subspace designs. In: FOCS 2013, pp. 608–617 (2013)

[23] Guruswami, V., Sudan, M.: Improved decoding of Reed–Solomon and algebraic-geometry codes. IEEE Trans. Inf. Theory **45**(6), 1757–1767 (1999)

[24] Guruswami, V., Xing, C.: List decoding Reed–Solomon, algebraic-geometric, and Gabidulin subcodes up to the Singleton bound. In: STOC 2013, pp. 843–852 (2013)

[25] Guo, Z., Xing, C., Yuan, C., Zhang, Z.: Random Gabidulin codes achieve list decoding capacity in the rank metric. In: FOCS 2024, pp. 1846–1873 (2024)

[26] Guruswami, V., Vardy, A.: Maximum-likelihood decoding of Reed–Solomon codes is NP-hard. IEEE Trans. Inf. Theory **51**(7), 2249–2256 (2005)

[27] Koetter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory **54**(8), 3579–3591 (2008)

[28] Lenstra, H.W., Jr.: Finding isomorphisms between finite fields. Math. Comp. **56**(193), 329–347 (1991)

[29] Loidreau, P.: A new rank metric codes based encryption scheme. In: PQCrypto 2017, LNCS 10346, pp. 3–17 (2017)

[30] Overbeck, R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptology **21**(2), 280–301 (2008)

[31] Renner, J., Puchinger, S., Wachter-Zeh, A.: LIGA: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. Des. Codes Cryptogr. **89**, 1279–1319 (2021)

[32] Raviv, N., Wachter-Zeh, A.: Some Gabidulin codes cannot be list decoded efficiently at any radius. IEEE Trans. Inf. Theory **62**(4), 1605–1615 (2016)

[33] Shoup, V.: New algorithms for finding irreducible polynomials over finite fields. Math. Comp. **54**(189), 435–447 (1990)

[34] Silva, D., Kschischang, F.R., Koetter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inf. Theory **54**(9), 3951–3967 (2008)

[35] Vardy, A.: The intractability of computing the minimum distance of a code. IEEE Trans. Inf. Theory **43**(6), 1757–1766 (1997)

[36] Wachter-Zeh, A.: Bounds on list decoding of rank-metric codes. IEEE Trans. Inf. Theory **59**(11), 7268–7277 (2013)