# Applications of Bruhat-Chevalley-Renner Decomposition to Metric-Aware Code-Based Cryptography

Mahir Bilen Can* Eli Naig†

November 15, 2025

**Abstract**

We introduce *metric-aware* code-based cryptography by moving beyond the Hamming metric to the Niederreiter-Rosenbloom-Tsfasman (NRT) and sum-rank metrics and by exploiting their linear isometry groups via Bruhat-Chevalley-Renner decompositions. On the structural side, we give isometry-invariant distance tests: a parity-check *prefix-rank* test for single-chain NRT, its *multi-prefix* extension for block-NRT, and a *block rank-profile* test for sum-rank. We also analyze orbit structure under the relevant isometry subgroups and prove NP-hardness of a block-NRT canonicalization problem via a reduction from Exact-3-Cover, pinning down the difficulty of public "structure recovery."

On the design side, we propose an *inner-outer* Niederreiter cryptosystem that couples a short rowwise single-chain NRT inner code with $k_V$ outer binary Goppa codes across columns. For the resulting matrix code we prove a distance guarantee $d_{\mathrm{NRT}} \geq \delta_V \cdot \min_t d^{(t)}$ and give a simple two-stage decoder (outer Goppa per coordinate, then inner per column). Public keys are dense, obfuscated parity-checks $M = SH_{\mathrm{sys}}(PD)$ drawn from a metric-preserving subgroup, preserving decodability while hiding structure. Finally, we reduce NRT and sum-rank syndrome decoding to classical Hamming/Rank decoding, yielding *one-wayness* of the public syndrome map at standard regimes.

**Key words.** Code-based cryptography; Niederreiter cryptosystem; Bruhat-Chevalley-Renner decomposition; NRT metric; sum-rank metric; product binary Goppa codes.

## 1 Introduction

Large-scale quantum computers threaten number-theoretic cryptosystems (RSA, ECC) via Shor's algorithm, accelerating the study and standardization of post-quantum cryptography (PQC). Code-based systems, in particular the McEliece and Niederreiter cryptosystems, have stood resilient since 1978 and feature prominently in the NIST PQC process [26, 3, 31]. Their main practical drawback is public-key size. Unless they are carefully implemented, algebraic compression (using quasi-cyclic/dyadic codes) leads to structural distinguishers and attacks [4, 11, 9].

Nevertheless, code-based cryptosystems remain attractive when bandwidth or latency constraints are not dominant and when public keys can be distributed once and reused. In such settings, Classic McEliece offers very small ciphertexts and fast decapsulation, making end-to-end

*Department of Mathematics, Tulane University, New Orleans, LA 70118 USA. Email: mcan@tulane.edu
†Department of Mathematics, Tulane University, New Orleans, LA 70118 USA. Email: enaig@tulane.edu

costs competitive [8]. Indeed, recent assessments by NIST emphasize that large key size, rather than cryptanalytic concerns, is the primary deployment hurdle, while confidence in the security of Classic McEliece remains high [1, 27]. Moreover, there is growing ecosystem support and experimentation: TLS and SSH prototypes and drafts accommodate larger key shares for code-based KEMs, and several projects (such as Rosenpass, Mullvad VPN, Crypto4A) have explored or integrated Classic McEliece in practice [32, 18, 22].

This work explores a complementary lever, that is a *metric-aware* analysis and design. By working in metrics beyond Hamming, notably the NRT and sum-rank metrics, and by exploiting their isometry groups through matrix decompositions (such as Bruhat-Chevalley-Renner (BCR) decompositions), we obtain parity-check distance tests, orbit, hence canonical-forms, and cryptographic constructions that retain the robustness of classical designs while broadening the design space. The first metric we utilize, that is the NRT metric, originates in the works of Niederreiter [29, 30] and Tsfasman-Rosenblyum [39], going back to 1990s. The second metric we use, that is the sum-rank metric, blends Hamming and rank metrics and provides the natural distance measure for multi-shot network coding. Both metrics admit rich linear isometry groups. In the former case, we have upper-triangular Borel actions (per block) coupled with block permutations. For the sum-rank metrics, we have left/right actions together with block permutations. These symmetries make them natural targets for BCR-based orbit decompositions and rank-profile invariants.

We now proceed to explain in more detail the main contributions of our paper. Our results can be organized into three main threads labeled $A, B$, and $C$.

We now proceed to explain in more detail the main contributions of our paper. Our results can be organized into three main threads labeled $A, B$, and $C$.

*(A) Distance tests and generic structure.*

- Single-chain NRT metric: We prove a *prefix-rank criterion* that reads the minimum NRT distance directly from parity-check prefixes (Proposition 3.2). We identify the *big* $B_r(\mathbb{F}_q) \times B_n(\mathbb{F}_q)$ *cell* in $M^{\text{full}}_{r\times n}(\mathbb{F}_q)$ (Proposition 3.4) and deduce that uniformly random $[n,k]_q$ codes are MDS NRT with probability $1 - o_q(1)$ (Theorem 3.7).

- Block-NRT metric: We generalize to a *multi-prefix rank criterion* invariant under the full block-NRT isometry group $G_n = (B_\ell(\mathbb{F}_q))^m \rtimes \mathcal{S}_m$ (Proposition 4.1). We also parameterize right-isometry orbits by *block-rook patterns* and give canonical representatives for the $GL_r(\mathbb{F}_q) \times G_n$ double cosets (Proposition 4.5).

- Sum-rank metric: We obtain a *block rank-profile test* for the minimum sum-rank distance from parity checks, invariant under a natural isometry subgroup $\mathcal{G}_{\text{SR}}$ (Proposition 5.2).

*(B) Algorithms, hardness, and attacks.*

- We formalize the classical *one-prefix attack* in the single-chain NRT setting and explain why it fails in block-NRT and sum-rank settings due to the exponential number of candidate multi-prefixes / rank-profiles (Algorithm 1 and Remark 7.1).

- We prove *NP-hardness* of a *Block-NRT Canonical Form* problem via a reduction from Exact-3-Cover (X3C), pinning down the difficulty of canonicalizing $GL_r(\mathbb{F}_q)\times G_n$ orbits (Section 8).

- We reduce *NRT* and *sum-rank* syndrome decoding to classical Hamming/Rank decoding (Theorems 9.4-9.5), implying worst-case NP-hardness and establishing *one-wayness* of the public syndrome map at standard parameter regimes (Corollary 9.7).

*(C) A Niederreiter design with provable distance/decoding.*

- We propose an *inner-outer* design that couples a short *rowwise single-chain NRT* (RT) inner code $V$ across the $\ell$ rows with $k_V$ outer *binary Goppa* codes across the $m$ columns (Definition 10.1). For the resulting matrix code we prove the distance guarantee

$$d_{\mathrm{NRT}}\big(\mathcal{C}_{\text{NRT-GC}}\big) \;\geq\; \delta_V \cdot \min_{t\in[k_V]} d^{(t)},$$

  where $\delta_V$ is the inner single-chain NRT distance and $d^{(t)}$ are the outer Hamming distances (Theorem 10.2). We also give a systematic parity-check and obfuscation recipe that yields statistically dense public keys while preserving decodability (Section 10.2), and a simple two-stage decoder (outer per $t$, then inner per column) (Subsection 10.3).

- We provide computable lower bounds for block-NRT and sum-rank distances from both generator and parity-check viewpoints to aid parameter selection (per Section 6).

Poset and chain metrics have long been studied for coding theory and decoding invariance; our use of Borel-type actions and orbit tools follows this line. For sum-rank, our distance tests sit alongside the MSRD/linearized Reed-Solomon landscape used in multi-shot network coding. We are not aware of prior work coupling an inner single-chain NRT code with outer binary Goppa codes to obtain a provable *multiplicative* block-NRT distance and a two-stage Niederreiter decoder.

The structure of our paper is as follows: Section 2 reviews preliminaries and poset/sum-rank metrics. Section 3 develops the prefix-rank criterion and the big-cell/MDS NRT results. Section 4 gives the multi-prefix test and block-rook orbit structure. Section 5 proves the sum-rank rank-profile test. Section 6 provides distance lower bounds from generators and parity checks. Section 7 discusses metric-based cryptosystems and analyzes the one-prefix attack. Section 8 establishes NP-hardness of Block-NRT canonicalization. Section 9 gives decoding-hardness reductions and the syndrome one-wayness corollary. Section 10 presents the inner-outer NRT-Goppa construction with distance/decoding guarantees.

## 2 Preliminaries

**Notation.** For $\ell \in \mathbb{Z}_{>0}$ write $[\ell] := \{1, \ldots, \ell\}$. We use standard asymptotics: for $m, n \in \mathbb{Z}_{>0}$, the relation $m(n) = \Theta(n)$ means that there exist constants $c_1, c_2 > 0$ and $n_0$ such that $c_1 n \leq m(n) \leq c_2 n$ for all $n \geq n_0$. Throughout, $\mathbb{F}_q$ denotes the finite field with $q$ elements (where $q$ is a prime power). Let $M_{k\times n}(\mathbb{F}_q)$ be the set of $k \times n$ matrices over $\mathbb{F}_q$; when $k = n$ we also write $M_n(\mathbb{F}_q)$. We denote by $M^{\mathrm{full}}_{k\times n}(\mathbb{F}_q)$ the set of *full row-rank* matrices in $M_{k\times n}(\mathbb{F}_q)$, and by $GL_n(\mathbb{F}_q)$ the group of invertible $n \times n$ matrices. The $n \times n$ identity matrix is denoted by $I_n$.

Fix integers $n \geq r \geq 1$. The following well-known formulas will be used repeatedly:

$$\big|M_{r\times n}(\mathbb{F}_q)\big| \;=\; q^{rn}, \qquad \big|M^{\mathrm{full}}_{r\times n}(\mathbb{F}_q)\big| \;=\; \prod_{i=0}^{r-1}\big(q^n - q^i\big) \;=\; q^{rn}\prod_{i=0}^{r-1}\Big(1 - q^{i-n}\Big). \tag{1}$$

In particular, $\left|GL_n(\mathbb{F}_q)\right| = \prod_{i=0}^{n-1}(q^n - q^i)$.

The subgroup $B_n(\mathbb{F}_q) \subseteq GL_n(\mathbb{F}_q)$ consisting of all invertible upper triangular matrices is called the *(standard) Borel subgroup* of $GL_n(\mathbb{F}_q)$. Suppose that $n = m\ell$ with $m, \ell \in \mathbb{Z}_{>0}$. When the base field $\mathbb{F}_q$ is clear, let

$$B_\ell := B_\ell(\mathbb{F}_q) = \{\, U \in GL_\ell(\mathbb{F}_q) \;:\; U \text{ upper triangular} \,\}$$

and define

$$P_n \;:=\; B_\ell^m \;\subset\; GL_n(\mathbb{F}_q)$$

via the block-diagonal embedding $(U_1, \ldots, U_m) \mapsto \mathrm{diag}(U_1, \ldots, U_m)$. Let $\mathcal{S}_m$ be the symmetric group on $\{1, \ldots, m\}$, embedded in $GL_n(\mathbb{F}_q)$ by

$$\sigma \;\longmapsto\; \sigma \otimes I_\ell,$$

so that $\sigma$ acts on $\mathbb{F}_q^{m\ell} \cong (\mathbb{F}_q^\ell)^m$ by permuting the $m$ contiguous blocks of length $\ell$. This action normalizes $P_n$, hence we obtain the semidirect product

$$G_n \;:=\; P_n \rtimes \mathcal{S}_m \;\subset\; GL_n(\mathbb{F}_q). \tag{2}$$

The group $G_n$ is the natural right-isometry group for the block-NRT metric and will play a central role in our constructions and invariants.

### 2.1 Bruhat-Chevalley-Renner Decomposition.

The doubled Borel subgroup $B_n(\mathbb{F}_q) \times B_n(\mathbb{F}_q)$ acts on $M_n(\mathbb{F}_q)$ by the natural two-sided action

$$(x, y) \cdot z = xzy^{-1}, \quad x, y \in B_n(\mathbb{F}_q),\; z \in M_n(\mathbb{F}_q).$$

The *Bruhat-Chevalley-Renner decomposition* of $M_n(\mathbb{F}_q)$ describes the orbit representatives for this action:

$$M_n(\mathbb{F}_q) = \bigsqcup_{\sigma \in \mathcal{R}_n} B_n(\mathbb{F}_q)\, \sigma\, B_n(\mathbb{F}_q), \tag{3}$$

where $\mathcal{R}_n$ is the set of all $n \times n$ binary matrices having at most one 1 in each row and each column. We call $\mathcal{R}_n$ the *Renner monoid* of $M_n(\mathbb{F}_q)$, and its elements *rook matrices* since they correspond to non-attacking rook placements on an $n \times n$ chessboard. Note that, if instead of $M_n(\mathbb{F}_q)$, its unit group $GL_n(\mathbb{F}_q)$ is decomposed as in (3), then the disjoint union is defined over the symmetric group, $\mathcal{S}_n$:

$$GL_n(\mathbb{F}_q) = \bigsqcup_{\sigma \in \mathcal{S}_n} B_n(\mathbb{F}_q)\, \sigma\, B_n(\mathbb{F}_q). \tag{4}$$

This decomposition is classically known as the Bruhat-Chevalley decomposition.

The BCR decomposition was first developed by Renner [37] in the setting of algebraic monoids over algebraically closed fields, and by Solomon [40] for matrix monoids over finite fields. General background on linear algebraic monoids can be found in [38, 36].

We denote by $\mathcal{R}_{k\times n}$ the set of all $k \times n$ binary matrices with at most one 1 in each row and each column.

**Proposition 2.1.** *Let $k \in \{1, \dots, n\}$. Every matrix $z \in M_{k\times n}(\mathbb{F}_q)$ admits a unique decomposition*

$$z = u'\sigma y',$$

*where $u' \in B_k(\mathbb{F}_q)$ is unipotent, $y' \in B_n(\mathbb{F}_q)$, and $\sigma \in \mathcal{R}_{k\times n}$ is a rook matrix.*

*Proof.* This follows immediately from BCR decomposition by embedding $z$ into an $n \times n$ matrix with zero rows below the $k$-th row. □

**Definition 2.2** (Rectangular BCR decomposition)**.** The factorization $z = u'\sigma y'$ from Proposition 2.1 will be called the *rectangular BCR decomposition* of $z$. Here $u' \in B_k(\mathbb{F}_q)$ is unipotent, $\sigma \in \mathcal{R}_{k\times n}$ is a rook matrix, and $y' \in B_n(\mathbb{F}_q)$.

## 2.2 Code-Based Cryptosystems

For background on coding theory, see the classical texts [20, 16, 25]. A *linear $[n, k]$ code over $\mathbb{F}_q$* is a $k$-dimensional subspace $C \subseteq \mathbb{F}_q^n$. Such a code admits a *generator matrix* $G \in M_{k\times n}(\mathbb{F}_q)$ of full rank $k$, and a *parity-check matrix* $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ of full rank $n - k$, with the relation

$$C = \{y \in \mathbb{F}_q^n : yH^\top = 0\}, \qquad GH^\top = 0.$$

For a vector $v \in \mathbb{F}_q^n$, the *Hamming weight* $w_{\mathrm{H}}(v)$ is the number of nonzero coordinates.

Suppose $c \in C$ is transmitted through a noisy channel and an error $e \in \mathbb{F}_q^n$ occurs, so the receiver obtains $r = c + e$. The *syndrome* of $r$ is

$$s = rH^\top = eH^\top \in \mathbb{F}_q^{n-k}.$$

If $s = 0$ then $r \in C$ and no error is detected; otherwise, syndrome decoding seeks the lowest-weight vector $e$ consistent with $s$, so that $r - e \in C$. This motivates the following computational problem.

**Definition 2.3** (Syndrome Decoding Problem)**.** Given $H \in M_{(n-k)\times n}(\mathbb{F}_q)$, a syndrome $s \in \mathbb{F}_q^{n-k}$, and an integer $t \geq 0$, find $e \in \mathbb{F}_q^n$ with $w_{\mathrm{H}}(e) \leq t$ such that $He^\top = s$.

The Syndrome Decoding Problem is NP-complete in the worst case [3]. In code-based cryptography, the public key is a matrix $H_{\mathrm{pub}}$ designed to be computationally indistinguishable from a random parity-check matrix, while the secret key contains additional structure that enables efficient decoding of error vectors of weight up to $t$.

We are now ready to discuss code based cryptosystems.

In the original McEliece cryptosystem [26], the private key is a linear code $C$ of length $n$, dimension $k$, and designed distance $2t+1$, together with an efficient decoding algorithm. Typically, $C$ is chosen to be a binary Goppa code.

- **Private key:** A generator matrix $G \in M_{k\times n}(\mathbb{F}_q)$ of $C$, together with efficient decoding for $t$ errors.
- **Public key:** $G_{\mathrm{pub}} = SGP$, where $S \in GL_k(\mathbb{F}_q)$ is an invertible scrambling matrix and $P \in \mathcal{S}_n$ is a permutation matrix.

- **Encryption:** To encrypt a message $m \in \mathbb{F}_q^k$, choose a random error vector $e \in \mathbb{F}_q^n$ with $w_{\mathrm{H}}(e) \leq t$, and compute
$$c = mG_{\mathrm{pub}} + e \in \mathbb{F}_q^n.$$
- **Decryption:** Compute $cP^{-1} = mSG + eP^{-1}$. Since $eP^{-1}$ has weight $\leq t$, the private decoder for $C$ recovers $mS$, and multiplying by $S^{-1}$ yields $m$.

### 2.3 The Niederreiter Cryptosystem

In Niederreiter's dual formulation [28], the cyphertext is a syndrome rather than a corrupted codeword. This cryptosystem is particularly convenient for our BCR-based variant.

- **Private key:** A parity-check matrix $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ of a code $C$ with efficient $t$-error decoding.
- **Public key:** $H_{\mathrm{pub}} = SHP$, where $S \in GL_{n-k}(\mathbb{F}_q)$ is invertible and $P \in \mathcal{S}_n$ is a permutation.
- **Encryption:** To encrypt a message $m$, deterministically encode it as an error vector $e \in \mathbb{F}_q^n$ with $w_{\mathrm{H}}(e) \leq t$ via a fixed injective mapping. The ciphertext is the syndrome
$$c = H_{\mathrm{pub}} e^\top \in \mathbb{F}_q^{n-k}.$$
- **Decryption:** Compute $c' = S^{-1}c = H(Pe)^\top$. Apply the private decoder of $C$ to recover $Pe$, then apply $P^{-1}$ to recover $e$, from which $m$ is reconstructed.

| | **McEliece (1978)** | **Niederreiter (1986)** |
|---|---|---|
| **Private key** | Generator matrix $G \in M_{k\times n}(\mathbb{F}_q)$ of a code $C$ with efficient $t$-error decoding | Parity-check matrix $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ of a code $C$ with efficient $t$-error decoding |
| **Public key** | $G_{\mathrm{pub}} = SGP$ with $S \in GL_k(\mathbb{F}_q)$ and $P \in \mathcal{S}_n$ | $H_{\mathrm{pub}} = SHP$ with $S \in GL_{n-k}(\mathbb{F}_q)$ and $P \in \mathcal{S}_n$ |
| **Encryption** | Message $m \in \mathbb{F}_q^k$: pick random error $e \in \mathbb{F}_q^n$ with $w_{\mathrm{H}}(e) \leq t$; ciphertext $c = mG_{\mathrm{pub}} + e$ | Message $m$: deterministically encode as error $e \in \mathbb{F}_q^n$ with $w_{\mathrm{H}}(e) \leq t$; ciphertext $c = H_{\mathrm{pub}} e^\top$ |
| **Decryption** | Compute $cP^{-1} = mSG + eP^{-1}$, decode using $C$ to recover $mS$, then multiply by $S^{-1}$ | Compute $c' = S^{-1}c = H(Pe)^\top$, decode using $C$ to recover $Pe$, then apply $P^{-1}$ to get $e$ and hence $m$ |
| **Ciphertext form** | Corrupted codeword $c \in \mathbb{F}_q^n$ | Syndrome $c \in \mathbb{F}_q^{n-k}$ |

Table 1: Comparison of the McEliece and Niederreiter cryptosystems. Both rely on the hardness of the syndrome decoding problem, but differ in whether ciphertexts are corrupted codewords (McEliece) or syndromes (Niederreiter).

**Remark 2.4.** The matrices $S$ and $P$ serve to *obfuscate* the structure of the private code. Without them, the public key would reveal the special algebraic structure of $C$ (for example, a Goppa code), leading to structural attacks. If $S$ and $P$ were chosen from the *isometry group* of $C$ (the group of linear transformations that map $C$ to an equivalent code), then the obfuscation would be ineffective: the public key would still betray equivalence to a known structured family. This observation motivates the scrambler design in our rook-based construction.

### 2.4 Poset Metrics

The theory of poset metrics on error-correcting codes was formalized in [5]. In this subsection, we provide definitions for completeness. For more information, we refer readers to the monograph [12].

Let $[n] = \{1, 2, \ldots, n\}$ be a finite set, and let $P$ be a partially ordered set (poset) structure on $[n]$. A *poset code* is a linear code $C \subseteq \mathbb{F}_q^n$ equipped with the *poset metric* induced by $P$. For a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, define the *support* of $x$ as

$$\operatorname{supp}(x) = \{i \in [n] : x_i \neq 0\}.$$

Given $A \subseteq [n]$, let $\langle A \rangle_P$ denote the *ideal generated by $A$ in $P$*, that is,

$$\langle A \rangle_P = \{j \in [n] : j \leq_P i \text{ for some } i \in A\}.$$

The *poset weight* of $x$ is then defined as

$$w_P(x) = |\langle \operatorname{supp}(x) \rangle_P|.$$

Finally, the *poset distance* between $x, y \in \mathbb{F}_q^n$ is

$$d_P(x, y) = w_P(x - y).$$

This generalizes several well-known metrics. For example, when $P$ is the antichain, the poset weight coincides with the Hamming weight.

## 3 NRT Metric (Single Chain)

An important poset metric is given by when the poset $P$ is a single chain:

$$1 < 2 < 3 < \cdots < n.$$

In this case, the induced poset metric is known as the *Niederreiter-Rosenbloom-Tsfasman (NRT) metric (defined by a chain)*. Given $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, its NRT weight is

$$w_{\mathrm{NRT}}(x) = \begin{cases} 0, & \text{if } x = 0, \\ \max\{i \in [n] : x_i \neq 0\}, & \text{otherwise.} \end{cases}$$

Equivalently, the NRT weight records the highest-indexed nonzero coordinate of $x$. Thus, the NRT distance between $x, y \in \mathbb{F}_q^n$ is given by

$$d_{\mathrm{NRT}}(x, y) = w_{\mathrm{NRT}}(x - y).$$

The NRT metric captures error patterns that are naturally *burst-like*: an error in position $i$ implies that all subsequent positions $j \leq i$ contribute to the weight. This makes the metric particularly relevant in settings where errors tend to propagate through consecutive coordinates, such as in certain communication channels or storage systems.

The NRT metric is, like the Hamming metric, translation-invariant. However, the structure of its linear isometry group is different: instead of all monomial matrices, the isometry group is given by the Borel subgroup of $GL_n(\mathbb{F}_q)$. This algebraic group connection makes NRT codes relevant to our discussion. We provide a proof of this fact for completeness.

**Proposition 3.1.** *The full linear isometry group of $(\mathbb{F}_q^n, d_{\mathrm{NRT}})$ is precisely $B_n(\mathbb{F}_q)$.*

*Proof.* We begin with proving that if $U \in B_n(\mathbb{F}_q)$ is invertible upper triangular, then $w_{\mathrm{NRT}}(Ux) = w_{\mathrm{NRT}}(x)$ for all $x \in \mathbb{F}_q^n$. Hence $d_{\mathrm{NRT}}(Ux, Uy) = d_{\mathrm{NRT}}(x, y)$ for all $x, y$.

Let $j^\star := w_{\mathrm{NRT}}(x)$, so $x_{j^\star} \neq 0$ and $x_i = 0$ for all $i > j^\star$. For any $i > j^\star$ we have

$$(Ux)_i = \sum_{j=1}^{n} U_{ij} x_j = \sum_{j \leq i} U_{ij} x_j.$$

But $x_j = 0$ for all $j > j^\star$, and $U_{ij} = 0$ whenever $i > j$ (upper triangular), so every term vanishes and $(Ux)_i = 0$. Thus $w_{\mathrm{NRT}}(Ux) \leq j^\star$.

At $i = j^\star$ we get

$$(Ux)_{j^\star} = \sum_{j \leq j^\star} U_{j^\star j}\, x_j = U_{j^\star j^\star} x_{j^\star},$$

since $U_{j^\star j} = 0$ for $j < j^\star$ in an upper triangular matrix. Because $U_{j^\star j^\star} \neq 0$ and $x_{j^\star} \neq 0$, we have $(Ux)_{j^\star} \neq 0$, so $w_{\mathrm{NRT}}(Ux) \geq j^\star$. Therefore $w_{\mathrm{NRT}}(Ux) = j^\star = w_{\mathrm{NRT}}(x)$. Hence, our claim follows.

Next, we will prove that if $T \in GL_n(\mathbb{F}_q)$ satisfies $w_{\mathrm{NRT}}(Tx) = w_{\mathrm{NRT}}(x)$ for all $x \in \mathbb{F}_q^n$, then $T$ is upper triangular with nonzero diagonal entries, $T \in B_n(\mathbb{F}_q)$. For this purpose, we apply the isometry to the basis vectors $e_i$. Since $w_{\mathrm{NRT}}(e_i) = i$, we must have $w_{\mathrm{NRT}}(Te_i) = i$ for each $i$. Thus the $i$-th column of $T$ (which equals $Te_i$) has all entries zero in rows $> i$ (otherwise the weight would exceed $i$), and has a nonzero entry in row $i$ (otherwise the weight would be $< i$). Hence every column $i$ has zeros below the diagonal and a nonzero diagonal entry $T_{ii} \neq 0$, which is exactly the condition that $T$ be invertible upper triangular. This finishes the proof of our claim as well as the proof of proposition. □

### 3.1 Minimum NRT distance from a parity-check matrix

Let $C \subseteq \mathbb{F}_q^n$ be a linear $[n, k]_q$ code with parity-check matrix $H \in M_{r \times n}(\mathbb{F}_q)$, $r = n - k$. For $t \in \{0, 1, \ldots, n\}$, we denote by $H_{[t]}$ the (sub)matrix formed by the first $t$ columns of $H$ with the convention that $H_{[0]}$ is the zero column vector of size $r$.

**Proposition 3.2** (Prefix rank criterion)**.** *The minimum NRT distance of $C$ is*

$$d_{\mathrm{NRT}}(C) \;=\; \min\big\{\, t \geq 1 :\; \mathrm{rank}(H_{[t]}) < t \,\big\} \;=\; 1 + \max\big\{\, t \geq 0 :\; \mathrm{rank}(H_{[t]}) = t \,\big\}.$$

*Equivalently, $d_{\mathrm{NRT}}(C) > t$ iff the columns $1, \ldots, t$ of $H$ are linearly independent.*

*Proof.* A codeword $x \in C$ has $w_{\mathrm{NRT}}(x) \leq t$ if and only if $x_{t+1} = \cdots = x_n = 0$ (hence, $x = (x_1, \ldots, x_t, 0, \ldots, 0) \neq 0$). The parity-check condition $Hx^\top = 0$ becomes $H_{[t]}\,(x_1, \ldots, x_t)^\top = 0$. Thus there exists a nonzero codeword of NRT weight $\leq t$ if and only if $H_{[t]}$ has a nontrivial kernel. Equivalently, $d_{\mathrm{NRT}}(C) \leq t$ if and only if $\mathrm{rank}(H_{[t]}) < t$. Taking the least such $t$ gives the first equation. The proof of the second equation is straightforward to see. □

The analog of the Singleton's bound for poset metrics is proven in [17]. In particular, on an $[n, k]_q$ code, the NRT metric satisfies

$$d_{\mathrm{NRT}}(C) \leq n - k + 1.$$

If the equality holds, then $C$ is called an *MDS NRT code*. As a consequence of our previous result, we obtain a slight improvement of this result in terms of parity-check matrices.

**Corollary 3.3.** *If $r$ denotes $n - k$, then we always $d_{\mathrm{NRT}}(C) \leq r + 1$. Moreover*

$$C \text{ is MDS NRT} \quad \Longleftrightarrow \quad \mathrm{rank}(H_{[r]}) = r \quad (\text{the first } r \text{ columns of } H \text{ are independent}).$$

*In other words,*

$$d_{\mathrm{NRT}}(C) = r + 1 \quad \Longleftrightarrow \quad \text{the leading } r \times r \text{ submatrix of } H \text{ has full rank.}$$

In light of our prefix rank criterion (Proposition 3.2), we have a simple algorithmic procedure for determining the minimum weight of the NRT metric from a parity-check matrix $H$:

- Incrementally build the rank of $H_{[t]}$ for $t = 1, 2, \ldots$.
- Let $r_0 := 0$, and for each $t$ set $r_t := \mathrm{rank}(H_{[t]})$.

Then the smallest $t$ with $r_t < t$ is $d_{\mathrm{NRT}}(C)$. Since $r_t \leq r$, this $t$ occurs by $t \leq r + 1$.

Going back to Proposition 3.1, right-multiplication by any $T \in B_n$ (invertible upper triangular) preserves $\mathrm{rank}(H_{[t]})$ for every prefix $t$, since $(HT)_{[t]} = H_{[t]}\,T_{[t]}$ and $T_{[t]} \in B_t$ is invertible. Hence $d_{\mathrm{NRT}}(C)$ is well-defined on the $B_n$-orbit of $H$, as expected for an NRT metric invariant.

### 3.2 The big $B_r(\mathbb{F}_q) \times B_n(\mathbb{F}_q)$ cell in $M^{\mathrm{full}}_{r\times n}(\mathbb{F}_q)$ and MDS NRT codes

Let $q$ be a prime power, fix integers $n > k \geq 1$, and put $r := n - k$. We already mentioned that the rook monoid $\mathcal{R}_n$ indexes the Bruhat-Chevalley-Renner decomposition of $M_n(\mathbb{F}_q)$. If $x \in \mathcal{R}_n$ has one-line notation $x = (a_1, \ldots, a_n)$ (with $a_j \in \{0, 1, \ldots, n\}$ the row index in column $j$, or 0 if that column is zero), then the orbit dimension $\dim(B_n(\mathbb{F}_q)xB_n(\mathbb{F}_q))$ admits the combinatorial formula

$$\dim(B_n(\mathbb{F}_q)xB_n(\mathbb{F}_q)) = \sum_{i=1}^{n} a_i^* - \mathrm{coinv}(x), \qquad a_i^* = \begin{cases} a_i + n - i, & a_i \neq 0, \\ 0, & a_i = 0, \end{cases}$$

where $\mathrm{coinv}(x)$ counts pairs $1 \leq i < j \leq n$ with $0 < a_i < a_j$. This gives a graded poset structure by orbit dimensions and identifies the *big cell* as the orbit of maximal dimension. For this development, see [7, Theorem 1.7].

**Proposition 3.4.** *Let $R_0 \in \mathcal{R}_{r,n}$ be the rectangular rook whose 1's lie at $(r,1),(r-1,2),\ldots,(1,r)$ (these are the pivot columns $\{1,2,\ldots,r\}$). Then the subset*

$$\mathcal{U} \;:=\; \{\, H \in M_{r,n}^{\mathrm{full}}(\mathbb{F}_q) :\; \det(H_{[r]\times[r]}) \neq 0 \,\}$$

*is Zariski open and dense in $M_{r,n}^{\mathrm{full}}(\mathbb{F}_q)$ and equals a single double coset:*

$$\mathcal{U} \;=\; B_r(\mathbb{F}_q)\, R_0\, B_n(\mathbb{F}_q).$$

*Proof.* Openness and density are immediate since $\det(H_{[r]\times[r]})$ is a nonzero polynomial. If $H \in \mathcal{U}$, Gaussian elimination using only upper-triangular column operations and upper-triangular row operations produces $L \in B_r$, $U \in B_n$ with $LHU = R_0$, hence $H \in B_r R_0 B_n$. Conversely, if $H = L^{-1}R_0U^{-1}$ then the leading $r\times r$ block equals $L^{-1}$(unit upper-triangular), hence invertible. □

**Corollary 3.5.** *If $H \in B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q)$, then $\mathrm{rank}(H_{[t]}) = t$ for all $1 \le t \le r$, and hence $d_{\mathrm{NRT}}(C) = r+1$ by Corollary 3.3.*

Every $[n,k]_q$ code can be viewed as a particular $\mathbb{F}_q$-rational point of the Grassmann variety of $k$-dimensional subspaces of $\mathbb{F}_q^n$.

**Lemma 3.6.** *If $H$ is sampled uniformly from $M_{r,n}^{\mathrm{full}}(\mathbb{F}_q)$ and $C = \ker(H)$, then the induced distribution on the Grassmannian of $k$-dimensional subspaces of $\mathbb{F}_q^n$ is uniform. Moreover, the event $\{\det(H_{[r]\times[r]}) \neq 0\}$ is invariant under left multiplication by $GL_r(\mathbb{F}_q)$, hence well-defined at the level of codes.*

*Proof.* Two full-rank matrices have the same row space iff they differ by left multiplication by a unique element of $GL_r(\mathbb{F}_q)$. The $GL_r(\mathbb{F}_q)$-action is free and all orbits have the same size. The leading-minor condition is preserved by left multiplication. □

**Theorem 3.7.** *Let $n > k \ge 1$ and $r = n-k$. If $C \subseteq \mathbb{F}_q^n$ is a uniformly random $[n,k]_q$ code, then*

$$\lim_{q\to\infty} \Pr\big[d_{\mathrm{NRT}}(C) = r+1\big] = \lim_{q\to\infty} \Pr[\textit{random } [n,k]_q \textit{ code is MDS NRT}] = 1$$

*Proof.* It follows from Singleton's bound for poset metrics [17] that $d_{\mathrm{NRT}}(C) = r+1$ if and only if $C$ is an MDS NRT code. Hence the first equality follows. For the second equality, we sample a random parity check $H \in M_{r,n}^{\mathrm{full}}(\mathbb{F}_q)$. By Lemma 3.6 this induces a uniform random code. By Proposition 3.4, the event $E = \{\det(H_{[r]\times[r]}) \neq 0\}$ is exactly the big double coset $B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q)$ in rectangular form, the analogue of the "big cell" among Borel subgroup orbits (compare with the $n\times n$ case in [7]). When $E$ holds, Corollary 3.5 gives $d_{\mathrm{NRT}}(C) = r+1$. In particular, we have

$$\Pr[d_{\mathrm{NRT}}(C) = r+1] \;=\; \Pr[H \in B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q)]$$

We deduce from [6, Eqn. (1.2)] that

$$\big|B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q)\big| = q^{\dim(B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q))-\mathrm{rank}(R_0)}(q-1)^{\mathrm{rank}(R_0)} = q^{rn-r}(q-1)^r. \tag{5}$$

It follows that

$$\begin{aligned}\Pr[H \in B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q)] &= \frac{\left|B_r(\mathbb{F}_q)R_0B_n(\mathbb{F}_q)\right|}{\left|M^{\text{full}}_{r\times n}(\mathbb{F}_q)\right|} \\ &= \frac{q^{rn-r}(q-1)^r}{q^{rn}\prod_{i=0}^{r-1}\left(1-q^{\,i-n}\right)} \qquad \text{(by Eqn. (1) and (5))} \\ &= \frac{\left(1-q^{-1}\right)^r}{\prod_{i=0}^{r-1}\left(1-q^{\,i-n}\right)} \\ &\geq \left(1-q^{-1}\right)^r.\end{aligned}$$

Hence, if $q$ is sent to $\infty$, the proof of our theorem follows. □

# 4 The Minimum Distance of a Block-NRT Code

Fix integers $m \geq 1$ (representing the number of blocks) and $\ell \geq 1$ (representing the block length) and set $n = m\ell$. Index coordinates as $(b, j)$ with $b \in \{1, \ldots, m\}$ (block) and $j \in \{1, \ldots, \ell\}$ (position in the block). We equip $\mathbb{F}_q^n$ with the *block-NRT* poset metric given by the direct sum of $m$ chains

$$(1,1) < (1,2) < \cdots < (1,\ell), \quad \ldots, \quad (m,1) < \cdots < (m,\ell),$$

and no relations across blocks. For $x \in \mathbb{F}_q^n$ write $x^{(b)} \in \mathbb{F}_q^\ell$ for the $b$th block. We define the *block-NRT weight of* $x$ by setting

$$w_{\text{bNRT}}(x) \;=\; \sum_{b=1}^{m} w_{\text{NRT}}\big(x^{(b)}\big), \quad \text{where} \quad w_{\text{NRT}}(y) = \begin{cases} 0, & y = 0, \\ \max\{j :\; y_j \neq 0\}, & y \neq 0. \end{cases}$$

Then $d_{\text{bNRT}}(x, y) = w_{\text{bNRT}}(x - y)$.

The full linear isometry group of $(\mathbb{F}_q^n, d_{\text{bNRT}})$ is known (see [33]) to coincide with the semidirect product $G_n \;:=\; (B_\ell(\mathbb{F}_q))^m \rtimes \mathcal{S}_m$ introduced in (2). To explain. we let $n = m\ell$ and write vectors in $\mathbb{F}_q^n$ as $m$ consecutive *column blocks* of length $\ell$. The group $G_n$ acts on matrices on the right by (i) an invertible upper-triangular $B_\ell(\mathbb{F}_q)$ within each block (preserves single-chain NRT weight inside a block), and (ii) a permutation of the $m$ blocks by $\mathcal{S}_m$. In particular, general linear group $GL_n(\mathbb{F}_q)$ on the right does not preserve the block-NRT metric.

The block-NRT weight of $X \in M_{\ell\times m}(\mathbb{F}_q)$ is the sum of the single-chain NRT weights of its columns. By Proposition 3.1, the linear isometries of the single-chain NRT metric on each length-$\ell$ column are precisely left multiplications by $B_\ell$. Allowing independent $B_\ell$ actions on each column (giving $B_\ell^m$) and arbitrary permutations of the $m$ columns (realized by $\sigma \otimes I_\ell$) yields $P_n \rtimes \mathcal{S}_m$, which clearly preserves $d_{\text{bNRT}}$. Conversely, any linear isometry must act by such column-wise upper-triangular transformations and block permutations, hence lies in $G_n$.

## 4.1 Multi-prefix rank criterion (block analogue of NRT prefix test)

Recall from Proposition 3.2 that, for the single block case, the minimum distance for the NRT metric can be determined from the initial minors of a parity check matrix. Here, we discuss a generalization of this result.

Let $H \in M_{r\times n}(\mathbb{F}_q)$ be full row rank ($r = n-k$) and partition its columns into blocks

$$H = \big[\, H^{(1)} \mid H^{(2)} \mid \cdots \mid H^{(m)} \,\big]$$

with $H^{(b)} \in M_{r\times \ell}(\mathbb{F}_q)$. For a *multi-prefix* $u = (u_1, \ldots, u_m) \in \{0, 1, \ldots, \ell\}^m$ define

$$H_{[u]} \;:=\; \big[\, H^{(1)}_{[u_1]} \mid \cdots \mid H^{(m)}_{[u_m]} \,\big], \quad \text{and} \quad |u|_1 := \sum_{b=1}^{m} u_b.$$

**Proposition 4.1.** *Let $n = m\ell$ and partition the $n$ columns of $H \in M_{r\times n}(\mathbb{F}_q)$ into $m$ consecutive blocks of length $\ell$:*

$$H = \big[\, H^{(1)} \mid H^{(2)} \mid \cdots \mid H^{(m)} \,\big], \qquad H^{(b)} \in M_{r\times \ell}(\mathbb{F}_q).$$

*For $u = (u_1, \ldots, u_m) \in \{0, 1, \ldots, \ell\}^m$ define the block-prefix submatrix*

$$H_{[u]} \;:=\; \big[\, H^{(1)}_{[u_1]} \mid \cdots \mid H^{(m)}_{[u_m]} \,\big] \in M_{r\times |u|_1}(\mathbb{F}_q) \qquad |u|_1 := \sum_{b=1}^{m} u_b,$$

*where $H^{(b)}_{[t]}$ denotes the first $t$ columns of block $b$. If $C = \ker(H) \subseteq \mathbb{F}_q^n$, then we have*

$$d_{\mathrm{bNRT}}(C) = \min\{\, |u|_1 \geq 1 :\ \mathrm{rank}(H_{[u]}) < |u|_1 \,\} = 1 + \max\{\, |u|_1 \geq 0 :\ \mathrm{rank}(H_{[u]}) = |u|_1 \,\}.$$

*Moreover, for every $T \in G_n$ and every $u$, there exists a blockwise permutation $u'$ such that*

$$u' = \pi^{-1}\cdot u \quad \textit{and} \quad (HT)_{[u]} \;=\; H_{[u']}\, \widetilde{T}_{[u']},$$

*where $\widetilde{T}_{[u']} \in \prod_{b=1}^{m} B_{u'_b}(\mathbb{F}_q)$. In particular, the criterion (and hence $d_{\mathrm{bNRT}}(C)$) is invariant under right multiplication by $G_n$.*

*Proof. Step 1.* For $u \in \{0, \ldots, \ell\}^m$, define the linear subspace

$$S[u] \;:=\; \big\{ x \in \mathbb{F}_q^n :\ \text{in block } b,\ x^{(b)}_j = 0 \text{ for all } j > u_b \big\}.$$

Then $\dim S[u] = |u|_1$. There is a natural linear isomorphism

$$\phi_u :\ \mathbb{F}_q^{|u|_1} \;\xrightarrow{\;\cong\;}\; S[u]$$

that packs a tuple $(x^{(1)}_{[u_1]}, \ldots, x^{(m)}_{[u_m]})$ into $x \in S[u]$ by placing those entries in the first $u_b$ coordinates of block $b$ and zeros elsewhere.

*Step 2.* By construction,

$$H\, \phi_u(v) \;=\; H_{[u]}\, v \qquad \text{for all } v \in \mathbb{F}_q^{|u|_1}.$$

Hence

$$\ker\big(H_{[u]}\big) \;\cong\; \ker(H) \cap S[u] \qquad \text{and} \qquad \ker(H) \cap S[u] \neq \{0\} \iff \mathrm{rank}(H_{[u]}) < |u|_1. \qquad (*)$$

*Step 3.* A nonzero vector $x \in \mathbb{F}_q^n$ has $w_{\mathrm{bNRT}}(x) \le t$ iff there exists $u$ with $|u|_1 \le t$ such that $x \in S[u]$ (namely, take $u_b := w_{\mathrm{NRT}}(x^{(b)})$ for each block). Therefore

$$\begin{aligned} d_{\mathrm{bNRT}}(C) &= \min\{\, w_{\mathrm{bNRT}}(x) : x \in C \setminus \{0\} \,\} \\ &= \min\{\, |u|_1 :\ (\ker(H) \cap S[u]) \setminus \{0\} \neq \emptyset \,\} \\ &= \min\{\, |u|_1 :\ \mathrm{rank}(H_{[u]}) < |u|_1 \,\}, \end{aligned}$$

where the last equality uses $(*)$.

*Step 4.* For fixed $H$, the map $u \mapsto \mathrm{rank}(H_{[u]})$ is monotone with respect to the componentwise order (if $u \le v$ then $H_{[u]}$ is a column submatrix of $H_{[v]}$). It also satisfies $\mathrm{rank}(H_{[u]}) \le |u|_1$. Let

$$t^\star \ :=\ \max\{\, |u|_1 :\ \mathrm{rank}(H_{[u]}) = |u|_1 \,\}.$$

By monotonicity, for every $t \le t^\star$ there exists some $u$ with $|u|_1 = t$ and $\mathrm{rank}(H_{[u]}) = t$, whereas for $t = t^\star + 1$ we must have $\mathrm{rank}(H_{[u]}) < |u|_1$ for every $u$ with $|u|_1 = t$. Thus the previous minimum equals $t^\star + 1$, yielding the second displayed equality.

*Step 5.* Every $T \in G_n$ can be written as $T = \Pi \cdot \mathrm{diag}\big(T^{(1)}, \dots, T^{(m)}\big)$ with $\Pi \in S_m$ a block permutation and each $T^{(b)} \in B_\ell$ upper triangular (invertible). Fix $u \in \{0, \dots, \ell\}^m$ and let $u' := \pi^{-1} \cdot u$, so that $u'_b = u_{\pi(b)}$. Then

$$(HT)_{[u]} = \big[\, H^{(\pi^{-1}(1))}(T^{(\pi^{-1}(1))})_{[u'_1]} \;\big|\; \cdots \;\big|\; H^{(\pi^{-1}(m))}(T^{(\pi^{-1}(m))})_{[u'_m]} \,\big] = H_{[u']}\, \widetilde{T}_{[u']},$$

where $\widetilde{T}_{[u']} := \mathrm{diag}\big((T^{(\pi^{-1}(1))})_{[u'_1]}, \dots, (T^{(\pi^{-1}(m))})_{[u'_m]}\big)$ and $(T^{(b)})_{[t]}$ denotes the top-left $t \times t$ block of $T^{(b)}$, which lies in $B_t$ and is invertible because $T^{(b)} \in B_\ell$ is upper triangular with nonzero diagonal. Therefore $\mathrm{rank}\big((HT)_{[u]}\big) = \mathrm{rank}\big(H_{[u']}\big)$, and

$$\exists\, u \text{ with } \mathrm{rank}\big((HT)_{[u]}\big) < |u|_1 \iff \exists\, u' \text{ with } \mathrm{rank}\big(H_{[u']}\big) < |u'|_1,$$

since $|u|_1 = |u'|_1$. The displayed distance formulas are thus invariant under $H \mapsto HT$. This finishes the proof of our result. □

**Remark 4.2.** With the block-NRT codes, the single-chain public shortcut disappears. An adversary given $s = Me^\top$ and $t$ no longer knows *which* multi-prefix $u$ (with $|u|_1 \le t$) bounds the support. Indeed, there are

$$N(m,t) \ =\ \#\{u \in \{0, \dots, \ell\}^m :\ |u|_1 \le t\} \ =\ \sum_{j=0}^{t} \binom{m+j-1}{j}$$

candidates (when $\ell \ge t$ this is $\binom{m+t}{t}$) for the support. If $t = \alpha n$ and $m = \Theta(n)$ hold, the number $N(m,t)$ is exponential in $n$, so the "one-prefix linear solve" attack is no longer polynomial.

## 4.2 Right-isometry Group Orbits

The goal of this subsection is to identify appropriate rook matrices for the orbits of the right-isometry groups for the block-NRT metric.

Let $n = m\ell$ and partition the $n$ columns into $m$ consecutive blocks of length $\ell$. The full linear isometry group $G_n$ acts on the parity-check matrices on the right. On the left, we have the left multiplication action of $GL_r(\mathbb{F}_q)$ that corresponds to row operations.

**Definition 4.3.** A *block-rook pattern* is a family of subsets

$$T := (T_1, \dots, T_m), \qquad T_b \subseteq [\ell],$$

with total size $\sum_{b=1}^{m} |T_b| = r$.

Given a block-rook pattern $T = (T_1, \dots, T_m)$ with $\sum_b |T_b| = r$, we build a full rank rectangular rook matrix $R_T \in M_{r\times n}(\mathbb{F}_q)$ as follows:

1. Form the ordered list of pivot columns by listing all pairs

   $$\mathsf{Piv} := \{\, (b,t) \;:\; b \in [m],\ t \in T_b \,\}$$

   in lexicographic order: first by $b$ then by $t$. Denote this order by $(b_1, t_1), \dots, (b_r, t_r)$.

2. For $i = 1, \dots, r$, place a 1 in row $r - i + 1$ and absolute column $(b_i{-}1)\ell + t_i$:

   $$\big(R_T\big)_{\,r-i+1,\ (b_i-1)\ell+t_i} \;=\; 1.$$

   Set all other entries of $R_T$ to 0.

Any other choice that uses the same set of columns but permutes the rows of $R_T$ represents the *same* $GL_r(\mathbb{F}_q) \times G_n$ double coset (row permutations lie in $GL_r(\mathbb{F}_q)$), so the particular row order above is a convenient canonical representative.

**Example 4.4.** Let $m = 3$, $\ell = 4$ (so $n = 12$) and $r = 5$. Take

$$T_1 = \{1, 3\}, \qquad T_2 = \{2\}, \qquad T_3 = \{1, 4\}.$$

Lexicographic ordering gives

$$(b_1, t_1) = (1, 1),\ (b_2, t_2) = (1, 3),\ (b_3, t_3) = (2, 2),\ (b_4, t_4) = (3, 1),\ (b_5, t_5) = (3, 4).$$

Placing 1's at rows $5, 4, 3, 2, 1$ and absolute columns $(1{-}1)\ell + 1 = 1,\ (1{-}1)\ell + 3 = 3,\ (2{-}1)\ell + 2 = 6,\ (3{-}1)\ell + 1 = 9,\ (3{-}1)\ell + 4 = 12$ yields

$$R_T = \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

(Vertical bars indicate the three blocks of four columns each.)

**Proposition 4.5.** *Every full row rank $H \in M^{\mathrm{full}}_{r\times n}(\mathbb{F}_q)$ lies in a unique $GL_r(\mathbb{F}_q) \times G_n$ double coset*

$$H \;\in\; GL_r(\mathbb{F}_q)\, R_J\, G_n,$$

*indexed by its block-rook pattern $J$ (equivalently, by the right block-prefix rank profile).*

In a later section, we will discuss lower bounds for the minimum distances. We close this section by a remark about the minimum distance itself.

**Remark 4.6.** Write $H = [\,H^{(1)}|\cdots|H^{(m)}\,]$ in blocks. For a multi-prefix

$$u = (u_1, \ldots, u_m) \in \{0, \ldots, \ell\}^m,$$

let $H_{[u]} = [\,H^{(1)}_{[u_1]}|\cdots|H^{(m)}_{[u_m]}]$ and $|u|_1 = \sum_b u_b$. Then for any $H \in GL_r(\mathbb{F}_q)R_T G_n$, we have

$$\operatorname{rank}\big(H_{[u]}\big) = \sum_{b=1}^{m} \#\{\, t \in T_b :\ t \le u_b \,\}.$$

Consequently, we have

$$d_{\mathrm{bNRT}}(\ker H) = \min\Big\{|u|_1 \ge 1 :\ \sum_b \#(T_b \cap [u_b]) < |u|_1\Big\}.$$

# 5 Sum-Rank Metric Codes

In this model, we fix $m$ blocks and block lengths $\ell_1, \ldots, \ell_m$ with $n = \sum_{b=1}^m \ell_b$. For each block $b$, we fix a positive integer $h_b$ and view block $b$ as $M_{\ell_b \times h_b}(\mathbb{F}_q)$ via a fixed $\mathbb{F}_q$-basis of an $\mathbb{F}_{q^{h_b}}$-module.

**Definition 5.1** (Sum-rank weight)**.** Given $x = (x^{(1)}, \ldots, x^{(m)}) \in \mathbb{F}_q^n$ with blocks $X^{(b)} \in M_{\ell_b \times h_b}(\mathbb{F}_q)$, define the block rank $w_{\mathrm{rk}}(x^{(b)}) := \operatorname{rank}_{\mathbb{F}_q}(X^{(b)})$ and

$$w_{\mathrm{SR}}(x) \ :=\ \sum_{b=1}^{m} \operatorname{rank}_{\mathbb{F}_q}(X^{(b)}), \qquad d_{\mathrm{SR}}(x,y) \ :=\ w_{\mathrm{SR}}(x-y).$$

For block $b$, let $L_b := GL_{\ell_b}(\mathbb{F}_q)$ act on the left of $X^{(b)} \in M_{\ell_b \times h_b}(\mathbb{F}_q)$, and let $R_b := GL_{h_b}(\mathbb{F}_q)$ act on the right (change of $\mathbb{F}_q$-basis inside the $h_b$-dimensional column space). Both actions preserve $\operatorname{rank}(X^{(b)})$ and hence the sum-rank weight $w_{\mathrm{SR}}$. Permuting blocks that share the same size pair $(\ell_b, h_b)$ also preserves $w_{\mathrm{SR}}$. We deduce from these observations a convenient (and sufficient) isometry subgroup,

$$\mathcal{G}_{\mathrm{SR}} := \Big(\prod_{b=1}^{m} (L_b \times R_b)\Big) \rtimes \prod_{(\ell,h)} \mathcal{S}_{m_{\ell,h}},$$

where $\mathcal{S}_{m_{\ell,h}}$ permutes the blocks whose sizes equal $(\ell, h)$. In particular, the block Borel product subgroup $P_n$, embedded into $\mathcal{G}_{\mathrm{SR}}$ as

$$P_n \ :=\ \prod_{b=1}^{m} B_{\ell_b}(\mathbb{F}_q) \ \subseteq\ \prod_{b=1}^{m} L_b$$

(upper triangular matrices in each $GL_{\ell_b}(\mathbb{F}_q)$), acts by isometries. Hence, all NRT-style triangular masks remain valid in the sum-rank setting as the subgroup $P_n \le \mathcal{G}_{\mathrm{SR}}$.

We proceed to describe a rank-profile distance test from parity-check viewpoint. Let $H \in M_{r\times n}(\mathbb{F}_q)$, $r = n-k$, be full row rank, partitioned as $H = [\,H^{(1)} \mid \cdots \mid H^{(m)}\,]$ with $H^{(b)} \in M_{r\times \ell_b}(\mathbb{F}_q)$. For an $m$-tuple $u = (u_1, \ldots, u_m)$ with $0 \le u_b \le \min\{\ell_b, h_b\}$, define

$$\mathsf{rk}_H(u) \ :=\ \max\Big\{\operatorname{rank}\Big(\big[\,H^{(1)}U^{(1)} \,\big|\, \cdots \,\big|\, H^{(m)}U^{(m)}\,\big]\Big) \ \Big|\ U^{(b)} \in M_{\ell_b \times u_b}(\mathbb{F}_q) \text{ has full column rank}\Big\}.$$

Intuitively, $U^{(b)}$ selects an $u_b$-dimensional $\mathbb{F}_q$-subplot inside block $b$. The "best case" rank of the concatenation determines whether a nonzero codeword of sum-rank weight $\le \sum_b u_b$ can exist.

**Proposition 5.2** (Sum-rank distance via block rank-profiles)**.** *Let $C = \ker(H)$. Define*

$$t^\star \;:=\; \max\Big\{\, \textstyle\sum_b u_b \;:\; \mathsf{rk}_H(u) = \sum_b u_b \,\Big\}.$$

*Then*

$$d_{\mathrm{SR}}(C) \;=\; 1 + t^\star \qquad \text{and} \qquad d_{\mathrm{SR}}(C) > t \iff \mathsf{rk}_H(u) = \sum_b u_b \text{ for all } u \text{ with } \sum_b u_b \le t.$$

*Moreover, $d_{\mathrm{SR}}(C)$ is invariant under right multiplication of $H$ by any element of $\mathcal{G}_{\mathrm{SR}}$, and in particular under $P_n$.*

*Proof.* Let $\mathcal{S}[u]$ be the $\mathbb{F}_q$-subspace of vectors whose $b$-th block has rank $\le u_b$ (equivalently, whose reshape has column space contained in an $u_b$-dimensional subspace). Using block packings as in the NRT proof, one gets $\ker(H) \cap \mathcal{S}[u] \neq \{0\}$ iff $\mathsf{rk}_H(u) < \sum_b u_b$. Monotonicity in $u$ then yields the stated formula. Right actions from $\mathcal{G}_{\mathrm{SR}}$ preserve ranks inside each block and hence preserve $\mathsf{rk}_H(u)$. □

# 6 Lower Bounds

In this section we describe lower bounds for minimum distances of the block-NRT as well as sum-rank codes.

## 6.1 Block-NRT case.

We begin with finding a lower bound for $d_{\mathrm{bNRT}}(C)$ from the generator matrix for the block-NRT case.

**Proposition 6.1** (Computation of $d_{\mathrm{bNRT}}(C)$ from a generator matrix)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear block-NRT code with parameters $n = m\ell$, dimension $k$, and generator matrix*

$$G = \big[\, G^{(1)} \mid G^{(2)} \mid \cdots \mid G^{(m)} \,\big], \qquad \text{where} \qquad G^{(b)} = [\, g_1^{(b)} \;\; g_2^{(b)} \;\; \cdots \;\; g_\ell^{(b)} \,].$$

*Here, each block $G^{(b)} \in \mathbb{F}_q^{k\times\ell}$ has $\ell$ columns. It corresponds to one chain $1 \prec 2 \prec \cdots \prec \ell$. For a profile $t = (t_1, \ldots, t_m) \in \{0, 1, \ldots, \ell\}^m$, define*

$$G^{(b)}_{>t_b} := [\, g^{(b)}_{t_b+1} \; g^{(b)}_{t_b+2} \; \cdots \; g^{(b)}_{\ell} \,] \in \mathbb{F}_q^{k\times(\ell-t_b)}, \qquad A(t) := \begin{bmatrix} (G^{(1)}_{>t_1})^\top \\ \vdots \\ (G^{(m)}_{>t_m})^\top \end{bmatrix} \in \mathbb{F}_q^{(\sum_b(\ell-t_b))\times k}.$$

*Thus, $G^{(b)}_{>t_b}$ is obtained from $G^{(b)}$ by removing its first $t_b$ columns. Let $|t|_1$ denote the sum $t_1 + \cdots + t_m$. Then, in this notation, we have*

(a) *The minimum NRT distance of $C$ satisfies*

$$d_{\mathrm{bNRT}}(C) = \min\big\{\, |t|_1 = t_1 + \cdots + t_m : \mathrm{rank}(A(t)) < k \,\big\}.$$

*Equivalently, $d_{\mathrm{bNRT}}(C)$ is the smallest integer $w$ for which there exists a profile $t$ with $|t|_1 = w$ such that* $\mathrm{nullity}(A(t)) \ge 1$. *If $t$ attains the minimum, then necessarily* $\mathrm{rank}(A(t - e_b)) = k$ *for each $b$ with $t_b > 0$.*

(b) *(*Lower bound from a full-rank top slice.*) If integers $s_1, \dots, s_m$ satisfy $0 \le s_b \le \ell$ and the stacked matrix*

$$A(s) = \begin{bmatrix} (G^{(1)}_{>s_1})^\top \\ \vdots \\ (G^{(m)}_{>s_m})^\top \end{bmatrix}$$

*has full column rank* $\operatorname{rank}(A(s)) = k$*, then*

$$d_{\mathrm{bNRT}}(C) \;\ge\; 1 + \sum_{b=1}^{m} s_b.$$

*Proof.* (a) For each $t$, the equation $A(t)u^\top = 0$ imposes that for every block $b$, all coordinates of the codeword $uG$ above level $t_b$ are zero. Hence there exists a nonzero codeword with block heights at most $t$ if and only if $\ker A(t) \neq \{0\}$, that is, $\operatorname{rank}(A(t)) < k$. Minimizing $|t|_1$ over such profiles therefore yields $d_{\mathrm{bNRT}}(C) = \min\{|t|_1 : \operatorname{rank}(A(t)) < k\}$. The minimality condition follows from the monotonicity of the rank in each coordinate $t_b$.

(b) Suppose $A(s)$ has full column rank $k$. Then for every $t \le s$ (componentwise) the submatrix $A(t)$ is obtained by deleting rows from $A(s)$, and hence also has full column rank $k$. Consequently $\operatorname{rank}(A(t)) = k$ for all $|t|_1 \le |s|_1$, so no nonzero $u \in \mathbb{F}_q^k$ can satisfy $A(t)u^\top = 0$. By part (a) and the rank-monotonicity argument used in Proposition 4.6, we conclude that $d_{\mathrm{bNRT}}(C) \ge 1 + \sum_{b=1}^{m} s_b$. □

Next, we describe a method for finding a lower bound for $d_{\mathrm{bNRT}}(C)$ from a parity-check matrix.

**Proposition 6.2** (A computable lower bound for $d_{\mathrm{bNRT}}(C)$ from a parity-check matrix)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear block-NRT code with $n = m\ell$, parity-check matrix $H \in M_{r\times n}(\mathbb{F}_q)$, $r = n - k$. Partition the columns of $H$ into $m$ chains (blocks)*

$$H = \big[\, H^{(1)} \mid H^{(2)} \mid \cdots \mid H^{(m)} \,\big], \qquad H^{(b)} = [\, h_1^{(b)} \;\cdots\; h_\ell^{(b)} \,] \in M_{r\times \ell}(\mathbb{F}_q),$$

*where inside each block the column order respects the chain $1 \prec 2 \prec \cdots \prec \ell$. For a profile $u = (u_1, \dots, u_m) \in \{0, 1, \dots, \ell\}^m$ define the* block-prefix submatrix

$$H[u] \;:=\; \big[\, H^{(1)}_{[u_1]} \;\big|\; \cdots \;\big|\; H^{(m)}_{[u_m]} \,\big], \quad H^{(b)}_{[u_b]} := [\, h_1^{(b)} \;\cdots\; h_{u_b}^{(b)} \,],$$

*and set $|u|_1 := u_1 + \cdots + u_m$. If there exists $s = (s_1, \dots, s_m)$ with $0 \le s_b \le \ell$ such that*

$$\operatorname{rank}\big(H[s]\big) \;=\; |s|_1,$$

*then the minimum NRT distance satisfies*

$$d_{\mathrm{bNRT}}(C) \;\ge\; 1 + |s|_1.$$

*Proof.* By the parity-check characterization of the NRT distance (see Prop. 4.1),

$$d_{\mathrm{bNRT}}(C) = \min\big\{|u|_1 \ge 1 :\; \operatorname{rank}(H[u]) < |u|_1\big\}.$$

Assume $\operatorname{rank}(H[s]) = |s|_1$. For any $u \le s$ (componentwise), $H[u]$ is obtained from $H[s]$ by deleting columns, hence $\operatorname{rank}(H[u]) = |u|_1$ (no loss of rank can occur before the number of columns). Therefore there is no $u$ with $|u|_1 \le |s|_1$ that violates full column rank. By the displayed formula, this implies $d_{\mathrm{bNRT}}(C) \ge 1 + |s|_1$. □

### 6.2 Sum-rank case.

Next, we discuss a lower bound for $d_{\mathrm{SR}}(C)$ from $H$ for the sum-rank case.

**Proposition 6.3** (A computable lower bound for $d_{\mathrm{SR}}(C)$ from a parity-check matrix)**.** *Fix block sizes $\ell_1, \ldots, \ell_m$ with $n = \sum_b \ell_b$ and integers $h_1, \ldots, h_m \geq 1$. Let $H \in M_{r\times n}(\mathbb{F}_q)$, $r = n - k$, be full row rank and partition its columns as*

$$H = \left[\, H^{(1)} \mid \cdots \mid H^{(m)} \,\right], \qquad H^{(b)} \in \mathbb{F}_q^{r\times \ell_b}.$$

*Let $C := \ker(H)$ and $d_{\mathrm{SR}}(C)$ be the sum-rank minimum distance. Suppose there exist disjoint column index sets $S_b \subseteq \{1, \ldots, \ell_b\}$ with*

$$s_b := |S_b| \;\leq\; \min\{\ell_b, h_b\} \quad \textit{for each } b,$$

*such that the union of columns $\{\, h_j^{(b)} : j \in S_b,\ b = 1, \ldots, m \,\}$ is linearly independent in $\mathbb{F}_q^r$. Then*

$$d_{\mathrm{SR}}(C) \;\geq\; 1 + \sum_{b=1}^{m} s_b.$$

*Proof.* Write $s = (s_1, \ldots, s_m)$ and let $t := \sum_b s_b$. For any $u = (u_1, \ldots, u_m)$ with $0 \leq u_b \leq s_b$ and $\sum_b u_b \leq t$, choose $U^{(b)} \in M_{\ell_b \times u_b}(\mathbb{F}_q)$ to be the selection matrix that picks any $u_b$ columns from $S_b$. By construction, the concatenation $[\, H^{(1)}U^{(1)} \mid \cdots \mid H^{(m)}U^{(m)} \,]$ is a *column submatrix* of the independent set of size $t$, hence has rank $\sum_b u_b$. Therefore, for every $u$ with $\sum_b u_b \leq t$ we have

$$\mathrm{rk}_H(u) \;=\; \sum_b u_b,$$

in the notation of the rank-profile test. Applying Proposition 5.2, which states that $d_{\mathrm{SR}}(C) > t$ iff $\mathrm{rk}_H(u) = \sum_b u_b$ for all $u$ with $\sum_b u_b \leq t$, we conclude $d_{\mathrm{SR}}(C) \geq 1 + t = 1 + \sum_b s_b$. □

## 7 Metric-Based Cryptosystems and Their Security Analyses

Our proposed cryptosystems proceed as in the classical McEliece/Niederreiter cryptosystems except that we use metrics other than Hamming metrics for our codes. This approach drastically changes the whole attack and security scenarios. The purpose of this section is to discuss these matters.

### 7.1 One-prefix attack to a single chain NRT code

We describe a possible *one-prefix* attack if a single chain NRT code is used instead of a block-NRT code. Let $M \in M_{r\times n}(\mathbb{F}_q)$ be a public parity-check (with $r = n - k$) and let $t \leq r$ be the published decoding radius. Given a ciphertext $s = Me^\top$ where the error has single-chain NRT weight $w_{\mathrm{NRT}}(e) \leq t$, the following public procedure recovers $e$ in polynomial time whenever all prefixes $M_{[u]}$ have full column rank for $u \leq t$.

We are now ready to formalize the *one-prefix attack* as a simple iterative procedure, given in Algorithm 1 below. At each step we test membership in a column span, and under the unique-decoding condition the attack either recovers the error vector or declares failure.

**Algorithm 1** One-prefix attack

**Require:** Syndrome $s$, matrices $M_{[u]}$, error bound $t$

**for** $u = 1$ to $t$ **do**
  Test if $s \in \mathrm{colspan}(M_{[u]})$ (for example, by row-reducing $[M_{[u]} \mid s]$ and checking $\mathrm{rank}([M_{[u]} \mid s]) = \mathrm{rank}(M_{[u]})$).
  **if** test is true **then**
    Solve the system $M_{[u]}x = s$ for unique $x \in \mathbb{F}_q^u$ (guaranteed when $\mathrm{rank}(M_{[u]}) = u$).
    **return** $e = (x_1, \ldots, x_u, 0, \ldots, 0) \in \mathbb{F}_q^n$
  **end if**
**end for**
**return** failure

Let us explain why one-prefix attack may work. Let $u^\star := w_{\mathrm{NRT}}(e)$. By definition of the single-chain NRT weight, $e = (e_1, \ldots, e_{u^\star}, 0, \ldots, 0)$ with $e_{u^\star} \neq 0$, hence $s = Me^\top \in \mathrm{colspan}(M_{[u^\star]})$. Minimality of $u^\star$ implies $s \notin \mathrm{colspan}(M_{[u]})$ for all $u < u^\star$. If, in addition, $\mathrm{rank}(M_{[u]}) = u$ for every $u \leq t$ (the standard uniqueness condition up to $t$), then for $u = u^\star$ the system $M_{[u]}x = s$ has a *unique* solution, necessarily $x = (e_1, \ldots, e_{u^\star})$, so the algorithm outputs the correct $e$.

Note that each membership test and solve can be done in $O(r^2 u)$ field operations by incremental rank maintenance. The overall running time is polynomial in $n$.

Nevertheless, the one-prefix attack does not always work. If some prefix is rank-deficient in the sense that $\mathrm{rank}(M_{[u_0]}) < u_0$ for some $u_0 \leq t$, then the membership test may pass at $u_0$ but the linear system has multiple solutions, so the procedure above does not yield a unique $e$. However, in that case the code has $d_{\mathrm{NRT}}(\ker M) \leq u_0$, so *unique* decoding up to the published radius $t$ is impossible for any decoder (trapdoor or public). Thus, in the single-chain setting one faces a dichotomy:

*either* all prefixes up to $t$ are full rank $\Rightarrow$ public decoding as above,
*or* some prefix $\leq t$ is rank-deficient $\Rightarrow$ unique decoding up to $t$ fails.

We proceed to explain why one-prefix attack is not successful if a block-NRT code is used. Indeed, for a block-NRT code with $m$ blocks, the attacker would need to guess a *multi-prefix* $u = (u_1, \ldots, u_m)$ with $|u|_1 \leq t$ and test $s \in \mathrm{colspan}(M_{[u]})$. However, there are

$$N(m,t) = \#\{u \in \{0, \ldots, \ell\}^m : \ |u|_1 \leq t\} = \sum_{j=0}^{t} \binom{m+j-1}{j}$$

such candidates (for $\ell \geq t$, $N(m,t) = \binom{m+t}{t}$), which grows exponentially when $t = \alpha n$ and $m = \Theta(n)$. In other words, the number of blocks grows linearly with $n$ up to constant factors. Under these conditions, the single-prefix shortcut disappears.

**Remark 7.1.** There is no "prefix" in the sum-rank case as in the block NRT case. A public attacker given $s = Me^\top$ and a budget $t$ must range over all rank profiles $u$ with $\sum_b u_b \leq t$ and, for each $u$, all $u_b$-dimensional column subspaces inside block $b$. The count is

$$\sum_{j=0}^{t} \sum_{\substack{u \in \mathbb{Z}_{\geq 0}^m \\ \sum u_b = j}} \prod_{b=1}^{m} \begin{bmatrix} \ell_b \\ u_b \end{bmatrix}_q,$$

where $\begin{bmatrix}\ell\\ u\end{bmatrix}_q$ is the Gaussian binomial (number of $u$-subspaces of $\mathbb{F}_q^\ell$). For $t = \alpha n$ and $m = \Theta(n)$ this is exponential in $n$, so the single-prefix shortcut from the chain-NRT case disappears.

All size and compression remarks from the previous section carry over to the sum-rank instantiation unchanged.

# 8 Hardness of Canonical Block-NRT Factorization

We start with introducing the notions of block-rook pattern, profile, and representative. As before, let $n = m\ell$ for $m, \ell \in \mathbb{Z}_{>0}$ and $n \geq 3$. We partition $n$ columns of elements of $M_{r\times n}^{\text{full}}(\mathbb{F}_q)$ into $\ell$ consecutive blocks $C_1, \ldots, C_\ell$ of width $m$. Recall also the notation $G_n$ for the right isometry group, defined in (2).

**Definition 8.1** (Block-rook canonical representative)**.** Fix a profile vector $\mathbf{k} = (k_1, \ldots, k_\ell)$ with $0 \leq k_b \leq m$ and set $r := \sum_b k_b$. Partition the $n = m\ell$ columns into blocks $C_1, \ldots, C_\ell$ of width $m$. Let $J_b$ be the set of the rightmost $k_b$ columns in block $C_b$, and put $J := \bigcup_b J_b$ so $|J| = r$. The *block-rook canonical representative of profile* $\mathbf{k}$, denoted $R(\mathbf{k}) \in M_{r\times n}(\mathbb{F}_q)$, is the matrix whose columns indexed by $J$ form the identity $I_r$, and whose non-pivot columns are unconstrained.

For a block-rook canonical representative $R(\mathbf{k})$ with profile $\mathbf{k}$, we define the *block-rook orbit of profile* $\mathbf{k}$ as the $GL_r(\mathbb{F}_q) \times G_n$-orbit of $R(\mathbf{k})$, that is,

$$\mathcal{O}_{\mathbf{k}} \;:=\; \{\, A\, R(\mathbf{k})\, B \;:\; A \in GL_r(\mathbb{F}_q),\; B \in G_n \,\}.$$

**Example 8.2.** Let $r = 6$, $\ell = 3$, $m = 4$, $n = m\ell = 12$, and fix the profile $\mathbf{k} = (2, 1, 3)$. Then $\mathbf{k}$ is admissible for $(6, 12)$. Partition the 12 columns of a general element of $M_{6\times 12}^{\text{full}}$ into three blocks

$$C_1 = \{1, 2, 3, 4\}, \qquad C_2 = \{5, 6, 7, 8\}, \qquad C_3 = \{9, 10, 11, 12\}.$$

Choose pivot columns as follows: two in $C_1$ (columns 2 and 4), one in $C_2$ (column 7), and three in $C_3$ (columns $9, 10, 12$). Arrange the pivot submatrix to be the $6 \times 6$ identity matrix. All non-pivot columns are unconstrained (denoted by $*$ below). Then a block-rook canonical representative $R(\mathbf{k}) \in M_{6\times 12}(\mathbb{F}_q)$ looks like

$$R(\mathbf{k}) \;=\; \left[\begin{array}{cccc|cccc|cccc} * & 1 & * & 0 & * & * & 0 & * & 0 & 0 & * & 0 \\ * & 0 & * & 1 & * & * & 0 & * & 0 & 0 & * & 0 \\ * & 0 & * & 0 & * & * & 1 & * & 0 & 0 & * & 0 \\ * & 0 & * & 0 & * & * & 0 & * & 1 & 0 & * & 0 \\ * & 0 & * & 0 & * & * & 0 & * & 0 & 1 & * & 0 \\ * & 0 & * & 0 & * & * & 0 & * & 0 & 0 & * & 1 \end{array}\right].$$

Here the set of pivot columns is $J = \{2, 4\} \cup \{7\} \cup \{9, 10, 12\}$, so in each block $C_b$ the number of pivots equals $k_b$. All entries in the remaining (non-pivot) columns are unconstrained.

**Remark 8.3.** Under the restricted right action of $G_n$, one generally cannot eliminate all non-pivot columns as in the full $GL_n(\mathbb{F}_q)$ case, hence the canonical representative only prescribes the pivot subset. This is the appropriate analogue of the rook form for block-NRT actions.

We now formulate two problems that will be useful for proving the security hardness of our cryptosystem. In the subsequent subsection, we will relate these problems to the "exact cover by 3-sets problem" abbreviated to X3C in the literature.

**Problem 8.4.** Given $M \in M_{r\times n}(\mathbb{F}_q)$, a block partition $C_1, \ldots, C_\ell$ of width $m$, and a profile $\mathbf{k}$ with $\sum_b k_b = r$, decide whether $M \in \mathcal{O}_{\mathbf{k}}$.

**Problem 8.5.** Given the same input, find $A \in GL_r(\mathbb{F}_q)$ and $B \in G_n$ such that $AMB = R(\mathbf{k})$, or report that none exist.

## 8.1 Exact Cover by 3-Sets (X3C).

Canonicalization under $GL_r(\mathbb{F}_q) \times G_n$ is the algebraic task that underlies "recovering structure" from obfuscated public matrices in block-NRT settings. If Problem 8.4 is NP-complete, then unless P = NP there is no polynomial-time algorithm that, given an arbitrary full-rank matrix $M$, can always recognize whether its orbit under $GL_r(\mathbb{F}_q) \times G_n$ contains a block-rook canonical representative of a given profile. It will be practical to give a name to this problem: For $\mathbf{k} = (k_1, \ldots, k_\ell)$, the *BNCF-Decision problem* asks whether there exist

$$A \in GL_r(\mathbb{F}_q), \qquad B \in G_n$$

such that

$$AMB = R(\mathbf{k}),$$

where $R(\mathbf{k})$ is the block-rook canonical representative of profile $\mathbf{k}$.

The BNCF-problem is exactly the problem that we are going to relate to X3C.

**Definition 8.6.** Let $U$ be the ground set defined by $U = \{u_1, \ldots, u_{3t}\}$. Let $\mathcal{S}$ be a family $\mathcal{S} = \{S_1, \ldots, S_s\} \subseteq \binom{U}{3}$ of 3-element subsets of $U$. The *X3C-problem* asks if whether there exists a subfamily $\mathcal{S}' \subseteq \mathcal{S}$ of size $t$ such that the sets in $\mathcal{S}'$ are pairwise disjoint and $\bigsqcup_{S\in\mathcal{S}'} S = U$.

X3C is a classical NP-complete problem [19, 15]. We reduce X3C to the block-NRT canonical-form problem below.

To this end, we will use three pivot columns per selected 3-set, which is the natural way to obtain a genuine row-wise rook pattern on the pivot subset.

**Construction 8.7.** Let $U = \{u_1, \ldots, u_{3t}\}$ and $\mathcal{S} = \{S_1, \ldots, S_s\} \subseteq \binom{U}{3}$ be an X3C instance. Set $r = 3t$ and $\ell = s$. For each set $S_j = \{u_a, u_b, u_c\}$, create a block $C_j$ of width $m = 3$ with three *element columns*

$$c_{j,1} = e_{u_a}, \qquad c_{j,2} = e_{u_b}, \qquad c_{j,3} = e_{u_c} \ \in \ \mathbb{F}_q^r,$$

and zeros elsewhere. Then we define the *instance matrix*,

$$M_I \in M_{r\times 3s}(\mathbb{F}_q),$$

as the $r \times n$ 0/1 matrix whose columns are the three unit vectors of the elements in each set, concatenated over all $j$. Notice that, $M_I$ is not a rook matrix in general. Indeed, the same element $u_i \in U$ may appear in multiple subsets, so the corresponding row can have several ones. The idea here is to find an appropriate profile vector to construct a rook matrix. To this end, we define

$$\mathbf{k} \ := \ (\underbrace{3, \ldots, 3}_{t \text{ entries}}, \underbrace{0, \ldots, 0}_{\ell - t \text{ entries}}).$$

**Remark 8.8.** In this construction, we assumed that the number of columns is a multiple of 3. When $n$ is not divisible by 3, we will use padding as explained in Remark 8.14 at the end of this section.

We proceed with an example.

**Example 8.9.** Let $U$ be the ground set defined by

$$U = \{u_1, \ldots, u_6\} \quad (t = 2,\ 3t = 6)$$

and take $s = 4$ sets

$$S_1 = \{u_1, u_2, u_3\}, \quad S_2 = \{u_4, u_5, u_6\}, \quad S_3 = \{u_1, u_4, u_5\}, \quad S_4 = \{u_2, u_3, u_6\}.$$

Clearly $\mathcal{S}' = \{S_1, S_2\}$ is an exact cover of $U$ by $t = 2$ triples.

We now build the corresponding instance for BNCF-Decision as in Construction 8.7. We set

$$r = 3t = 6, \qquad \ell = s = 4, \qquad m = 3, \qquad n = 3s = 12.$$

For each $j \in \{1, 2, 3, 4\}$ we form a block $C_j \in M_{6\times 3}(\mathbb{F}_q)$ whose columns are the unit vectors of the elements in $S_j$.

Explicitly, writing rows in the order $(u_1, \ldots, u_6)$, we have

$$C_1 = \left[e_{u_1} \,|\, e_{u_2} \,|\, e_{u_3}\right] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad C_2 = \left[e_{u_4} \,|\, e_{u_5} \,|\, e_{u_6}\right] = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$C_3 = \left[e_{u_1} \,|\, e_{u_4} \,|\, e_{u_5}\right] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \qquad C_4 = \left[e_{u_2} \,|\, e_{u_3} \,|\, e_{u_6}\right] = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The instance matrix is then

$$M_I = \left[C_1 \,\|\, C_2 \,\|\, C_3 \,\|\, C_4\right] \in M_{6\times 12}(\mathbb{F}_q),$$

where the 12 columns are exactly the 3 unit columns of each $S_j$, concatenated blockwise. The profile vector for this instance matrix is

$$\mathbf{k} = (3, 3, 0, 0),$$

meaning that in a YES-instance we expect exactly three pivot columns in each of two blocks, and no pivots in the remaining two blocks.

We now state the two key lemmas whose proofs are simple.

**Lemma 8.10.** *If the X3C instance has an exact cover $\mathcal{S}' = \{S_{j_1}, \ldots, S_{j_t}\}$, then there exist $A \in GL_r(\mathbb{F}_q), B \in G_n$ with $AM_IB = R(\mathbf{k})$ for a block-rook representative of profile $(\underbrace{3, \ldots, 3}_{t}, 0, \ldots, 0)$.*

*Proof.* Write each selected set as $S_{j_a} = \{u_{a_1}, u_{a_2}, u_{a_3}\}$. Let $B \in G_n$ be a block permutation that moves the blocks $\{C_{j_a}\}_{a=1}^{t}$ to the first $t$ block positions. Within each selected block, optionally permute the three columns to match a fixed pivot order. In unselected blocks, $B$ is arbitrary. Indeed, its effect is immaterial. Then the first $t$ blocks of $M_IB$ are exactly the unit columns $(e_{u_{a_1}}, e_{u_{a_2}}, e_{u_{a_3}})$. Because $\mathcal{S}'$ is an exact cover, these $3t$ rows are all distinct, so they form a rook matrix on some pivot row set $P$. We take $A$ to be a row permutation (or $I_r$) so that the rook sits in a prescribed row order. All non-pivot columns are unconstrained. Therefore $AM_IB = R(\mathbf{k})$ for the profile $(\underbrace{3, \ldots, 3}_{t}, 0, \ldots, 0)$. □

**Example 8.11** (From an exact cover to a block-rook form)**.** Continuing Example 8.9, the X3C instance has the exact cover $\mathcal{S}' = \{S_1, S_2\}$. We now exhibit matrices $A \in GL_6(\mathbb{F}_q)$, $B \in G_{12}$ such that $AM_IB$ is a block-rook canonical form of profile $\mathbf{k} = (3, 3, 0, 0)$.

In this example the desired blocks already occupy the first two block positions, so we can take $B$ to be block-diagonal with

$$B = \operatorname{diag}(I_3,\ I_3,\ B_3,\ B_4),$$

where $I_3$ acts on the columns inside $C_1$ and $C_2$, and $B_3, B_4 \in S_3$ are arbitrary $3 \times 3$ permutation matrices acting within $C_3$ and $C_4$. (Their precise values do not matter, since these blocks carry no pivots.)

The first two blocks of $M_IB$ are thus still

$$C_1 = \big[e_{u_1}, e_{u_2}, e_{u_3}\big], \qquad C_2 = \big[e_{u_4}, e_{u_5}, e_{u_6}\big].$$

Because $\mathcal{S}'$ is an exact cover, the six rows

$$u_1, u_2, u_3, u_4, u_5, u_6$$

each appear exactly once among these six columns. Hence the $6 \times 6$ submatrix spanned by rows $\{u_1, \ldots, u_6\}$ and the pivot columns in $C_1, C_2$ is a rook matrix: each of these rows and each of these columns has a single 1.

To put this rook into a fixed canonical row order, we take $A$ to be the row permutation that sends $(u_1, \ldots, u_6)$ to the prescribed pivot order (e.g., the identity permutation if the canonical order is already $(u_1, \ldots, u_6)$). Then $AM_IB$ has the form

$$AM_IB = \big[R_1 \,\|\, R_2 \,\|\, * \,\|\, *\big],$$

where $R_1, R_2$ are $6 \times 3$ rook blocks (each column has a single 1 in a distinct row, and different blocks use disjoint row sets), and the remaining columns (indicated by $*$) are non-pivot columns. This is exactly a block-rook representative of profile $(3, 3, 0, 0)$, as claimed in Lemma 8.10.

**Lemma 8.12.** *Conversely, suppose there exist $A \in GL_r(\mathbb{F}_q)$ and $B \in G_n$ such that $AM_IB$ is a block-rook canonical representative with profile $\mathbf{k} = (\underbrace{3, \ldots, 3}_{t}, 0, \ldots, 0)$. Then the set of blocks carrying the $3t$ pivot columns corresponds to an exact cover of $U$ by $t$ sets from $\mathcal{S}$.*

*Proof.* By definition of the block-rook form, the pivot subset consists of exactly $3t$ columns, three from each of $t$ blocks, and these pivot columns occupy distinct rows. Since every column of $M_I$ is a unit vector, the only way for the pivot subset to be rook on the rows is that each $u_i$ appears exactly once among the chosen pivot columns. Hence the corresponding $t$ blocks select $t$ sets whose union is $U$ and are pairwise disjoint. Hence it is an exact cover. □

We now give an example towards explaining why the pivot blocks must form an exact cover.

**Example 8.13.** We continue to use Example 8.9, with $U = \{u_1, \ldots, u_6\}$ and blocks $C_1, \ldots, C_4$. Now assume toward a contradiction that a block-rook canonical representative with profile $\mathbf{k} = (3, 3, 0, 0)$ could be obtained from $M_I$ by applying some $A \in GL_6(\mathbb{F}_q)$ and some $B \in G_{12}$, but that the two pivot blocks did not correspond to an exact cover of $U$.

For instance, consider selecting blocks $C_1$ and $C_4$ as pivot blocks. They encode the sets

$$S_1 = \{u_1, u_2, u_3\}, \qquad S_4 = \{u_2, u_3, u_6\}.$$

Any choice of three pivot columns in $C_1$ and three pivot columns in $C_4$ must include each element of these sets at least once. However, $S_1$ and $S_4$ both contain $u_2$ and $u_3$, so among the six pivot columns we necessarily see $u_2$ at least twice or $u_3$ at least twice (in fact both), before any row operations are applied.

Since $A$ is invertible, it acts on rows by forming linear combinations, but it cannot turn two identical unit vectors $e_{u_i}, e_{u_i}$ into unit vectors in distinct rows. Any linear combination of two columns supported on the same row will still be supported on that row. Hence no choice of $A$ can make the pivot subset rook on the rows. Therefore blocks $C_1$ and $C_4$ cannot both carry three pivot columns in a block-rook form.

The same obstruction occurs for any pair of blocks that are not disjoint on $U$: if two sets $S_j$ and $S_{j'}$ share an element $u_i$, then choosing three pivot columns in each of $C_j, C_{j'}$ necessarily uses the row $u_i$ at least twice in the pivot subset, contradicting the rook property.

Consequently, the only way to obtain a block-rook representative with profile $(3, 3, 0, 0)$ is to pick two blocks whose underlying sets are pairwise disjoint and whose union is all of $U$, i.e., an exact cover. In our example this forces the pivot blocks to be exactly $C_1$ and $C_2$, corresponding to the exact cover $\{S_1, S_2\}$. This illustrates the converse direction of Lemma 8.12: the set of blocks carrying the $3t$ pivot columns indeed defines an exact cover of $U$ by $t$ sets from $\mathcal{S}$.

**Remark 8.14** (Padding for general $n$)**.** The reduction sets $\ell = s$ and $m = 3$, hence $n = 3s$ by construction. To allow arbitrary $n$, we pad with at most two dummy columns (equivalently, append a dummy block of width 3) and extend the profile by 0 so that the new block carries no pivots. This preserves YES/NO instances and keeps the reduction polynomial. Likewise, for block width $m' \geq 3$, place three "element columns" per block and fill the remaining $m' - 3$ columns with dummy entries. We then continue to use $k_b \in \{0, 3\}$ as before.

# 9 Decoding Hardness

We formalize decoding for our metrics and relate it, via Karp reductions, to the classical Hamming and Rank Syndrome Decoding problems. Throughout, all matrices are over a finite field $\mathbb{F}_q$, and $H \in M_{r \times n}(\mathbb{F}_q)$ has full row rank.

## 9.1 Syndrome decoding problems

**Definition 9.1** (Hamming Syndrome Decoding (HSD))**.** Given $(H, s, t)$ with $H \in M_{r\times n}(\mathbb{F}_q)$, $s \in \mathbb{F}_q^r$, and $t \in \mathbb{N}$, decide (or find) $e \in \mathbb{F}_q^n$ such that $He^\top = s$ and $w_{\mathrm{H}}(e) \le t$. This is NP-complete (decision) and NP-hard (search) [3].

**Definition 9.2** (Block-NRT Syndrome Decoding (NRT-SD))**.** Fix a column partition $n = m\ell$ into $\ell$ blocks of size $m$ and the column NRT weight $w_{\mathrm{NRT}}(\cdot)$ (first nonzero per column contributes its row index $+1$). Given $(H, s, t, \text{partition})$, decide (or find) $e \in \mathbb{F}_q^n$ such that $He^\top = s$ and $w_{\mathrm{NRT}}(e) \le t$.

**Definition 9.3** (Sum-Rank Syndrome Decoding (SR-SD))**.** Fix a partition $n = \sum_{b=1}^{\ell} n_b$; view each block $e_b$ as an $r_b \times n_b$ matrix over the base field and define $w_{\mathrm{SR}}(e) = \sum_{b=1}^{\ell} \mathrm{rank}(e_b)$. Given $(H, s, t, \text{partition})$, decide (or find) $e$ with $He^\top = s$ and $w_{\mathrm{SR}}(e) \le t$.

## 9.2 Reductions from classical decoding

We show that the classical decoding problems reduce, in a size- and time-preserving manner, to our metric variants. Hence NRT-SD and SR-SD are at least as hard as their classical Hamming or Rank counterparts.

**Theorem 9.4** (HSD $\le_p$ NRT-SD)**.** *For any HSD instance $(H, s, t)$ over $\mathbb{F}_q$ of length $n$, there is a polynomial-time reduction to an NRT-SD instance $(H', s', t', \text{partition})$ over the same field such that solutions correspond 1-to-1. Setting block size $m = 1$ and $\ell = n$ gives $H' = H$, $s' = s$, $t' = t$, and $w_{\mathrm{NRT}}(e) = w_{\mathrm{H}}(e)$ for all $e \in \mathbb{F}_q^n$. Consequently, NRT-SD is NP-hard (search) and NP-complete (decision).*

*Proof.* With $m = 1$, each column is its own block and the NRT weight counts the number of nonzero columns exactly once. Thus $w_{\mathrm{NRT}}(e) = w_{\mathrm{H}}(e)$. □

**Theorem 9.5** (HSD $\le_p$ SR-SD and Rank-SD $\le_p$ SR-SD)**.** *For any HSD instance $(H, s, t)$, choosing the sum-rank partition with all blocks of size 1 yields $w_{\mathrm{SR}}(e) = w_{\mathrm{H}}(e)$, giving an equivalent SR-SD instance. Conversely, for any Rank Syndrome Decoding instance of length $n$ (single block), taking the sum-rank partition with $\ell = 1$ recovers rank weight exactly. Hence SR-SD is NP-hard (decision and search).*

*Proof.* Immediate from the definitions: the sum-rank metric specializes to the Hamming metric (all blocks size 1) and to the rank metric (single block). □

Thus, any algorithm solving NRT-SD or SR-SD in polynomial time would solve HSD or Rank-SD in polynomial time. Therefore, decoding in our metrics is at least as hard as decoding in the classical settings.

## 9.3 Implications for Niederreiter cryptosystems

We next discuss the cryptographic implications of these hardness reductions.

**Definition 9.6** (Metric weight)**.** Let metric $\in \{\mathrm{Ham}, \mathrm{NRT}, \mathrm{SR}\}$ denote one of the metrics considered in this work. For $e \in \mathbb{F}_q^n$, define

$$w_{\mathrm{metric}}(e) := d_{\mathrm{metric}}(e, 0).$$

**Corollary 9.7** (Syndrome one-wayness under NRT/SR decoding hardness)**.** *Fix parameters $(q, n, r, t)$ and a partition (block-NRT or sum-rank). Let $H \leftarrow \mathcal{D}$ be sampled as in KeyGen and let $e$ be drawn from a distribution supported on $\{e : w_{\text{metric}}(e) \leq t\}$. Given $(H, s)$ with $s = He^\top$, recovering any $e'$ with $w_{\text{metric}}(e') \leq t$ and $He'^\top = s$ is at least as hard as HSD (block-NRT case) or as hard as HSD/Rank-SD (sum-rank case), by Theorems 9.4 and 9.5.*

Information-set decoding (ISD) algorithms, initiated by Prange [35] and refined through Stern [41], Dumer [10], May–Meurer–Thomae [23], and May–Ozerov [24], form the canonical exponential-time decoding attacks on random linear codes. In code-based cryptography, the security level is determined by the best known ISD work factors, typically evaluated for random $(n, k, t)$ codes in the relevant metric. Our parameter choices follow the classical McEliece/Niederreiter practice of selecting $(n, k, t)$ such that these ISD complexities exceed $2^\lambda$.

The hardness reductions above provide worst-case NP-hardness. As in the classical setting, cryptographic security further relies on the empirical intractability of decoding random-looking public keys (ISD attacks) at the chosen parameters.

## 9.4 Parameter-level comparability to classical designs

Classical Niederreiter over binary Goppa codes chooses $(n, k, t)$ so that Prange/Dumer/May–Ozerov ISD costs exceed $2^\lambda$. In our setting:

- **Block-NRT:** ISD strategies (choosing an information set, guessing per-block structure, etc.) generalize with essentially the same exponential profile when $m = \Theta(n)$; once the partition is fixed, the work factors emulate the Hamming case. By Theorem 9.4, any asymptotic improvement would contradict HSD hardness.
- **Sum-rank:** SR decoding inherits hardness from both Hamming and Rank; the single-block case is Rank-SD (NP-hard) and the all-blocks-size-1 case is Hamming-SD. Known rank-metric ISD lower bounds therefore apply to SR-SD via the one-block slice.

Hence, at equal $(n, k, t)$ and comparable field sizes, decoding in our block-NRT or sum-rank Niederreiter systems is *no easier* than in the classical designs, up to metric-specific constant factors.

## 9.5 Security takeaway

In the next theorem, $w_{\text{metric}}$ is the metric weight of Definition 9.6.

**Theorem 9.8** (Decoding hardness carries over)**.** *Suppose there exists a PPT adversary that, on a nonnegligible fraction of public keys $H \leftarrow \mathcal{D}$ and syndromes $s = He^\top$ with $w_{\text{metric}}(e) \leq t$, outputs some $e'$ with $He'^\top = s$ and $w_{\text{metric}}(e') \leq t$. Then there exists a PPT adversary that solves HSD (NRT case) or HSD* or *Rank-SD (sum-rank case) with the same success probability and comparable running time.*

*Proof.* Embed the given HSD (or Rank-SD) instance into our metric using the partitions of Theorems 9.4–9.5, feed the embedded instance to the assumed adversary, and map the recovered error back unchanged. □

### 9.6 Notes on obfuscation and decodability

Our public key is $M = SHB$ with $S \in GL_r(\mathbb{F}_q)$ dense and $B$ drawn from an isometry subgroup ($G_n$ for the block-NRT metric; $\mathcal{G}_{\mathrm{SR}}$ for the sum-rank metric). These scramblers *preserve* metric weight and thus the decoding radius while making $M$ statistically dense. The reductions above do not rely on any distributional indistinguishability property of $M$, so the decoding hardness statements apply as stated. The reduction in Theorem 9.8 is oblivious to these transformations.

**Remark 9.9.** We establish *one-wayness* of the public syndrome map by reducing block-NRT and sum-rank decoding to classical Hamming/Rank decoding at our parameter regimes. We do not claim IND-CPA/CCA security; a standard KEM transform can be layered on top. The Fujisaki–Okamoto (FO) transform [14] (or salted SFO variants) yields an IND-CCA2 KEM in the random-oracle model under the same decoding-hardness assumptions.

Public keys are obfuscated parity-check matrices $M = SH_{\mathrm{sys}}(PD)$ drawn from a metric-preserving subgroup. Indistinguishability of $M$ is therefore heuristic in the same sense as in Classic McEliece/Niederreiter.

## 10 Inner–Outer Design via a Rowwise NRT Inner Code

We present a metric-aware concatenated design that couples a short *inner* code across the $\ell$ rows (measured in the single-chain NRT metric with a set of *outer* binary Goppa codes [34] across the $m$ columns. The resulting code is a matrix code in $M_{\ell\times m}(\mathbb{F}_{2^s})$ that is naturally measured in the block-NRT metric and achieves a multiplicative distance boost over plain Hamming-metric Goppa codes while retaining modular decoding in the spirit of Forney concatenation [13].

### 10.1 Construction

We fix the following ingredients.

- An *inner* linear code $V \leq \mathbb{F}_{2^s}^{\ell}$ of dimension $k_V$ and single-chain NRT distance $\delta_V \geq 2$. Let $G_V \in M_{\ell\times k_V}(\mathbb{F}_{2^s})$ be a generator matrix of $V$.
- For each coordinate $t \in [k_V]$, an *outer* binary Goppa code $C^{(t)} \subseteq \mathbb{F}_{2^s}^{m}$ of length $m$ and Hamming distance $d^{(t)}$, with error-correction radius $t^{(t)} = \lfloor (d^{(t)} - 1)/2 \rfloor$. Let $H^{(t)}$ be a parity-check for $C^{(t)}$.

The inner code handles the row structure under a chain NRT metric, while each outer code processes columns independently under the Hamming metric.

**Definition 10.1** (Inner–outer concatenation)**.** Let $u^{(t)} \in \mathbb{F}_{2^s}^{m}$ denote the outer codeword in $C^{(t)}$ for coordinate $t$, and form the $k_V \times m$ matrix

$$U = \begin{bmatrix} (u^{(1)}) \\ \vdots \\ (u^{(k_V)}) \end{bmatrix}.$$

Define the concatenated code

$$\mathcal{C}_{\text{NRT-GC}} = \{A = G_V\, U \ \in \ M_{\ell\times m}(\mathbb{F}_{2^s})\}.$$

Thus for every column index $j$,

$$a_{*,j} = G_V \left(u_j^{(1)}, \ldots, u_j^{(k_V)}\right)^\top \in V \subseteq \mathbb{F}_{2^s}^\ell. \tag{6}$$

Equivalently, each column of $A$ is an inner-codeword obtained by applying the inner map to the tuple of outer symbols at that column.

We measure $A \in M_{\ell \times m}(\mathbb{F}_{2^s})$ in the block-NRT metric: each nonzero column contributes the position of its last nonzero entry (plus 1), so the distance is the sum of the single-chain NRT weights of the columns.

**Theorem 10.2** (Minimum block-NRT distance)**.** *For $\mathcal{C}_{\text{NRT-GC}}$ as in Definition 10.1,*

$$d_{\text{NRT}}\big(\mathcal{C}_{\text{NRT-GC}}\big) \;\geq\; \delta_V \cdot \min_{t \in [k_V]} d^{(t)}.$$

*Proof.* Take any nonzero $A \in \mathcal{C}_{\text{NRT-GC}}$. At least one outer sequence $u^{(t)}$ is nonzero and therefore has Hamming weight at least $d^{(t)}$. For each column $j$ with $u_j^{(t)} \neq 0$, the column $a_{*,j}$ is given by (6). By definition of the inner NRT distance, any nonzero output of $G_V$ has single-chain NRT weight at least $\delta_V$. Thus each such column contributes at least $\delta_V$ to the block-NRT weight, yielding $w_{\text{bNRT}}(A) \geq \delta_V \, d^{(t)}$. Minimizing over $t$ completes the proof. □

**Remark 10.3.** If $V$ is an NRT-MDS code (achievable via an upper-triangular $G_V$) with $\delta_V = \ell - k_V + 1$, and if all outers are identical $C^{(t)} = C$ with distance $d$, then

$$d_{\text{bNRT}}\big(\mathcal{C}_{\text{NRT-GC}}\big) \geq (\ell - k_V + 1)\, d.$$

For $k_V = 1$ and a generator vector whose last nonzero row is $\ell - 1$, one obtains the simple bound $d_{\text{bNRT}} \geq \ell \cdot d$ with a trivial inner map. This yields a genuine multiplicative distance gain compared to plain Hamming-metric Goppa codes.

## 10.2 Parity-check structure and obfuscation

A systematic parity-check for $\mathcal{C}_{\text{NRT-GC}}$ is obtained by *lifting* the outer checks through the inner map. Let $G_V = [\, b_1 \; \cdots \; b_{k_V} \,]$ with $b_t \in \mathbb{F}_{2^s}^\ell$. Define

$$H_{\text{sys}} = \begin{bmatrix} H^{(1)} \otimes b_1^\top \\ H^{(2)} \otimes b_2^\top \\ \vdots \\ H^{(k_V)} \otimes b_{k_V}^\top \end{bmatrix} \in M_{r \times (\ell m)}(\mathbb{F}_{2^s}), \qquad r = \sum_{t=1}^{k_V} \operatorname{rank}(H^{(t)}).$$

Here $\otimes$ denotes the Kronecker product, so each parity-check row of $C^{(t)}$ is replicated across the $\ell$ rows according to the inner basis vector $b_t$. This mirrors classical concatenated-code constructions (e.g., [13]) in an NRT-aware setting.

**Public key obfuscation.** For our Niederreiter-style cryptosystems, we publish the obfuscated matrix

$$M = S\, H_{\mathrm{sys}}\, (PD),$$

where $S \in GL_r(\mathbb{F}_{2^s})$ is dense, $P$ is a column permutation, and $D$ is a nonsingular diagonal matrix. We restrict $(PD)$ to the monomial subgroup $(B_\ell(\mathbb{F}_{2^s}))^m \rtimes \mathcal{S}_m$, which preserves the block-NRT weight and destroys visible Kronecker or low-weight patterns. More general $GL_n(\mathbb{F}_{2^s})$ right actions are not metric-preserving and are therefore avoided.

This obfuscation preserves the decoding radius, hides the block and Kronecker structure, and makes $M$ appear statistically dense. Left-mixing by $S$ destroys row locality; $P$ removes column grouping; and $D$ destroys unit entry patterns. Empirically, $M$ is indistinguishable from a random full-rank matrix under known structural tests, while retaining efficient secret decoding.

## 10.3 Decoding

Decoding naturally decomposes into an outer Hamming stage and an inner single-chain NRT stage:

1. **Outer Goppa decoding across columns.** Compute $(S^{-1}, (PD)^{-1})$ privately to recover row-blocks corresponding to $H^{(t)} \otimes b_t^\top$. For each $t$, extract the syndrome sequence in $\mathbb{F}_{2^s}^m$ and apply the Patterson Goppa decoder to obtain $\widehat{u}^{(t)}$ provided the error budget per coordinate is $\le t^{(t)}$.

2. **Inner columnwise NRT map.** For each column $j$, collect the tuple $\widehat{u}_j = (\widehat{u}_j^{(1)}, \ldots, \widehat{u}_j^{(k_V)})$ and reconstruct $a_{*,j} = G_V\, \widehat{u}_j$. If the public error model uses canonical NRT column errors (one nonzero at the last nonzero row), this step is algebraic; otherwise run a short NRT decoder on $V$ of length $\ell$.

Both outer and inner stages are parallelizable across Goppa coordinates and columns, respectively.

## 10.4 Comparison with plain Hamming–Goppa constructions

A single Goppa code $C \subseteq \mathbb{F}_{2^s}^m$ under the Hamming metric has $d_{\mathrm{Ham}}(C) = d$. Viewed as a matrix code with one nonzero row, its block-NRT minimum distance remains $d$. In contrast, our inner–outer scheme satisfies

$$d_{\mathrm{bNRT}}\big(\mathcal{C}_{\text{NRT-GC}}\big) \;\ge\; \delta_V \cdot d_{\min}, \qquad d_{\min} = \min_t d^{(t)},$$

multiplying the guaranteed NRT distance by $\delta_V \ge 2$. Thus for fixed outer parameters, the NRT-aware concatenation strictly improves the block-NRT distance compared to the plain Goppa construction.

Furthermore, the public matrix $M = SH_{\mathrm{sys}}PD$ inherits Niederreiter-style syndrome-decodin hardness at chosen parameters, while the inner structure is masked by the left/right scramblers. Visible Kronecker or low-weight structure is removed by $S$, $P$, and $D$. Recovering canonical forms under the block-NRT isometry group remains computationally hard, consistent with the hardness arguments in Section 9. The inner coupling does not weaken the obfuscation.

In conclusion, our codes have the following advantages:

- *Higher block-NRT distance at similar outer parameters:* choosing $V$ with $\delta_V = \ell - k_V + 1$ gives a multiplicative factor $\approx \ell/k_V$.
- *Modular decoding:* outer Goppa decoders are classical; the inner step is short ($\ell$ symbols) and admits constant-time implementations.
- *Parallelism:* outer decoders run independently in $t$ and across columns; inner decoding is column-parallel.
- *Metric alignment:* the design is native to the block-NRT metric and adapts naturally to the sum-rank metric by bundling columns.

### 10.5 Wiretap channels and a block-NRT specialization

Connections between ordered/NRT metrics and wiretap coding already appear in Barg and Park [2]. In the sum-rank setting, the support-theoretic framework and generalized weights are developed in [21]. The point of this subsection is therefore more specific. We record a block-prefix parity-check formulation in the notation of Proposition 4.1, which fits naturally with the metric-aware viewpoint of the present paper.

Let $n = m\ell$ and let

$$H = \left[\, H^{(1)} \mid \cdots \mid H^{(m)} \,\right] \in M_{r\times n}(\mathbb{F}_q)$$

be a full-rank matrix with $H^{(b)} \in M_{r\times \ell}(\mathbb{F}_q)$, and set

$$C := \ker(H) \subseteq \mathbb{F}_q^n.$$

For a profile $u = (u_1, \ldots, u_m) \in \{0, 1, \ldots, \ell\}^m$, define the prefix observation map

$$\pi_u : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{|u|_1}, \qquad \pi_u(x) = \big((x_1^{(1)}, \ldots, x_{u_1}^{(1)}), \ldots, (x_1^{(m)}, \ldots, x_{u_m}^{(m)})\big),$$

and define the complementary block-suffix matrix

$$H_{(u,\ell]} := \left[\, H^{(1)}_{(u_1,\ell]} \mid \cdots \mid H^{(m)}_{(u_m,\ell]} \,\right] \in M_{r\times(n-|u|_1)}(\mathbb{F}_q),$$

where $H^{(b)}_{(u_b,\ell]}$ denotes the last $\ell - u_b$ columns of $H^{(b)}$.

We consider the usual syndrome/coset encoder: a secret $S \in \mathbb{F}_q^r$ is encoded by choosing $X$ uniformly from the affine space

$$\{\, x \in \mathbb{F}_q^n : \; Hx^\top = S \,\}.$$

Equivalently, one may choose $X$ uniformly in $\mathbb{F}_q^n$ and then set

$$S = HX^\top.$$

In this form, $S$ is uniform on $\mathbb{F}_q^r$, and conditioned on $S = s$, the vector $X$ is uniform on the coset $\{x \in \mathbb{F}_q^n : \; Hx^\top = s\}$.

**Proposition 10.4.** *Fix $u \in \{0, \ldots, \ell\}^m$ and $z \in \mathbb{F}_q^{|u|_1}$. Let*

$$\Sigma_u(z) := \{\, Hx^\top : \; x \in \mathbb{F}_q^n, \; \pi_u(x) = z \,\} \subseteq \mathbb{F}_q^r.$$

*Then $\Sigma_u(z)$ is an affine subspace of $\mathbb{F}_q^r$ whose translation space is* $\mathrm{colspan}(H_{(u,\ell]})$*. In particular,*

$$|\Sigma_u(z)| = q^{\mathrm{rank}(H_{(u,\ell]})}.$$

*Moreover, conditioned on $\pi_u(X) = z$, the secret $S$ is uniformly distributed on $\Sigma_u(z)$.*

*Proof.* Fix $u$ and $z$. Let $x(z) \in \mathbb{F}_q^n$ be the vector whose first $u_b$ coordinates in block $b$ are the prescribed entries of $z$ and whose remaining coordinates are zero. Every vector $x \in \mathbb{F}_q^n$ satisfying $\pi_u(x) = z$ can be written uniquely as

$$x = x(z) + y,$$

where, in block $b$, the first $u_b$ coordinates of $y^{(b)}$ are zero. If $y' \in \mathbb{F}_q^{n-|u|_1}$ collects the free suffix coordinates of $y$, then

$$Hx^\top = Hx(z)^\top + H_{(u,\ell]}(y')^\top.$$

Therefore

$$\Sigma_u(z) = Hx(z)^\top + \mathrm{colspan}(H_{(u,\ell]}),$$

which is an affine subspace with translation space $\mathrm{colspan}(H_{(u,\ell]})$. Its cardinality is therefore $q^{\mathrm{rank}(H_{(u,\ell]})}$.

Now choose $X$ uniformly in $\mathbb{F}_q^n$ and set $S = HX^\top$. Conditioned on $\pi_u(X) = z$, the suffix coordinates of $X$ remain uniform in $\mathbb{F}_q^{n-|u|_1}$. Hence $H_{(u,\ell]}(y')^\top$ is uniformly distributed on $\mathrm{colspan}(H_{(u,\ell]})$, and thus $S$ is uniformly distributed on the affine subspace $\Sigma_u(z)$. □

**Corollary 10.5.** *Let $\mu \geq 0$. The above encoder is perfectly secret against every eavesdropper that observes a block-prefix profile $u$ with $|u|_1 \leq \mu$ if and only if*

$$\mathrm{rank}(H_{(u,\ell]}) = r \qquad \text{for all } u \in \{0, \dots, \ell\}^m \text{ with } |u|_1 \leq \mu.$$

*Proof.* By Proposition 10.4, for a fixed profile $u$ and a fixed observation $z$, the set of compatible secrets is the affine subspace $\Sigma_u(z)$ of cardinality $q^{\mathrm{rank}(H_{(u,\ell]})}$. Thus every secret remains possible, and indeed equally likely, after the observation $\pi_u(X)$ if and only if $\Sigma_u(z) = \mathbb{F}_q^r$ for every $z$, which is equivalent to $\mathrm{rank}(H_{(u,\ell]}) = r$. □

**Theorem 10.6.** *Let $C = \ker(H)$. For $\mu \geq 0$, the following are equivalent:*

1. *The encoder is perfectly secret against every block-prefix observation of total size at most $\mu$.*
2. *For every profile $u \in \{0, \dots, \ell\}^m$ with $|u|_1 \leq \mu$, one has*

$$\mathrm{rank}(H_{(u,\ell]}) = r.$$

3.

$$d_{\mathrm{bNRT}}(C^\perp) > \mu.$$

*In particular, the largest block-prefix observation budget guaranteeing perfect secrecy is*

$$\mu_{\max} = d_{\mathrm{bNRT}}(C^\perp) - 1.$$

*Proof.* The equivalence of (1) and (2) is Corollary 10.5. We prove that (2) and (3) are equivalent.

Assume first that (2) fails. Then there exists a profile $u$ with $|u|_1 \leq \mu$ such that

$$\operatorname{rank}(H_{(u,\ell]}) < r.$$

Hence there exists a nonzero row vector $a \in \mathbb{F}_q^r$ such that

$$aH_{(u,\ell]} = 0.$$

Set

$$y := aH \in \mathbb{F}_q^n.$$

Then $y \in C^\perp$, $y \neq 0$, and all coordinates of $y$ outside the first $u_b$ positions of block $b$ vanish. Therefore

$$w_{\mathrm{bNRT}}(y) \leq |u|_1 \leq \mu,$$

so $d_{\mathrm{bNRT}}(C^\perp) \leq \mu$. Hence (3) fails.

Conversely, assume that (3) fails. Then there exists $0 \neq y \in C^\perp$ with

$$w_{\mathrm{bNRT}}(y) \leq \mu.$$

Since $C^\perp$ is the row space of $H$, we may write

$$y = aH$$

for some nonzero row vector $a \in \mathbb{F}_q^r$. For each block $b$, let $u_b := w_{\mathrm{NRT}}(y^{(b)})$. Then

$$|u|_1 = w_{\mathrm{bNRT}}(y) \leq \mu,$$

and by definition of the NRT weight, the coordinates of $y$ in block $b$ beyond position $u_b$ are all zero. This means precisely that

$$aH_{(u,\ell]} = 0.$$

Therefore the rows of $H_{(u,\ell]}$ are linearly dependent, and so

$$\operatorname{rank}(H_{(u,\ell]}) < r.$$

Thus (2) fails. This proves the equivalence of (2) and (3). □

**Remark 10.7.** The ordered-wiretap connection itself is already present in [2]. The point of Theorem 10.6 is to express the secrecy threshold directly in the block-prefix notation that underlies Proposition 4.1. In this sense, the subsection is a specialization to the language of the present paper rather than a first application of ordered metrics to wiretap coding.

Likewise, in the sum-rank setting, support spaces and generalized weights are already developed in [21]. For that reason, we do not state a parallel sum-rank wiretap theorem here, although the same philosophy suggests a packetized eavesdropper model governed by rank profiles.

## Acknowledgement

This work was supported in part by the Provost's Proof of Concept (PPOC) Grant from the Tulane Innovation Institute.

## References


[1] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David A. Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. Status report on the fourth round of the nist post-quantum cryptography standardization process. NIST Interagency/Internal Report (IR) 8545, National Institute of Standards and Technology, March 2025.

[2] Alexander Barg and Woomyoung Park. On linear ordered codes. *Mosc. Math. J.*, 15(4):679–702, 2015.

[3] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[4] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Attacking and defending the McEliece cryptosystem. In *Post-Quantum Cryptography – PQCrypto 2008*, volume 5299 of *LNCS*, pages 31–46. Springer, 2008.

[5] Richard A. Brualdi, Janine Smolin Graves, and K. Mark Lawrence. Codes with a poset metric. *Discrete Math.*, 147(1-3):57–72, 1995.

[6] Mahir Bilen Can and Lex E. Renner. $H$-polynomials and rook polynomials. *Internat. J. Algebra Comput.*, 18(5):935–949, 2008.

[7] Mahir Bilen Can and Lex E. Renner. Bruhat-Chevalley order on the rook monoid. *Turkish J. Math.*, 36(4):499–519, 2012.

[8] Classic McEliece Team. Classic McEliece: Implementation (implementors' guide and parameters). Project website, 2025. Version 2025.01.01. Accessed 2025-10-24.

[9] Alain Couvreur, Philippe Gaborit, Ayoub Otmani, Jean-Pierre Tillich, and Virginie Zémor. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. In *ASIACRYPT 2014*, volume 8874 of *LNCS*, pages 92–111. Springer, 2014.

[10] I. I. Dumer. Two algorithms for the decoding of linear codes. *Problemy Peredachi Informatsii*, 25(1):24–32, 1989.

[11] Jean-Charles Faugére, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 279–298. Springer, 2010.

[12] Marcelo Firer, Marcelo Muniz S. Alves, Jerry Anderson Pinheiro, and Luciano Panek. *Poset codes: partial orders, metrics and coding theory.* SpringerBriefs in Mathematics. Springer, Cham, 2018.

[13] G. D. Forney. *Concatenated Codes.* MIT Press, 1966.

[14] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *CRYPTO 1999*, volume 1666 of *LNCS*, pages 537–554. Springer, 1999.

[15] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, San Francisco, 1979.

[16] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[17] Jong Yoon Hyun and Hyun Kwang Kim. Maximum distance separable poset codes. *Des. Codes Cryptogr.*, 48(3):247–261, 2008.

[18] Simon Josefsson. Classic McEliece goes to IETF and OpenSSH. Blog post, December 2023. Accessed 2025-10-24.

[19] Richard M. Karp. Reducibility among combinatorial problems. In Raymond E. Miller and James W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, New York, 1972.

[20] F. Jessie MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*, volume 16 of *North-Holland Mathematical Library*. North-Holland Publishing Company, Amsterdam, 1977.

[21] Umberto Martínez-Peñas. Theory of supports for linear codes endowed with the sum-rank metric. *Des. Codes Cryptogr.*, 87(10):2295–2320, 2019.

[22] John Preuß Mattsson, Erik Thormarker, Göran Selander, Santeri Paavolainen, Sini Ruohomaa, Juha Sääskilahti, Taylor Hartley, Helena Vahidi Mazinani, and Mohsin Kahn. ML-KEM is Great! What's missing? Presentation, NIST CSRC, 2025. Accessed 2025-10-24.

[23] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $O(2^{0.054n})$. In *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[24] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In *EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[25] Robert J. McEliece. *The Theory of Information and Coding: A Mathematical Framework for Communication*, volume 3 of *Encyclopedia of Mathematics and its Applications*. Addison–Wesley, Reading, MA, 1977. Reprinted by Cambridge University Press, 2002.

[26] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 42-44:114–116, 1978.

[27] National Institute of Standards and Technology. Nist pqc standardization process: Hqc announced as a 4th round selection. News article, March 2025. Accessed 2025-10-24.

[28] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 15(2):159–166, 1986.

[29] Harald Niederreiter. Point sets and sequences with small discrepancy. *Monatsh. Math.*, 104(4):273–337, 1987.

[30] Harald Niederreiter. A combinatorial problem for vector spaces over finite fields. *Discrete Math.*, 96(3):221–228, 1991.

[31] NIST. Post-quantum cryptography standardization, 2024. Accessed: 2025-09-09.

[32] Open Quantum Safe Project. SSH (OQS-OpenSSH): Post-Quantum and Hybrid Key Exchange Prototypes. Project page, 2025. Accessed 2025-10-24.

[33] Luciano Panek, Marcelo Firer, and Marcelo Muniz Silva Alves. Symmetry groups of Rosenbloom-Tsfasman spaces. *Discrete Math.*, 309(4):763–771, 2009.

[34] N. Patterson. The algebraic decoding of goppa codes. *IEEE Trans. Inf. Theory*, pages 468–472, 1975.

[35] E. Prange. The use of information sets in decoding cyclic codes. In *IRE Trans. Inform. Theory*, volume 8, pages 5–9, 1962.

[36] Mohan S. Putcha. *Linear algebraic monoids*, volume 133 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1988.

[37] Lex E. Renner. Analogue of the Bruhat decomposition for algebraic monoids. *J. Algebra*, 101(2):303–338, 1986.

[38] Lex E. Renner. *Linear algebraic monoids*, volume 134 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, V.

[39] M. Yu. Rozenblyum and M. A. Tsfasman. Codes for the $m$-metric. *Problemy Peredachi Informatsii*, 33(1):55–63, 1997.

[40] Louis Solomon. The Bruhat decomposition, Tits system and Iwahori ring for the monoid of matrices over a finite field. *Geom. Dedicata*, 36(1):15–49, 1990.

[41] Jacques Stern. A method for finding codewords of small weight. In *Coding theory and applications (Toulon, 1988)*, volume 388 of *Lecture Notes in Comput. Sci.*, pages 106–113. Springer, New York, 1989.