

# Faster Sparse Matrix Inversion and Rank Computation in Finite Fields

Sílvia Casacuberta ✉

Harvard University, Cambridge, MA, USA

Rasmus Kyng ✉

ETH Zürich, Switzerland

---

## Abstract

We improve the current best running time value to invert sparse matrices over finite fields, lowering it to an expected  $O(n^{2.2131})$  time for the current values of fast rectangular matrix multiplication. We achieve the same running time for the computation of the rank and nullspace of a sparse matrix over a finite field. This improvement relies on two key techniques. First, we adopt the decomposition of an arbitrary matrix into block Krylov and Hankel matrices from Eberly et al. (ISSAC 2007). Second, we show how to recover the explicit inverse of a block Hankel matrix using low displacement rank techniques for structured matrices and fast rectangular matrix multiplication algorithms. We generalize our inversion method to block structured matrices with other displacement operators and strengthen the best known upper bounds for explicit inversion of block Toeplitz-like and block Hankel-like matrices, as well as for explicit inversion of block Vandermonde-like matrices with structured blocks. As a further application, we improve the complexity of several algorithms in topological data analysis and in finite group theory.

**2012 ACM Subject Classification** Theory of computation → Design and analysis of algorithms

**Keywords and phrases** Matrix inversion, rank computation, displacement operators, numerical linear algebra

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2022.33

**Related Version** *Full Version*: <https://arxiv.org/abs/2106.09830>

**Funding** *Sílvia Casacuberta*: This work was partly done while S. Casacuberta was at ETH Zurich, funded by the startup grant of Prof. Kyng.

**Acknowledgements** We are thankful to Richard Peng and Markus Püschel for helpful suggestions and comments.

## 1 Introduction

The problem of solving a linear system  $Ax = b$  efficiently is a fundamental question in linear algebra, central to both scientific applications and complexity results. Algorithms for linear system solving are generally divided into direct and iterative methods. The term *direct method* refers to solving  $Ax = b$  by applying an (implicit) representation of  $A^{-1}$  to  $b$  using a decomposition that is exact up to numerical error. Examples include Gaussian Elimination, Cholesky Factorization, and QR decomposition. In contrast, iterative methods successively converge to the solution [50]. The most basic algorithm among direct methods is Gaussian Elimination, while in the iterative case Conjugate Gradient is most commonly used [25]. A key consideration when developing algorithms for linear systems is the underlying field, as methods for solvers in finite fields, rationals, and reals all differ substantially.

Any algorithm that directly computes  $A^{-1}$  leads to a solver for linear equations in  $A$ . Strassen was the first to show that matrix inversion is equivalent to matrix multiplication in any ring via a divide-and-conquer approach [53]. In the RealRAM model, this implies that given a matrix  $A \in \mathbb{R}^{n \times n}$  and a vector  $b \in \mathbb{R}^n$ , the linear system  $Ax = b$  is solvable



© Sílvia Casacuberta and Rasmus Kyng;

licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 33; pp. 33:1–33:24

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

in time  $O(n^\omega)$ , where  $\omega$  denotes the exponent of matrix multiplication. The constant  $\omega$  has a current best bound of  $\omega < 2.37286$  [1], which culminates an extensive line of work on fast matrix multiplication based on the analysis of the Coppersmith–Winograd tensor [9, 11, 18, 46, 54, 56]. Besides square matrix multiplication, rectangular matrix multiplication is central to many problems in algorithm design [18], such as the all-pairs shortest paths problem [60] and linear program solvers [8]. On the other hand, iterative algorithms via the Conjugate Gradient or the Lanczos algorithm yield a running time of  $O(n \cdot \text{nnz}(A))$  for solving  $Ax = b$  in RealRAM [25, 39], where  $\text{nnz}(A)$  denotes the number of non-zeroes in the matrix  $A$ .

However, running times in the RealRAM model can be misleading. For example, in finite precision arithmetic, even Gaussian Elimination is not stable by default, as first shown by Wilkinson [58]. Ill-conditioned systems can yield very wrong solutions due to the round-off errors that may arise. But, when restricted to matrices with polynomial condition number, a running time of  $O(n^{\omega+o(1)})$  can be achieved with guaranteed numerical stability in finite precision arithmetic [12]. Conjugate Gradient is also not stable in finite precision arithmetic – as observed in folklore and formally shown in [41]. If we instead work with finite fields, round-off error is no longer a concern, preventing instability. This provides a simpler setting for developing fast linear algebra algorithms, which in turn can shed light into the rational and real cases.

The first iterative algorithms for the finite field setting were adaptations of previously-known existing methods over the reals, such as the finite field version of the Conjugate Gradient and Lanczos algorithms proposed in [38]. In this case, the motivation for working in finite fields emerged in the area of cryptography; more concretely, in the problems of factoring and the discrete logarithm, which require solving large sparse linear systems over the field  $GF(2)$ . Nonetheless, this sparked interest for developing iterative algorithms for linear systems directly for finite fields, instead of adapting them from the real setting. A prominent example is Wiedemann’s algorithm [57], which yields a probabilistic method for solving linear systems in  $O(n \cdot \text{nnz}(A))$  field operations with only a  $O(\text{nnz}(A))$  space requirement. Wiedemann’s algorithm is based on the observation that, when applying a square matrix repeatedly to a vector, the resulting sequence of vectors is linear recursive. His method then relates the generating polynomial of this sequence with the minimal polynomial of the matrix, which can be computed efficiently over finite fields with the Berlekamp–Massey algorithm [29], among others.

In some contexts, we want to compute  $A^{-1}$  instead of merely solving a linear equation  $Ax = b$ . This may occur, for example, if we need to solve many linear equations in  $A$ . Frequently, algorithms for computing  $A^{-1}$  also suggest methods for determining the rank of  $A$  (as  $A^{-1}$  exists if and only if the matrix has full row and column rank).

In the finite field setting there is a complexity gap between the running time for linear system solving and that of inverse computation of sparse matrices. Linear systems can be solved in  $O(n \cdot \text{nnz}(A))$  time using for example Wiedemann’s algorithm [57]. There are also sub-matrix-multiplication-time algorithms for computing the inverse of a sparse matrix [14, 15], but these are somewhat slower: With  $\text{nnz}(A) = \tilde{O}(n)$ , the running time is  $\tilde{O}(n^{2.28})$ . Until recently, there was no such complexity gap in the real finite precision arithmetic setting, where both running times were  $O(n^\omega)$  [53]. However, [49] showed that sparse linear system solving under real finite precision arithmetic can be done faster than matrix-multiplication time, achieving  $O(n^{2.331645})$  running time for an  $n \times n$  matrix  $A$  with  $\text{nnz}(A) = \tilde{O}(n)$ . This value was recently improved to  $O(n^{2.27159})$  [42].

Over rationals, linear systems can be solved exactly using finite precision, making it possible to solve ill-conditioned problems in this setting. However, the bit complexity of the rational solutions is high, which makes it difficult to obtain fast algorithms. In particular, if one works with high bit complexity representations of intermediate calculations, this leads to slow implementations of direct methods such as Gaussian Elimination. Somewhat surprisingly, many of these issues can be resolved by relying on  $p$ -adic arithmetic for the intermediate calculations, as shown in a pioneering work by [13]. The key idea is to bridge the numerical stability of finite fields with the rationals by means of  $p$ -adic integers and a “rational reconstruction” algorithm, so that one can rely on the finite field numerical stability, and yet recover a rational solution. Elements of the ring of  $p$ -adic integers, denoted  $\mathbb{Z}_p$  for a prime  $p$ , are infinite series of powers of  $p$ . Assuming a bound  $d = O(1)$  for the bitlength of entries in  $A$ , Dixon showed that  $O(n \log n)$   $p$ -adic digits suffice for recovering the exact rational solution via the rational reconstruction algorithm, where each  $p$ -adic digit can be seen as an element of the finite field  $\mathbb{Z}/p\mathbb{Z}$ . For example, by using Dixon’s  $p$ -adic approach, one can merge Wiedemann’s algorithm with rational reconstruction to obtain an exact rational solution of an integer linear system [33]. While Dixon’s algorithm has a running time of  $O(n^3)$  for linear system solving over the rationals (which is that of Gaussian Elimination, except that in Dixon’s algorithm the solution is guaranteed to be exact), Storjohann achieved a running time of  $\tilde{O}(n^\omega)$  by leveraging rational reconstruction with a divide-and-conquer method for the  $p$ -adic expansion [52].

Concurrently, [14, 15] also improved Dixon’s algorithm to achieve a running time of  $\tilde{O}(n^{2.5})$  for sparse linear system solving over the rationals, and of  $\tilde{O}(n^{2.28})$  for sparse matrix inversion over finite fields. In their case, their running time improvement relies on efficient matrix projections and block Krylov methods. Their main ideas on block Krylov methods and structured matrices were recently adapted to the finite precision arithmetic setting to achieve the first sub-matrix-multiplication algorithm for sparse linear systems [49]. In this case, we encounter the reverse situation to the first adaptations of the Conjugate Gradient and Lanczos algorithms to the finite precision real setting, and it is the adaptation of a finite field algorithm to the reals what has achieved a significant running time improvement. This motivates the detailed study of the matrix inversion problem in the finite field setting, given that no sub-matrix-multiplication algorithm for it is known in finite precision real arithmetic.

In this paper, we study the problem of matrix inversion and rank computation of an  $n \times n$  matrix  $A$  over a finite field, focusing on sparse matrices and certain other classes of structured matrices. In the process, we also study the problems of computing the nullspace when  $A$  is singular and the Schur complement of a non-singular principal minor.

We obtain an expected final running time for all four problems of

$$\hat{O}(mn \phi(n) + s^\omega m + n^{\omega_s} + mn^2)$$

field operations, where  $\phi(n)$  denotes the time required to apply  $A$  to a vector,  $s$  is the blocking factor dividing  $n$  and  $m$  is its complement (so that  $sm = n$ , where both  $s$  and  $m$  are parameters of the algorithm),  $\omega$  is the exponent of matrix multiplication [1], and  $\omega_s$  is the corresponding exponent for multiplication of an  $n \times s$  matrix by an  $s \times n$  one. We are using the abbreviation  $\omega_s = \omega(\log_n s)$  where  $\omega(k)$  is the exponent for multiplication of an  $n \times n^k$  matrix by an  $n^k \times n$  one, as introduced in the context of fast rectangular matrix multiplication in [19]. The notation  $\hat{O}(\cdot)$  hides factors  $O(n^{o(1)})$ .

In the case where the matrix  $A$  is sparse or, more generally, whenever  $\phi(n) = \hat{O}(n)$ , the above running time becomes  $\hat{O}(n^{\omega(k)})$ , where  $k = \log_n s$  is the only value satisfying  $\omega(k) = 3 - k$ . This corresponds to an expected  $O(n^{2.2131})$  running time using the current

best known bound on  $\omega(k)$ . Our method relies on the construction of [15] for factoring an arbitrary matrix into block Krylov and block Hankel matrices. We modify their algorithm by inverting the block Hankel matrix explicitly, as opposed to working with its implicit formula. To do so, we employ displacement rank methods combined with fast rectangular matrix multiplication algorithms.

## 1.1 Related Work

Our construction is closely related to the one presented in [15]. They improve Dixon’s algorithm for the exact solution of linear systems over the rationals, lowering the running time from  $\tilde{O}(n^3)$  to  $\tilde{O}(n^{2.5})$ . Each of the  $O(n \log n)$  iterations of Dixon’s algorithm requires the application of  $A^{-1} \bmod p$  to a vector. Thus, Dixon’s running time relies on both inverting the matrix  $A$  quickly in  $\mathbb{Z}/p\mathbb{Z}$  and then being able to apply it efficiently to a vector. The improvements by Eberly et al. [15] rely on two central constructions. First, they introduced efficient block projections which allow for the use of Krylov-type methods without a too high exponentiation of  $A$ . Scalar block Krylov methods for linear system solving were already in use in the seminal paper of Wiedemann in 1986 for sparse linear systems in finite fields based on the Berlekamp–Massey algorithm [57]. Still, the  $p$ -adic version of Wiedemann’s algorithm by Kaltofen and Saunders [33] does not improve Dixon’s running time, because one needs to apply powers of  $A$  up until  $A^n$  to a vector at each iteration. This motivates the introduction of blocks to Wiedemann’s algorithm, which limits the required powers of  $A$  to  $A^m$ , where  $m = n/s$  is the number of blocks. The block version of Wiedemann’s algorithm was first proposed by Coppersmith [10] through a block generalization of the Berlekamp–Massey algorithm. Shortly after, Kaltofen [32] proposed using block Toeplitz systems (which can be solved quickly) instead of the block Berlekamp–Massey algorithm in Coppersmith’s algorithm. Eberly et al. introduced efficient block projections  $u$  and  $v$  in this setting, which enables them to construct  $uA^i v$  much faster than in the case of the random block projections in Coppersmith or Kaltofen. The second key ingredient of the Eberly et al. algorithm is the observation that the Gram matrix of the Krylov space matrix is a block Hankel matrix. This leads to a very effective decomposition of  $A^{-1} \bmod p$  into two Krylov space matrices and the inverse of a block Hankel matrix, which is highly structured. The Krylov space matrices are computed efficiently because the input matrix  $A$  is assumed to be sparse, i.e., it has only  $\tilde{O}(n)$  non-zero entries. Thus, it allows for efficient matrix-vector products: computing  $A \rightarrow Ab$  only requires  $\tilde{O}(n)$  operations.

While a Hankel matrix appears to lose all of its structure when inverted, Kailath et al. [31] showed how to circumvent this loss. They introduced the notion of *displacement rank*, which consists of applying an invertible linear operator to the Hankel matrix so that its inverse can be expressed as the sum of only two  $LU$  products. Bitmead and Anderson [3] used this fact along with FFT convolutions to compute the solution of Toeplitz/Hankel systems in sub-quadratic time. Their algorithm can be extended to the block case by viewing the block matrices as  $m \times m$  matrices whose entries are in turn  $s \times s$  matrices such that each operation on an  $s$ -by- $s$  block takes  $\hat{O}(s^\omega)$  time. In parallel to the displacement rank methods, Labahn et al. [37] presented a set of formulae for the inverse of a block Hankel or block Toeplitz matrix, which are expressed in terms of certain matrix Padé forms. This is the algorithm that is used by Eberly et al. to invert a block Hankel matrix. However, this approach allows for less generality than the displacement rank method. Beyond structured matrices such as Toeplitz/Hankel and sparse ones, several fast algorithms and hardness results have been developed when considering structured linear systems more broadly, such as those for graph-structured linear systems (e.g., graph Laplacians) [34, 35, 51]. Laplacian systems have also been recently studied in the finite field setting [27].

## 1.2 Our Results and Contributions

In this paper, we improve the current fastest algorithms for sparse matrix inversion, as well as for rank and nullspace computation, over finite fields. In particular, we study the structure of the low displacement rank generators that correspond to the inverse of a block Hankel matrix. Instead of using the Beckermann–Labahn formula as done in [15], we turn to the low displacement rank algorithms for block Toeplitz/Hankel matrices, and observe that the block Hankel inverse can be recovered explicitly from the product of its rectangular generators, which in turn can be done efficiently with the current fast rectangular matrix multiplication algorithms. This yields a final running time for inverting a non-singular  $n \times n$  matrix  $A$  over a finite field of  $\hat{O}(mn\phi(n) + s^\omega m + n^{\omega_s} + mn^2)$ . By using the current best bound on  $\omega_s = \omega(\log_n s)$  as given by [19] and by optimizing for the block sizes, we obtain an expected final running time of  $O(n^{2.2131})$  in the case of sparse matrices (Theorem 4). More precisely, the running time of our algorithm is equal to  $\hat{O}(n^{\omega(k)})$ , where  $k$  is the only value satisfying the equation  $\omega(k) = 3 - k$ . Moreover, we obtain the same running time for the computation of the rank and nullspace of sparse matrices over finite fields (Theorem 21), as well as for computing the Schur complement of a non-singular principal minor (Lemma 20).

Our algorithm for inverting explicitly a block Hankel matrix (Theorem 2), which is the building block of our improved running time for sparse matrix inversion in finite fields, extends more generally to other structured matrices. Our construction extends to more general matrix classes where a displacement rank operator exists, and is thus applicable to block Toeplitz-like or Hankel-like matrices (Theorems 11 and 13); i.e., matrices with similar structure with respect to the Toeplitz or Hankel displacement operator, respectively. Our technique is also applicable to other types of displacement operators, such as for block Vandermonde matrices (Theorems 18). The use of fast rectangular matrix multiplication combined with rectangular low displacement generators thus provides a new faster scheme for structured block-matrix inversion, which yields the best current upper bound. We state sufficient conditions that the displacement operator must satisfy in order that our scheme be applicable (Section 3.4).

## 1.3 Applications

Our results have numerous applications, given that computing the inverse or the rank of a sparse matrix over a finite field is a central problem in linear algebra. We include two applications in topology and algebra. First, we reduce the complexity of Las Vegas type output-sensitive algorithms as in [7] for the computation of persistence diagrams in topological data analysis (Theorems 24 and 25). For this, we rely on the fact that matrices of boundary operators are sparse. Second, motivated by [20], we provide an improved running time for testing whether an element is a unit in a group ring of a finite metacyclic group  $G$ , and if so, computing the  $G$ -orbit of its inverse (Theorem 26). This is feasible because right-translation matrices in group rings of metacyclic groups are block Toeplitz.

## 2 Inversion of Matrices in Finite Fields

In this section we present the procedure outlined in Algorithm 1. Section 3 contains the theoretical framework needed for Algorithm 2, which is more general than the former. However, their running times are equivalent and specified in Theorem 4.

## 2.1 Preliminaries

Throughout this paper,  $F$  is a finite field,  $\phi(n)$  is the running time required to apply the input  $n \times n$  matrix to a vector, and  $s, m$  refer to the blocking factors of a matrix (with  $n = sm$ ). For the running times,  $\hat{O}(\cdot)$  hides factors  $O(n^{o(1)})$ , where  $n$  is the dimension of the input matrices (which is generally clear from the context), and  $\tilde{O}(\cdot)$  hides logarithmic factors. Moreover,  $\omega < 2.37286$  is the minimum value such that two  $n \times n$  matrices can be multiplied using  $O(n^{\omega+o(1)})$  arithmetic operations [1]. Analogously,  $\omega(k)$  is the minimum value such that the product between an  $n \times n^k$  matrix and an  $n^k \times n$  one can be performed using  $O(n^{\omega(k)+o(1)})$  arithmetic operations [19]. We use the abbreviation  $\omega_s = \omega(\log_n s)$ . Lastly,  $\beta > 0.31389$  is the dual exponent of matrix multiplication (Definition 12), and  $\alpha$  refers to the displacement rank of a matrix with respect to some fixed displacement operator (Definition 7).

## 2.2 Construction

We begin by recalling the structure presented in Eberly et al. [15]. Consider an arbitrary invertible matrix  $A$  of size  $n \times n$  over a finite field  $F$ . We remark that one should first precondition the matrix  $A$  as  $DAD$ , where  $D$  denotes the diagonal matrix of indeterminates as defined in [15, Theorem 2.1], which ensures with high probability the non-singularity of the subsequent Krylov matrices  $K_u, K_v$  defined below. However, for notational simplicity, we will keep denoting the matrix by  $A$ . We also remark that this preconditioning of  $A$  is the only step in the algorithm that causes the final running time to be probabilistic. In particular, all running times given in Section 3 are deterministic.

Let  $s \in \mathbb{Z}$  be the blocking size, and let  $m = n/s$ . Eberly et al. define an efficient block projection in  $F^{n \times s}$  as follows. Let

$$u = [I_s \quad \cdots \quad I_s]^T$$

consist of  $m$  copies of  $I_s$ , the identity matrix of size  $s \times s$ . We then define the following two Krylov matrices:

$$K_u = [u \quad Au \quad A^2u \quad \cdots \quad A^{m-1}u], \quad K_v = \begin{bmatrix} u^T \\ u^T A \\ \vdots \\ u^T A^{m-1} \end{bmatrix},$$

which Eberly et al. show to be non-singular. Both  $K_u$  and  $K_v$  have size  $n \times n$  and  $m$  blocks of size  $n \times s$  and  $s \times n$ , respectively. The computation of  $K_u$  and  $K_v$  requires computing  $A^i u$  and  $u^T A^i$  for  $0 \leq i \leq m-1$ . This requires  $m-1$  applications of  $A$  to  $u$ , for a total of  $O(n\phi(n))$  operations. The key insight of Eberly et al. is that  $H = K_v A K_u$  is a block Hankel matrix:

$$H = \begin{bmatrix} u^T A u & \cdots & u^T A^m u \\ \vdots & \ddots & \vdots \\ u^T A^m u & \cdots & u^T A^{2m-1} u \end{bmatrix} \in F^{n \times n}. \quad (2.1)$$

By the definition of  $u$ , we can compute  $wu$  for any  $w \in F^{s \times n}$  with  $O(sn)$  operations. Hence, computing each  $u^T(A^i u)$  takes  $O(sn)$  operations. Finally, we have  $0 \leq i \leq 2m-1$  such products, and so the total cost for building the block Hankel matrix  $H$  is  $O(n^2)$ , since  $sm = n$ .

### 2.3 Motivation for Running Time Improvement

Since  $H = K_v A K_u$ , computing the inverse  $A^{-1}$  amounts to computing  $K_u H^{-1} K_v$ . There are two ways of proceeding, which rely on the question of whether to keep the block Hankel inverse implicit (with, for example, the off-diagonal formula of Beckermann and Labahn [2]; see Theorem 1), or to make it explicit before multiplying it with the Krylov matrices.

After obtaining an efficient representation of  $H^{-1}$ , Eberly et al. show that  $H^{-1}M$  can be computed for an arbitrary  $M \in F^{n \times n}$  in time  $\hat{O}(s^\omega m^2)$ . This is the convenient set-up for solving a linear system in a Dixon-like scheme, since we need to be able to apply a vector efficiently to  $H^{-1}$  at each iteration. We propose a different scheme for inverting  $A^{-1}$ . The Eberly et al. construction does not take advantage of the Krylov structure of  $K_u$  when computing  $H^{-1}K_u$ , and instead treats  $K_u$  as an arbitrary matrix. However, multiplying an arbitrary matrix with  $K_u$  or  $K_v$  takes only  $O(mn^2)$ . Thus, we propose the following alternative construction:

1. After inverting  $H^{-1}$  efficiently and obtaining an implicit formula for the inverse, we recover  $H^{-1}$  *explicitly* with fast rectangular matrix multiplication.
2. Next we treat  $H^{-1}$  as an arbitrary matrix and compute  $H^{-1}K_u$  by exploiting the Krylov structure of  $K_u$ . Finally, we compute  $K_v \cdot (H^{-1}K_u)$  by using the Krylov structure of  $K_v$ .

### 2.4 Inverting a Block Hankel Matrix Explicitly

First, we need to compute the inverse of the block Hankel matrix  $H^{-1}$ . There are several efficient algorithms to invert (block) Toeplitz/Hankel matrices, which generally fall into two categories: either they use the low displacement structure as introduced by Kailath et al. [31] or they build on the inverse formulae of Gohberg–Semencul [24] and Trench [55]. In this section we focus on the second kind, since it is the method followed by Eberly et al. However, we will then argue that the displacement rank method is much more general and applicable in other settings, so in Section 3 we will turn to the low displacement rank methods. Building on the Gohberg–Semencul, Heining, and Krupnik formulae [22, 23, 24], Labahn et al. [37] generalized their methods to block Hankel matrices and presented a new set of formulae for the inverse of block Hankel/Toeplitz matrices which only requires their non-singularity. They did so by representing  $H^{-1}$  with matrix Padé forms, as shown in [36].

► **Theorem 1** ([37, Theorem 3.1]). *Given a block Hankel matrix  $H$  with blocks of size  $s \times s$  and  $m$  blocks in each row/column (where  $sm = n$ ), the inverse  $H^{-1}$  can be expressed as*

$$H^{-1} = \begin{bmatrix} v_{m-1} & \cdots & v_1 & v_0 \\ \vdots & \ddots & \ddots & \vdots \\ v_1 & \ddots & & \\ v_0 & & & \end{bmatrix} \cdot \begin{bmatrix} q_{m-1}^* & \cdots & q_0^* \\ & \ddots & \vdots \\ & & q_{m-1}^* \end{bmatrix} - \begin{bmatrix} q_{m-2} & \cdots & q_0 & 0 \\ \vdots & \ddots & \ddots & \\ q_0 & \ddots & & \\ 0 & & & \end{bmatrix} \cdot \begin{bmatrix} v_m^* & \cdots & v_1^* \\ & \ddots & \vdots \\ & & v_m^* \end{bmatrix},$$

where  $v_i, v_i^*, q_i$  and  $q_i^*$  are  $s \times s$  matrices.

Let us denote the four matrices in Theorem 1 as  $H^{-1} = VQ^* - QV^*$ , where  $V$  and  $Q$  are anti-triangular block Hankel matrices and  $V^*$  and  $Q^*$  are triangular block Toeplitz matrices. As noted by Eberly et al., by using the fast algorithms for Padé formulations from [21], the matrices  $V, Q, V^*, Q^*$ , and thus the implicit representation of  $H^{-1}$  in Theorem 1 (which is also known as the *off-diagonal inverse formula*), can be computed with  $\hat{O}(s^\omega m)$  operations in  $F$ . The question is then: what is the most efficient way to recover  $H^{-1}$  *explicitly* from its implicit representation above?

By using fast algorithms for matrix polynomials [6], we can compute the product  $H^{-1}M$  for an arbitrary  $M \in F^{n \times n}$  in time  $\hat{O}(s^\omega m^2)$ . Thus, by setting  $M = I_n$ , or just by treating  $Q^*$  and  $V^*$  as arbitrary matrices, we can recover  $H^{-1}$  explicitly in  $\hat{O}(s^\omega m^2)$ . We would like to do better, given that  $Q^*$  and  $V^*$  have a very particular structure. To obtain a better upper bound for the explicit recovery of a block Hankel inverse matrix, we will instead use fast rectangular matrix multiplication. Given that  $V, Q, V^*, Q^*$  are (anti-) triangular block Hankel and Toeplitz matrices, we can associate rectangular matrices of sizes  $n \times s$  and  $s \times n$  to them, which consist of the  $m$  non-repeated blocks. In other words, we define

$$\bar{V} = \begin{bmatrix} v_{m-1} \\ \vdots \\ v_1 \\ v_0 \end{bmatrix}, \quad \bar{Q} = \begin{bmatrix} q_{m-2} \\ \vdots \\ q_0 \\ 0 \end{bmatrix} \in F^{n \times s}, \quad \begin{aligned} \bar{Q}^* &= [q_{m-1}^* \ \cdots \ q_0^*], \\ \bar{V}^* &= [v_m^* \ \cdots \ v_1^*] \in F^{s \times n} \end{aligned} \quad (2.2)$$

from  $V, Q^*, Q, V^*$ . Our key insight is that to compute  $VQ^*$  we can instead perform the rectangular product  $\bar{V}\bar{Q}^*$  and then recover  $VQ^*$  from  $\bar{V}\bar{Q}^*$  in  $O(n^2)$  time by adding through each anti-diagonal. This is due to the following correspondence between  $VQ^*$  and  $\bar{V}\bar{Q}^*$ :

$$[VQ^*]_{i,j} = \sum_{1 \leq k \leq \min\{j, m-i+1\}} [\bar{V}\bar{Q}^*]_{i+k-1, j-k+1} \quad (2.3)$$

where  $[VQ^*]_{i,j}$  denotes the  $s \times s$  block of  $VQ^*$  located at row  $i$  and column  $j$ . To put it more visually, after performing the rectangular product  $\bar{V}\bar{Q}^*$ , we obtain the  $n \times n$  matrix

$$\bar{V}\bar{Q}^* = \begin{bmatrix} v_{m-1}q_{m-1}^* & v_{m-1}q_{m-2}^* & \cdots & v_{m-1}q_0^* \\ v_{m-2}q_{m-1}^* & v_{m-2}q_{m-2}^* & \cdots & v_{m-2}q_0^* \\ \vdots & \vdots & \ddots & \vdots \\ v_0q_{m-1}^* & v_0q_{m-2}^* & \cdots & v_0q_0^* \end{bmatrix}.$$

We can then build  $VQ^*$  from  $\bar{V}\bar{Q}^*$  by adding through each anti-diagonal one block at a time, for a total of  $O(n^2)$ , since

$$VQ^* = \begin{bmatrix} v_{m-1}q_{m-1}^* & v_{m-1}q_{m-2}^* + v_{m-2}q_{m-1}^* & \cdots & \sum_{k=1}^m v_{m-k}q_{k-1}^* \\ v_{m-2}q_{m-1}^* & v_{m-2}q_{m-2}^* + v_{m-3}q_{m-1}^* & \cdots & \sum_{k=2}^m v_{m-k}q_{k-2}^* \\ v_{m-3}q_{m-1}^* & v_{m-3}q_{m-2}^* + v_{m-4}q_{m-1}^* & \cdots & \sum_{k=3}^m v_{m-k}q_{k-3}^* \\ \vdots & \vdots & \ddots & \vdots \\ v_0q_{m-1}^* & v_0q_{m-2}^* & \cdots & v_0q_0^* \end{bmatrix}.$$

We thus obtain the following cost:

► **Theorem 2.** For a block Hankel matrix  $H \in F^{n \times n}$  with blocking size  $s = n/m$ , computing  $H^{-1}$  explicitly requires  $\hat{O}(n^{\omega_s})$  field operations, which corresponds to the running time required to multiply an  $n \times s$  matrix with an  $s \times n$  matrix.

**Proof.** Computing the product  $\bar{V}\bar{Q}^*$  costs  $n^{\omega_s}$ . Then, we recover  $VQ^*$  from  $\bar{V}\bar{Q}^*$  using Equation (2.3). This recovery only needs reading through the entries of  $\bar{V}\bar{Q}^*$ , which costs  $O(n^2)$ . The same reasoning applies to the product  $QV^*$ . ◀



Once  $H^{-1}$  has been made explicit, we need to multiply it on both sides by the Krylov matrices  $K_u$  and  $K_v$  to obtain  $A^{-1}$ :

$$A^{-1} = K_u H^{-1} K_v.$$

Not only can we multiply  $K_v$  efficiently with an arbitrary matrix  $M$  from the right ( $K_v M$ ), as shown by Eberly et al., but we can also do it from the left ( $M K_v$ ). Hence, after obtaining  $H^{-1}$  explicitly, we perform the product  $H^{-1} K_v$  as follows, by effectively treating  $H^{-1}$  as an arbitrary matrix  $M$  now that it has been made explicit. Split  $H^{-1}$  into  $m$  blocks of  $s$  consecutive columns  $H_i^{-1}$ , for  $0 \leq i \leq m-1$ . Using Horner's scheme to apply  $K_u$  to each block and summing the results, we then obtain

$$\begin{aligned} H^{-1} K_u &= \sum_{i=0}^{m-1} H_0^{-1} u^T A^i \\ &= (\cdots (H_{m-1}^{-1} u^T A + H_{m-2}^{-1} u^T) A + H_{m-3}^{-1} u^T) A + \cdots + H_1^{-1} u^T) A + H_0^{-1} u^T. \end{aligned} \quad (2.4)$$

By the special structure of  $u^T$ , we can compute each  $H_i^{-1} u^T$  in  $O(n^2)$ , yielding a total of  $O(mn^2)$ . Then we multiply each  $H_i^{-1} u^T$  by  $A$ , and since there are a total of  $m$  such products, the final running time of computing  $M K_u$  is again  $O(mn \phi(n) + mn^2)$ .

Finally, we perform the product  $K_v \cdot (H^{-1} K_u)$  by now treating  $H^{-1} K_u$  as an arbitrary matrix. We obtain the same running time as for  $H^{-1} K_u$  by performing a similar construction. Split  $H^{-1} K_u$  into  $m$  blocks of  $s$  consecutive rows  $(H^{-1} K_u)_i$ , for  $0 \leq i \leq m-1$ . Thus,

$$\begin{aligned} K_v \cdot (H^{-1} K_u) &= \sum_{i=0}^{m-1} A^i u (H^{-1} K_u)_i \\ &= u (H^{-1} K_u)_0 + A[u (H^{-1} K_u)_1 + A[u (H^{-1} K_u)_2 + \cdots + A u (H^{-1} K_u)_{m-1}] \cdots]. \end{aligned} \quad (2.5)$$

By the same argument as before, the final running time for this product is  $O(mn \phi(n) + mn^2)$ .

■ **Algorithm 1** Inverting an arbitrary matrix over a finite field with the off-diagonal formula.

- 
- 1: **procedure** MATRIXINV1( $A$ ) ▷ Theorem 4
  - 2:   Fix  $s$  and  $m$  blocking factors such that  $n = sm$ . ▷ Values  $s, m \leftarrow n^{0.7869}, n^{0.2131}$
  - 3:   ▷ are optimal at the current rectangular matrix multiplication time.
  - 4:    $u \leftarrow [I_s \cdots I_s]^T$
  - 5:    $K_v \leftarrow [u \ A^T u \ (A^2)^T u \ \cdots \ (A^{m-1})^T u]^T$
  - 6:    $H \leftarrow K_v A K_u$  is block Hankel. ▷ Equation (2.1), [15]
  - 7:    $H^{-1} \leftarrow V Q^* - Q V^*$  ▷ Theorem 1, [37]
  - 8:    $\overline{V}, \overline{Q^*}, \overline{Q}, \overline{V^*} \leftarrow$  as defined in Equation (2.2)
  - 9:   Perform the two rectangular products  $\overline{V} \overline{Q^*}$  and  $\overline{Q} \overline{V^*}$ . ▷ Fast algorithm by [19]
  - 10:   Recover  $V Q^*$  and  $Q V^*$  recursively. ▷ Equation (2.3)
  - 11:   Compute  $A^{-1} \leftarrow K_u H^{-1} K_v$ . ▷ Equations (2.4), (2.5)
  - 12:   **return**  $A^{-1}$ .
  - 13: **end procedure**
- 

The total cost for building  $A^{-1}$  is then  $\hat{O}(mn \phi(n) + s^\omega m + n^{\omega_s} + mn^2)$ . In the sparse case where  $\phi(n) = \hat{O}(n)$ , this cost becomes  $\hat{O}(s^\omega m + n^{\omega_s} + mn^2)$ .

■ **Algorithm 2** Inverting an arbitrary matrix over a finite field with displacement rank operators.

---

```

1: procedure MATRIXINV2( $A$ ) ▷ Theorem 4
2:   Fix  $s$  and  $m$  blocking factors such that  $n = sm$ . ▷ Values  $s, m \leftarrow n^{0.7869}, n^{0.2131}$ 
3:   ▷ are optimal at the current rectangular matrix multiplication time.
4:    $u \leftarrow [I_s \cdots I_s]^T$ 
5:    $K_v \leftarrow [u \ A^T u \ (A^2)^T u \ \cdots \ (A^{m-1})^T u]^T$ 
6:    $H \leftarrow K_v A K_u$  is block Hankel. ▷ Equation (2.1), [15]
7:   Compute  $X_i, Y_i$  so that  $\Delta_{Z_0^T, Z_0}(H^{-1}) = \sum_{i=1}^{\alpha} X_i Y_i^T$ . ▷ Def. 7, [3] (Thm. 9)
8:   Perform the  $\alpha$  rectangular products  $X_i Y_i^T$ . ▷ Fast algorithm by [19]
9:   Recover  $H^{-1}$  recursively. ▷ Equation (3.4)
10:  Compute  $A^{-1} \leftarrow K_u H^{-1} K_v$ . ▷ Equations (2.4), (2.5)
11:  return  $A^{-1}$ .
12: end procedure
    
```

---

For the proof of Theorem 4 below, we need to quote the following fact:

► **Lemma 3** ([26, Eq. 2.6]). *Multiplying an  $n \times s$  matrix by an  $s \times n$  matrix can be done with the same number of arithmetic operations as multiplying an  $s \times n$  matrix by an  $n \times n$  matrix.*

► **Theorem 4.** *For a non-singular matrix  $A \in F^{n \times n}$  where  $F$  is a finite field, the inverse  $A^{-1}$  can be computed in expected time*

$$\hat{O}(mn\phi(n) + s^\omega m + n^{\omega_s} + mn^2),$$

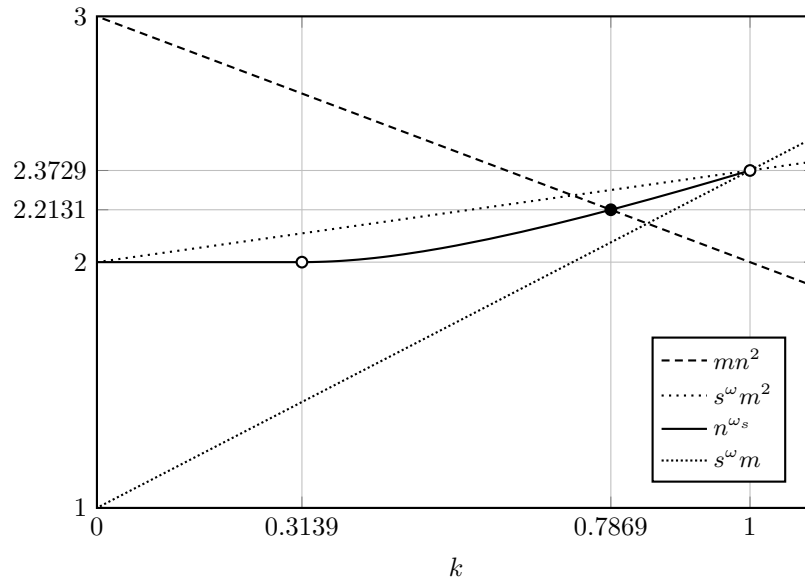
where  $sm = n$ , by calling the procedure  $\text{MATRIXINV}(A)$  (this applies to both versions 1 and 2; see Algorithm 1 and Algorithm 2). If  $\phi(n) = \hat{O}(n)$ , e.g., if  $A$  is sparse, then the inverse  $A^{-1}$  can be computed in expected time  $\hat{O}(n^{\omega(k)})$ , where  $k = \log_n s$  is the only value that satisfies  $\omega(k) = 3 - k$ . With the current values of rectangular matrix multiplication, this corresponds to  $O(n^{2.2131})$  arithmetic operations.

**Proof.** We first note that  $s^\omega m \leq n^{\omega_s} \leq s^\omega m^2$ . The second inequality follows from the definition of  $\omega_s$ , since multiplying an  $n \times s$  matrix by an  $s \times n$  one can be done with  $m^2$  multiplications of  $s \times s$  matrices. Since it is possible to multiply two  $n \times n$  matrices by multiplying  $m$  times an  $s \times n$  matrix by an  $n \times n$  matrix by Lemma 3, we conclude that  $mn^{\omega_s} \geq n^\omega$ . Consequently,

$$n^{\omega_s} \geq m^{-1} n^\omega = m^{-1} s^\omega m^\omega = s^\omega m^{\omega-1} \geq s^\omega m,$$

which yields the first inequality.

Since  $s^\omega m \leq n^{\omega_s}$ , we need to pick optimal blocking factors  $s$  and  $m$  with  $sm = n$  such that  $\max\{n^{\omega_s}, mn^2\}$  is minimized. Note that  $mn^2 = (ns^{-1})n^2 = n^{3-\log_n s}$  is a decreasing function of  $s$  while  $n^{\omega_s}$  is an increasing function of  $s$  depicted in Figure 1 in [19] and in Figure 1 below. Hence the optimal value of  $s$  is achieved at the crossing point between the graphs of  $n^{\omega_s}$  and  $mn^2$ , which occurs at the only value of  $k = \log_n s$  that satisfies  $\omega(k) = 3 - k$ . Using the data given in Table 3 of [19], we find by interpolation the solution  $k = 0.7869$ , corresponding to  $s = n^{0.78668}$  and  $\omega_s = \omega(0.78668) = 2.21312$ . This yields a running time bound for inverting a sparse  $n \times n$  matrix over a finite field of  $O(n^{2.2131})$ . ◀



■ **Figure 1** Graphic visualization of the minimization process that yields our running time. As functions of  $k = \log_n s$ , we have  $n^{\omega_s} = n^{\omega(k)}$ ,  $mn^2 = n^{3-k}$ ,  $s^\omega m = n^{1+(\omega-1)k}$ , and  $s^\omega m^2 = n^{2+(\omega-2)k}$ . The curves plot the respective exponents for comparison. The value 0.3139 corresponds to the current best bound on the dual exponent of matrix multiplication [19].

### 3 Generalization to Structured Matrices

The idea of using rectangular matrix multiplication on the low rank generators of a structured matrix extends to more general settings. Since the off-diagonal inverse formula from the previous section relates only to Hankel matrices, we switch to low displacement rank methods for matrix inversion. First, these are simpler algorithms than the Padé-based ones, and they extend more naturally to the block setting. Second, they allow us to obtain running times not only for Toeplitz and Hankel matrices, but for Toeplitz-like and Hankel-like matrices, as well as other types of structured matrices.

The notion of low displacement rank was first introduced by Kailath et al. [31], and referred only to Toeplitz matrices:

► **Definition 5** ([31]). *The (+)-displacement rank of a matrix  $M$  is the smallest integer  $\alpha_+(M)$  such that we can write*

$$M = \sum_{i=1}^{\alpha_+(M)} L_i U_i$$

for some lower-triangular Toeplitz matrices  $\{L_i\}$  and upper-triangular Toeplitz matrices  $\{U_i\}$ .

The (−)-displacement rank is defined similarly, by replacing  $L_i U_i$  with  $U_i L_i$ . The key theorem in displacement rank methods states the following:

► **Theorem 6** ([31, Theorem 1]). *The ( $\pm$ )-displacement rank of a matrix is equal to the ( $\mp$ )-displacement rank of its inverse, i.e., for all non-singular matrices  $M$ ,*

$$\alpha_+(M) = \alpha_-(M^{-1}) \quad \text{and} \quad \alpha_-(M) = \alpha_+(M^{-1}).$$

Soon after, it became evident that the notion of displacement rank can be applied to other types of structured matrices beyond Toeplitz. Following the notation of [5], we can then refer to the notion of displacement rank in greater generality, which extends Definition 5 to other kinds of operators.

► **Definition 7.** Given a matrix  $A \in F^{n \times n}$ , let  $\Delta_{P,Q}$  denote the displacement operator of  $A$ , for  $P, Q \in F^{n \times n}$ , which takes the form

$$\Delta_{P,Q}(A) = A - PAQ.$$

Two matrices  $X, Y \in F^{n \times \alpha}$  are called generators of length  $\alpha$  for  $A$  if  $\Delta_{P,Q}(A) = XY^T$ . In the block case, generators are rectangular matrices of size  $n \times \alpha$ s. For any matrix  $A$  and its associated operator  $\Delta_{P,Q}$ , the value  $\alpha = \text{rank}(\Delta_{P,Q}(A))$  is called the displacement rank of  $A$ .

In this context, we are always interested in the case where  $\alpha$  is small relative to  $n$ , i.e., when  $\alpha = o(n)$ , and then we say that the matrix  $A$  is  $\Delta_{P,Q}$ -like, or that it has a structure of type  $\Delta_{P,Q}$ . This is what we mean throughout this section by *Toeplitz-like* or *Hankel-like* matrices. Thus, this notion extends well-beyond the definitions in [31] for Toeplitz matrices, not only because we allow other types of structured matrices, but also because  $\alpha$  can be any constant other than 2. Remarkably, the proof given in [31] for Theorem 6 does not depend on the definition of the operator, and only requires some general rank properties to hold. In contrast, the off-diagonal formula of Beckermann and Labahn does not allow for such generalizations. Moreover, the displacement rank algorithms are more readily generalizable to the block setting, which we require.

Closely related to the rectangular matrices in the off-diagonal formula of Beckermann and Labahn in the previous section, these generators are also compact data structures representing  $A$ . When  $A$  has low displacement rank with respect to  $\Delta_{P,Q}$ , we can represent  $\Delta_{P,Q}(A)$  with two matrices that have size only  $n \times \alpha$ , hence using a total space of  $2n\alpha$  instead of  $n^2$ . We always choose  $P$  and  $Q$  such that  $\Delta_{P,Q}$  is an invertible linear operator. Hence we can also recover  $A$  from the compact representation of  $\Delta_{P,Q}(A)$ .

For  $f \in \mathbb{Z}$ , define the circulant matrix:

$$Z_f = \begin{bmatrix} 0 & & & f \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}. \quad (3.1)$$

Then, in the case of a Toeplitz matrix  $T$ , the generators  $P, Q$  correspond to  $P = Z_0$  and  $Q = Z_0^T$ . In the case of a Hankel matrix, the matrices  $P, Q$  correspond to  $P = Z_0^T$  and  $Q = Z_0$ . It is clear that Toeplitz matrices  $T$  and Hankel matrices  $H$  have displacement rank 2, but the key insight is that now both  $\Delta_{P,Q}(T^{-1})$  and  $\Delta_{P,Q}(H^{-1})$  have rank 2 as well. Displacement operators thus yield compressed bilinear expressions for structured matrices.

### 3.1 Explicit Inversion of Low Displacement Rank Matrices

The notion of displacement rank extends naturally to blocked matrices. We first consider the case of explicitly inverting a block Toeplitz/Hankel-like matrix, using the notation in [49]. Throughout this section we will use the notation for Toeplitz-like matrices (including Algorithm 3), and then show how the analogous results follow for Hankel-like matrices. The following theorem applies when using the Toeplitz operator with  $P = Z_0$ ,  $Q = Z_0^T$ . Let  $A \in F^{n \times n}$  be a block matrix with block size  $s \times s$  and  $m \times m$  blocks.

► **Theorem 8** ([3, 31]). *Given generators  $X_i, Y_i$  of size  $n \times s$  and displacement rank  $\alpha$ , the equation  $A - Z_0 A Z_0^T = \sum_{i=1}^{\alpha} X_i Y_i^T$  has the unique solution  $A = \sum_{i=1}^{\alpha} L(X_i) U(Y_i)$ , where  $L(X_i)$  is a lower-triangular Toeplitz matrix whose first column is  $X_i$ , and  $U(Y_i) = L(Y_i)^T$ .*

Here we use the following correspondence between rectangular matrices  $W \in F^{n \times s}$  and  $n \times n$  lower (or upper) Toeplitz triangular matrices:

$$W = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_m \end{bmatrix} \in F^{n \times s}, \quad L(W) = \begin{bmatrix} w_1 & 0 & 0 & \dots & 0 \\ w_2 & w_1 & 0 & \dots & 0 \\ w_3 & w_2 & w_1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ w_m & w_{m-1} & w_{m-2} & \dots & w_1 \end{bmatrix} \in F^{n \times n}, \quad U(W) = L(W)^T.$$

The functional equation  $A - Z_0 A Z_0^T = \sum_{i=1}^{\alpha} X_i Y_i^T$  is coherent with the definition of the generators  $X$  and  $Y$  of length  $\alpha$  from the previous section. We can either express  $\Delta_{Z_0, Z_0^T}(A)$  as  $XY^T$ , where  $X$  and  $Y$  have size  $n \times \alpha s$ , or we can express  $\Delta_{Z_0, Z_0^T}(A)$  as  $\sum_{i=1}^{\alpha} X_i Y_i^T$ , where each  $X_i$  or  $Y_i$  has size  $n \times s$ .

The algorithm presented in Bitmead and Anderson [3] uses Theorem 6 applied to the inverse  $A^{-1}$ :

► **Theorem 9** ([3, Theorem 2]). *Given a blocked input matrix  $A$  with blocking size  $s = n/m$ , the rectangular generators  $X_i, Y_i$  of  $\Delta_{Z_0, Z_0^T}(A^{-1})$  can be found in time  $\hat{O}(\alpha s^{\omega} m \log^2 m)$ .*

► **Remark 10.** While the [3] algorithm refers specifically to Toeplitz matrices, it is easily extendable to Hankel matrices with the same runtime, as formally discussed in [47, 48].

Their scheme is very efficient to then apply a vector to  $A^{-1}$ , since the rectangular blocked structure of  $X_i$  and  $Y_i$  allows for the use of FFT to perform convolutions between the vector and the blocks of  $X_i$  and  $Y_i$ . However, in some applications, as shown in Sections 2 and 4 in this paper, it is convenient to be able to retrieve the block Toeplitz matrix explicitly from its rectangular generators, such as in the case of sparse matrix inversion. In this case, none of the methods for structured matrix inversion have addressed the upper bound for *explicit* inversion, and the running times are always given assuming that the representation of the structured matrices remains implicit. There is no extensive analysis for the decompression stage; i.e., when we want to recover  $A^{-1}$  from the rectangular generators of  $\Delta_{P, Q}(A^{-1})$ . In this setting, the only known way to recover  $A^{-1}$  explicitly is to apply the  $n/s = m$  canonical block vectors. This requires  $m$  convolutions with  $A^{-1}$ , which yields a total running time of  $\hat{O}(s^{\omega} m^2 \log^2 m)$ . Rather, we can apply our scheme to recover

$$A^{-1} = \sum_{i=1}^{\alpha} L(X_i) U(Y_i) \tag{3.2}$$

explicitly, where  $\alpha$  is the displacement rank. We apply a similar approach to what we did in Section 2 for the Beckermann–Labahn formula. Note that the off-diagonal formula for  $H^{-1}$  of Section 2 is a special case of displacement in the Hankel case, with  $P = Z_0^T$  and  $Q = Z_0$ .

We first multiply the rectangular matrices  $X_i, Y_i \in F^{n \times s}$  to obtain  $X_i Y_i^T$  in time  $\hat{O}(n^{\omega s})$ . Using fast rectangular matrix multiplication methods, this can be done better than in time  $\hat{O}(s^{\omega} m^2)$ . To then recover  $L(X_i) U(Y_i)$  from  $X_i Y_i^T$ , we can just read along each diagonal (thus performing only  $O(m^2)$  sums of  $s \times s$  matrices), since

$$[L(X_i) U(Y_i)]_{j,k} = \sum_{1 \leq \ell \leq \min\{j,k\}} [X_i Y_i^T]_{j+1-\ell, k+1-\ell}. \tag{3.3}$$

Because we need to repeat this procedure  $\alpha$  times, we obtain the following running time.

► **Theorem 11.** *Given a blocked matrix  $A \in F^{n \times n}$  with displacement rank  $\alpha$  with respect to the Toeplitz/Hankel operator and blocking size  $s = n/m$ , the inverse  $A^{-1}$  can be recovered explicitly from its low rank representation in time*

$$\hat{O}(\alpha(n^{\omega_s} + n^2)) = \hat{O}(\alpha n^{\omega_s}).$$

Hence,  $A^{-1}$  can be computed explicitly by calling the procedure `BLOCKSTRUCTINV`( $A, s, m$ ) (see Algorithm 3) in total time  $\hat{O}(\alpha s^{\omega} m \log m + \alpha n^{\omega_s}) = \hat{O}(\alpha n^{\omega_s})$ .

In particular, the running time given in Theorem 11 is an improvement over  $\hat{O}(s^{\omega} m^2)$  for all structured matrices with respect to the Toeplitz/Hankel displacement operator, i.e., for those matrices such that  $\alpha = o(n)$  with  $\alpha = \text{rank}(\Delta_{Z_0, Z_0^T}(A))$  or  $\alpha = \text{rank}(\Delta_{Z_0^T, Z_0}(A))$ . In the case of the Hankel operator, Equation (3.2) becomes

$$A^{-1} = \sum_{i=1}^{\alpha} G(X_i)U(Y_i), \quad (3.4)$$

where  $G(\cdot)$  is the block Hankel matrix defined as

$$G(W) = \begin{bmatrix} w_1 & \dots & w_{n-2} & w_{n-1} & w_n \\ w_2 & \dots & w_{n-1} & w_n & 0 \\ w_3 & \dots & w_n & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ w_n & \dots & 0 & 0 & 0 \end{bmatrix}, \quad (3.5)$$

and Equation (3.3) instead becomes the recovery formula

$$[G(X_i)U(Y_i)]_{j,k} = \sum_{1 \leq \ell \leq \min\{k, m-j+1\}} [X_i Y_i^T]_{j+\ell-1, k-\ell+1}. \quad (3.6)$$

## 3.2 Upper Bound for Inversion of Block Toeplitz/Hankel-Like Matrices

We begin by recalling the definition of the dual exponent:

► **Definition 12** ([19]). *The dual exponent of matrix multiplication, denoted by  $\beta$ , is defined as the quantity  $\beta = \sup\{k \mid \omega(k) = 2\}$ .*

In other words,  $\beta$  is defined as the asymptotically maximum number  $b \leq 1$  such that multiplying an  $n \times n^b$  matrix by an  $n^b \times n$  matrix can be done in  $n^{2+o(1)}$  time. In the particular case when  $A$  is a blocked Toeplitz/Hankel-like matrix, we obtain the following:

► **Theorem 13.** *Given a blocked Toeplitz/Hankel-like matrix in  $F^{n \times n}$  with blocking size  $s = n/m$  and displacement rank  $\alpha = n^{o(1)}$ , its explicit inverse can be obtained in time  $\hat{O}(s^{\omega} m + n^{\omega_s} + n^2) = \hat{O}(n^{\omega_s})$ . For  $s < n^{\beta}$  where  $\beta$  is the dual exponent, this running time becomes  $O(n^{2+o(1)})$ .*

**Proof.** Computing the implicit inverse given by Theorem 9 requires  $\hat{O}(s^{\omega} m)$  operations. Multiplying the rectangular generators requires  $\hat{O}(n^{\omega_s})$  operations, and finally recovering the inverse from their product requires  $O(n^2)$  operations. ◀

► **Remark 14.** The current best lower bound for  $\beta$  was obtained in [19], and is  $\beta \geq 0.31389$ . Thus our algorithm achieves exactly  $\hat{O}(n^2)$  for inverting Toeplitz/Hankel-like matrices with blocking size  $s$  smaller than  $n^{0.31389}$ .

Note that  $n^{\omega_s}$  as given by [19] is strictly smaller than  $s^{\omega}m^2$  for values of  $s < n$  (see Figure 1 and the proof of Theorem 4). Thus, this improves on the best upper bound for the explicit inversion of block Toeplitz/Hankel matrices, which was  $\hat{O}(s^{\omega}m^2)$ . This running time can be obtained by applying FFT  $m$  times to the low displacement rank representation, essentially treating each column of the matrix as a separate vector. This is also the running time that Eberly et al. obtain for multiplying  $H^{-1}M$  with an arbitrary matrix  $M$ . However, their procedure noted no difference between performing the product  $H^{-1}M$  or the product  $L(X_i)U(Y_i)$ , which occurs between matrices that are both very structured (triangular and Toeplitz/Hankel).

■ **Algorithm 3** Inverting a block Toeplitz/Hankel-like matrix.

---

```

1: procedure BLOCKSTRUCTINV( $A, s, m$ )
2:   For the Toeplitz operator,  $P = Z_0, Q = Z_0^T$ .
3:   For the Hankel operator,  $P = Z_0^T, Q = Z_0$ . ▷ Theorem 11
4:    $\Delta_{P,Q} \leftarrow$  displacement operators associated to  $A$ . ▷ Definition 7
5:   Let  $X_i, Y_i$  be rectangular generators such that  $\Delta_{P,Q}(A^{-1}) = \sum_{i=1}^{\alpha} X_i Y_i^T$ .
6:   Compute  $X_i, Y_i \in F^{n \times s}$ . ▷ [3] algorithm (Thm. 9)
7:   Perform the  $\alpha$  rectangular products  $X_i Y_i^T$ . ▷ Fast algorithm by [19]
8:   In block Toeplitz-like case,
9:     return  $A^{-1} = \sum_{i=1}^{\alpha} L(X_i)U(Y_i)$ . ▷ Using Equation (3.3)
10:  In block Hankel-like case,
11:    return  $A^{-1} = \sum_{i=1}^{\alpha} G(X_i)U(Y_i)$ . ▷ Using Equation (3.4)
12: end procedure

```

---

### 3.3 Other Displacement Operators

The idea of recovering the explicit inverse directly from the rectangular product  $XY^T$ , where  $X, Y \in F^{n \times \alpha s}$  are rectangular generators such that  $\Delta_{P,Q}(A^{-1}) = XY^T$ , extends to other kinds of matrices beyond Toeplitz/Hankel-like that also have low rank generators. This is also one of the improvements of our method over that of [15], since the algorithm that they use to invert the block Hankel matrix (namely the off-diagonal formula of Beckermann and Labahn) works strictly only for Hankel matrices, and does not generalize to other types of structured matrices. While most papers on subquadratic algorithms for structured linear system solvers have focused on the Toeplitz/Hankel case, a variety of operators exist for other types of structured matrices [48]. Well-known cases of such matrices are Vandermonde and Cauchy.

**Vandermonde matrices.** In this case, besides the circulant matrix  $Z_0$ , we use the following notation for diagonal and Vandermonde matrices:

$$D(U) = \begin{bmatrix} u_1 & & & & \\ & u_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & u_n \end{bmatrix}, \quad V(U) = \begin{bmatrix} 1 & u_1 & u_1^2 & \dots & u_1^{n-1} \\ 1 & u_2 & u_2^2 & \dots & u_2^{n-1} \\ 1 & u_3 & u_3^2 & \dots & u_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & u_n & u_n^2 & \dots & u_n^{n-1} \end{bmatrix}. \quad (3.7)$$

### 33:16 Faster Sparse Matrix Inversion and Rank Computation in Finite Fields

The displacement operator for a Vandermonde matrix  $V(U)$  is defined as

$$\Delta_{D(U), Z_0^T}(A) = A - D(U) A Z_0^T,$$

which yields a rank-1 matrix precisely when  $A = V(U)$ . The analogous version of Theorem 8 for Vandermonde-like matrices with displacement rank  $\alpha$  reads as follows:

► **Theorem 15** ([48, §4.4]). *Given scalars  $u_1, \dots, u_n$  and generators  $X, Y \in F^{n \times \alpha}$ , or equivalently given generators  $X_i, Y_i \in F^{n \times 1}$ , where  $1 \leq i \leq \alpha$ , the equation*

$$\Delta_{D(U), Z_0^T}(A) = A - D(U) A Z_0^T = \sum_{i=1}^{\alpha} X_i Y_i^T = XY^T$$

has the unique solution

$$A = \sum_{i=1}^{\alpha} D(X_i) V(U) L(Y_i)^T. \quad (3.8)$$

The analogous version of Theorem 9 is in turn:

► **Theorem 16** ([47]). *Given a blocked input matrix  $A$  with blocking size  $s = n/m$ , the rectangular generators  $X_i, Y_i$  of  $\Delta_{D(U), Z_0^T}(A^{-1})$  can be found in time  $\hat{O}(\alpha s^\omega m \log^2 m)$ .*

A block version of Theorem 15 is obtained by letting the  $u_i$  be  $s \times s$  matrices. In this case,  $X, Y \in F^{n \times \alpha s}$ . If  $s > 1$ , then the recovery formula (3.8) does not hold in general, due to the non-commutativity of the parameter matrices  $u_i$  with the blocks of  $X$ . However, the following decompressing relation for block Vandermonde-like matrices does hold.

► **Lemma 17.** *Given matrices  $u_1, \dots, u_m \in F^{s \times s}$  and generators  $X, Y \in F^{n \times \alpha s}$ , where  $m = n/s$ , or equivalently given generators  $X_i, Y_i \in F^{n \times s}$ , where  $1 \leq i \leq \alpha$ , the equation*

$$\Delta_{D(U), Z_0^T}(A) = A - D(U) A Z_0^T = \sum_{i=1}^{\alpha} X_i Y_i^T = XY^T$$

has the unique solution

$$A_{i,j} = \sum_{k=1}^j u_i^{j-k} [XY^T]_{i,k}. \quad (3.9)$$

**Proof.** The equality  $A - D(U)AZ_0^T = XY^T$  implies that  $A_{i,1} = [XY^T]_{i,1}$  for all  $i$ , and

$$A_{i,j} = [XY^T]_{i,j} + u_i A_{i,j-1} \text{ for } j > 1 \text{ and every } i. \quad (3.10)$$

This proves (3.9) and provides an efficient recursion for computing the entries of  $A$ . The resulting matrix coincides with (3.8) if  $u_1, \dots, u_m$  commute with the components of  $X$ . ◀

► **Theorem 18.** *For a block Vandermonde-like  $n \times n$  matrix  $A$  with displacement rank  $\alpha$ , block size  $s = n/m$  and parameter matrices  $u_1, \dots, u_m$ , the running time required to compute  $A^{-1}$  explicitly is  $\hat{O}(\alpha n^\omega s + \tau m^2)$ , where  $\tau$  is the maximum cost of multiplying one of the matrices  $u_i$  by an arbitrary  $s \times s$  matrix.*

**Proof.** By Theorem 16, we can compute the rectangular generators of  $A^{-1}$  in subquadratic time, and then obtain  $\Delta_{D(U), Z_0^T}(A^{-1})$  with  $\alpha$  rectangular multiplications. Recovering  $A^{-1}$  from  $\Delta_{D(U), Z_0^T}(A^{-1})$  by means of (3.10) requires  $m^2$  sums of  $s \times s$  matrices and  $m^2$  products by the matrices  $u_1, \dots, u_m$ . Thus the recovery step amounts to  $\hat{O}(\tau m^2)$ . ◀



Note that if the matrices  $u_1, \dots, u_m$  are scalar multiples of the identity, or are sparse, or more generally whenever  $\tau < n^{\omega_s}$ , the running time required for inverting such a matrix explicitly is  $\hat{O}(\alpha n^{\omega_s})$ . For any  $\tau < s^w$ , the above yields a running time improvement over [15]. The final algorithm is analogous to the one presented in Algorithm 3.

### 3.4 General Statement

For any block structured matrix with structure matrices  $P, Q$ , we can attempt to find a recursive way to reconstruct  $A^{-1}$  from  $\Delta_{P,Q}(A^{-1})$  in time  $\tilde{O}(\alpha n^2)$  by examining the structure of the unique solution to the corresponding functional equation. If so, then we can recover the explicit inverse in time  $O(\alpha(n^2 + n^{\omega_s}))$  from its low displacement rank generators by employing fast rectangular matrix multiplication. More concretely, given an invertible blocked matrix  $A \in F^{n \times n}$  with blocking size  $s$  associated with a displacement operator  $\Delta_{P,Q}$  such that  $\Delta_{P,Q}(A^{-1}) = A^{-1} - PA^{-1}Q = XY^T$  has rank  $\alpha s$  with  $\alpha = o(n)$ , suppose that the following conditions hold:

1. There exists a fast algorithm for obtaining the rectangular generators  $X, Y \in F^{n \times \alpha s}$  of  $A^{-1}$  from  $A$ .
2. The matrix  $A^{-1}$  can be quickly recovered from  $\Delta_{P,Q}(A^{-1})$ .

Then  $A^{-1}$  can be computed explicitly in the time required for the above two operations plus an additional  $\hat{O}(\alpha n^{\omega_s})$  time, where  $n^{\omega_s}$  is the running time for multiplication of an  $n \times s$  matrix by an  $s \times n$  one. For the types of matrices discussed in this paper, i.e., block Toeplitz, Hankel, and Vandermonde, the operation in Condition 1 can be performed in  $\hat{O}(\alpha s^\omega m)$  time and the operation in Condition 2 can be performed in  $\hat{O}(\alpha n^2)$  time.

In the case of block Toeplitz/Hankel-like matrices, Condition 1 is ensured by the algorithm in [3] (with running time  $\hat{O}(\alpha s^\omega m \log^2 m)$ ; see Theorem 9 and Remark 10), and Condition 2 is given by our construction in Theorem 11. In the case of block Vandermonde-like matrices, Condition 1 is given by the algorithm in [47] (with also running time  $\hat{O}(\alpha s^\omega m \log^2 m)$ ; see Theorem 16), and Condition 2 follows from the recursion (3.10), assuming that the parameter matrices  $u_1, \dots, u_m$  of the displacement operator are simple enough, e.g., sparse. Our heuristic is potentially generalizable to other block structured matrices that have an associated displacement operator, such as Cauchy, Toeplitz+Hankel, Bézout, Sylvester, Frobenius, or Loewner. We remark that for a block Cauchy matrix  $C(U, V) = ((u_i - v_j)^{-1})_{i,j=1}^m$ , which has displacement operator  $\Delta_{D(U), D(V)}(A) = D(U)A - AD(V) = XY^T$ , the block version of the scalar recovery equation  $A = \sum_{i=1}^{\alpha} D(X_i)C(U, V)D(Y_i)$  is  $A_{i,j} = (u_i - v_j)^{-1} [XY^T]_{i,j}$ . However, this block recovery formula requires to impose strong commutativity restrictions on the displacement parameter matrices  $u_i, v_j$ , such as assuming that they are scalar multiples of the identity.

## 4 Rank and Nullspace Computation

As noted in Section 5 of [15], the algorithm we improved in Section 2 for fast sparse matrix inversion can also be used to compute both the rank and the nullspace of a matrix over a finite field  $F$ . Our same running time improvement also holds.

Eberly et al. compute the rank and nullspace with probabilistic algorithms in two steps: first, they apply the algorithm by Kalfoten and Saunders [33] to compute the rank of  $A$  with high probability. This algorithm first preconditions the matrix  $A$  with random upper and lower triangular Toeplitz matrices  $U, L \in F^{n \times n}$  and a random diagonal matrix  $D \in F^{n \times n}$  and set  $\tilde{A} = UALD$ , which allows them to subsequently prove that all the leading  $i \times i$  minors of  $\tilde{A}$  for  $1 \leq i \leq r$  are non-singular, where  $r$  is the rank of  $A$ . The final (deterministic) running time is as follows:

► **Theorem 19** ([33]). *For any matrix  $A \in F^{n \times n}$ , computing the rank of  $A$  with high probability can be done in  $\hat{O}(n^2 + n\phi(n))$  operations in  $F$ .*

A black-box application is a matrix-vector multiplication, which costs  $\hat{O}(n)$  operations for sparse matrices and also for structured matrices. The algorithm requires that the finite field  $F$  has sufficiently many elements, yet this can be arranged by passing to an algebraic extension. However, the [33] algorithm does not certify the output rank, and there is no known method to do so in the running time given in Theorem 19 [15].

The second step is to certify the rank obtained by the algorithm in [33], which otherwise is not guaranteed to be correct. An algorithm for rank certification and nullspace computation is presented in Section 5 of Eberly et al. The algorithm is as follows. We first partition the preconditioned matrix (which we rename as  $A$ ) into four blocks determined by the leading (non-singular)  $r \times r$  minor  $A_0$ :

$$A = \begin{bmatrix} A_0 & A_1 \\ A_2 & A_3 \end{bmatrix}. \quad (4.1)$$

Next, we invert  $A_0$ , and here is where we apply our algorithm for black-box matrix inversion (Theorem 4), which takes  $O(n^{2.2131})$  field operations, instead of the Eberly et al. construction and running time. If  $A_0$  is invertible, then the actual rank of  $A$  is at least the estimated  $r$  given by the [33] algorithm.

Finally, we compute the Schur complement of the principal minor, namely  $A_2 A_0^{-1} A_1 - A_3$ , and check if it is 0. If so, we output the rank  $r$  and the nullspace of  $A$ , which is given by

$$\begin{bmatrix} A_0^{-1} A_1 \\ -I \end{bmatrix}. \quad (4.2)$$

To compute the Schur complement, we can no longer use the fact that we can multiply  $A_0^{-1}$  efficiently with an arbitrary matrix as in Eberly et al., since in our construction we made the inverse explicit. However, since  $A$  is an efficient black box (due to the original sparsity and the structure of the preconditioning matrices  $U, L, D$ ), we can still treat  $A_1 \in F^{r \times (n-r)}$  and  $A_2 \in F^{(n-r) \times r}$  as efficient black boxes.

► **Lemma 20.** *For a matrix  $A \in F^{n \times n}$  with a non-singular leading minor  $A_0$ , the Schur complement  $A_2 A_0^{-1} A_1 - A_3$  can be computed in time*

$$\hat{O}(mn\phi(n) + n^{\omega_s} + mn^2 + n\phi(n)).$$

*If  $\phi(n) = \hat{O}(n)$ , then an expected number of  $O(n^{2.2131})$  operations is required.*

**Proof.** Let  $r \in \mathbb{Z}$  be such that  $A_0 \in F^{r \times r}$ , and thus  $A_1 \in F^{r \times (n-r)}$  and  $A_2 \in F^{(n-r) \times r}$ . By Theorem 4, the time to invert  $A_0$  explicitly is  $\hat{O}(mn\phi(n) + n^{\omega_s} + mn^2)$ . To compute  $A_0^{-1} A_1$ , we will instead perform the product  $A_1^T (A_0^{-1})^T$  and then transpose. First consider the case where  $r \leq n - r$ , and divide  $A_1^T \in F^{(n-r) \times r}$  into square blocks of size  $r \times r$ . Applying each block to  $(A_0^{-1})^T$  requires at most  $r\phi(n)$  operations, and there are  $\lfloor n/r \rfloor$  such blocks. Therefore, computing  $A_0^{-1} A_1$  requires  $n$  black-box applications of  $A_1$ , or at most  $n\phi(n)$  operations. In the second case, we have  $r \geq n - r$ . We add  $2r - n$  rows of 0s to  $A_1^T$  to turn it into a square matrix and then perform the product  $A_1^T (A_0^{-1})^T$  with  $r$  black-box applications. Overall, we require at most  $n\phi(n)$  operations to compute  $A_0^{-1} A_1$ . The same construction carries over when performing the product  $A_2 \cdot (A_0^{-1} A_1)$ , which we can obtain with at most  $n$  black-box applications of  $A_2$ . ◀

By assembling the [33] algorithm for probabilistically computing the rank with the Eberly et al. nullspace computation and rank certification, along with our speed-up for sparse matrix inversion, we obtain the following final running time:

► **Theorem 21.** *Let  $A \in F^{n \times n}$  be a non-singular matrix, where  $F$  is a finite field. The procedure  $\text{MATRIXRANKANDNULLSPACE}(A)$  (see Algorithm 4) returns the rank  $r$  of  $A$ , and a matrix  $N$  whose columns form a basis of the nullspace of  $A$ , in expected time*

$$\hat{O}(mn\phi(n) + s^\omega m + n^{\omega_s} + mn^2),$$

where  $sm = n$ . If  $\phi(n) = \hat{O}(n)$ , e.g., if  $A$  is sparse, then the inverse  $A^{-1}$  can be computed in expected time  $\hat{O}(n^{\omega(k)})$ , where  $k = \log_n s$  is the only value that satisfies  $\omega(k) = 3 - k$ . With the current values of rectangular matrix multiplication, this corresponds to  $O(n^{2.2131})$  arithmetic operations.

**Proof.** Given a sparse matrix  $A \in F^{n \times n}$ , using the algorithm described in this section and Lemma 2, we can compute a basis  $\{v_i\}$  of the nullspace of the preconditioned matrix  $\tilde{A} = UALD$  in time  $O(n^{2.2131})$ . Then  $\{LDv_i\}$  is a basis of the nullspace of  $A$ . Since  $D$  is a diagonal matrix and  $L$  is a lower triangular Toeplitz matrix, the additional multiplications only cost  $O(n^2)$  and thus do not add an overhead to the running time. ◀

■ **Algorithm 4** Computing the rank and nullspace of an arbitrary matrix over a finite field.

---

```

1: procedure MATRIXRANKANDNULLSPACE( $A$ )                                ▷ Theorem 21
2:    $r \leftarrow$  rank of  $A$  w.h.p.                                       ▷ [33] algorithm (Thm. 19)
3:   Partition  $A$  into the 4 blocks  $A_0, A_1, A_2, A_3$ .                   ▷ Equation 4.1
4:   Compute  $A_0^{-1}$  (if singular, re-try the [33] algorithm).           ▷ Alg. 1 or Alg. 2
5:   Compute the Schur complement  $A_2A_0^{-1}A_1 - A_3$ .                 ▷ Lemma 20
6:   if  $A_2A_0^{-1}A_1 - A_3 = 0$  then
7:      $N \leftarrow [A_0^{-1}A_1 | -I]^T$                                    ▷ Nullspace of  $A$ 
8:     return  $r, N$ .
9:   else
10:    Restart from Line 2.
11:  end if
12: end procedure

```

---

More generally, the rank and nullspace algorithm presented in this section yield the following observation:

► **Remark 22.** For any matrix inversion algorithm  $\text{MATRIXINV}$  with running time  $T_{\text{MATRIXINV}}$ , the algorithm  $\text{MATRIXRANKANDNULLSPACE}$  requires an expected running time of

$$T_{\text{MATRIXRANKANDNULLSPACE}} = T_{\text{MATRIXINV}} + n\phi(n).$$

In particular, for sparse matrices the running time of the two algorithms is the same.

## 5 Applications

The algorithm described in Section 4 for computation of the rank and nullspace of a sparse matrix over a finite field has multiple applications. Some relevant to theoretical computer science include efficient decoding of algebraic-geometric codes [29, 43], low density parity check codes [4], discrete logarithm computations in cryptography [30], and (multivariate) polynomial interpolation [44].

## 5.1 Topological Data Analysis

Our first detailed example deals with the calculation of persistent homology in topological data analysis. Persistent homology is a widely used technique to determine shape features of point clouds [16, 17, 59]. To a point cloud  $X$  (i.e., a finite set of points in Euclidean space) one associates a filtered simplicial complex  $V(X) = \{V_\varepsilon(X)\}_{\varepsilon>0}$  by one of several possible methods [45]; for instance, the *Vietoris–Rips complex* contains, for each value of  $\varepsilon$ , a  $k$ -simplex for each set of  $k + 1$  points in  $X$  with diameter less than or equal to  $\varepsilon$ . The *persistence diagram* of  $X$  has a point  $(b, d)$  with  $d > b$  for each homology generator in any dimension of  $V(X)$  arising at a parameter value  $\varepsilon = b$  (birth) and vanishing at  $\varepsilon = d$  (death). The *persistence* or *lifetime* of such a homology class is then defined to be  $d - b$ . A non-zero homology class in dimension  $k$  is represented by a  $k$ -cycle that is not a boundary.

Computing a persistence diagram for a point cloud  $X$  requires finding ranks of matrices of boundary operators on  $V(X)$ ; see [45, §5.3]. For convenience, we assume that coefficients in the field  $F = \mathbb{Z}/2\mathbb{Z}$  are used. The maximum number of linearly independent homology classes in dimension  $k$  of a simplicial complex is called the  $k$ -th *Betti number* of that complex. The running time of algorithms based on Gaussian Elimination for the calculation of Betti numbers and persistent homology is  $O(n^3)$  where  $n$  is the total number of simplices in the given complex. Using less straightforward methods, the complexity was reduced to  $O(n^\omega)$  in [40]. An output-sensitive algorithm for the computation of persistence diagrams was described in [7] with the following running time.

► **Theorem 23** ([7]). *Given a filtered simplicial complex with  $n$  simplices, let  $C_\Gamma$  denote the number of homology generators with persistence at least  $\Gamma$  for any threshold  $\Gamma > 0$ . Then, a persistence diagram over  $\mathbb{Z}/2\mathbb{Z}$  can be computed deterministically in  $O(C_\Gamma n^\omega \log n)$  time or probabilistically in expected  $O(C_\Gamma n^{3-1/(\omega-1)})$  time.*

Imposing that  $C_\Gamma$  be at most of the order of  $\log n$  is a reasonable assumption in practice, because homology classes with small persistence are treated as noise in most applications of topological data analysis. Since  $3 - 1/(\omega - 1) = 2.2716$  for the current value of  $\omega$ , the following theorem improves the running time obtained in [7]. This constitutes an interesting application of our results in which the sparsity of the matrix is inherent.

► **Theorem 24.** *For a filtered simplicial complex with a total number of  $n$  simplices, a persistence diagram over  $\mathbb{Z}/2\mathbb{Z}$  can be computed in expected time  $O(n^{2.2131})$  if the persistence of homology generators is bounded below so that their number is at most logarithmic in  $n$ .*

**Proof.** The algorithm of [7] requires computing ranks of a collection of sparse submatrices of an  $n \times n$  matrix, which can be done with  $O(n^{2.2131})$  field operations by Theorem 21. ◀

We also provide the following complexity for ordinary (not persistent) homology. Although this result also applies to simplicial complexes equipped with a filter function, its randomized nature obstructs the precise determination of persistence of cycles.

► **Theorem 25.** *If a simplicial complex  $V$  has a total number of  $n$  simplices, then the Betti numbers of  $V$  with coefficients in a finite field together with a basis of cycles in each dimension can be computed in expected time  $O(n^{2.2131})$ .*

**Proof.** The matrices of boundary operators on  $V$  can be assembled into a single  $n \times n$  matrix  $A$  such that  $A_{i,j} = \pm 1$  if and only if the  $i$ -th simplex occurs in the boundary of the  $j$ -th simplex. Hence this matrix  $A$  is upper triangular and has  $k + 1$  non-zero entries in each column corresponding to a  $k$ -simplex. Since dimension depends logarithmically on the number of simplices (because a  $k$ -simplex has  $2^{k+1} - 1$  faces), the total number of non-zero entries in  $A$  is  $O(n \log n)$ . Consequently,  $A$  is sparse.

It then follows from Theorem 21 that the rank and nullspace of  $A$  can be computed with an expected number of  $O(n^{2.2131})$  operations. The rank of the boundary operator on each dimension can be obtained similarly by restricting the calculation to the corresponding submatrix. Knowledge of the nullspace of  $A$  yields a set of linearly independent generating cycles in each dimension. Since the number of dimensions is  $O(\log n)$ , our claim follows. ◀

## 5.2 Units in Group Rings

For a finite group  $G$  of order  $n$  and a ring  $R$  with unity, the group ring  $R[G]$  is isomorphic to a certain subring of the ring of  $n \times n$  matrices over  $R$ , as proved in [28]. If we assume that the elements of  $G$  are ordered as  $g_1, \dots, g_n$ , then we may consider the matrix  $M(G) = (g_i^{-1}g_j)$  for  $i = 1, \dots, n$  and  $j = 1, \dots, n$ . The elements in the group ring  $R[G]$  are formal sums of elements  $g_i \in G$  with coefficients  $\beta_{g_i} \in R$ . For each element  $\beta = \sum_{i=1}^n \beta_{g_i} g_i$  in  $R[G]$  we are concerned with the problem of determining whether a given element  $\beta$  is a unit or not.

Following the method outlined in [20], to each element  $\beta \in R[G]$  we may assign the matrix  $M_\beta = (\beta_{g_i^{-1}g_j})$ . This is the matrix of right-multiplication by  $\beta$  written in the  $R$ -basis  $g_1, \dots, g_n$ . Hence  $\beta \mapsto M_\beta$  sets up an injective ring homomorphism [28, Theorem 1]. This yields a method to test if a given element  $\beta \in R[G]$  is a unit, by checking if the matrix  $M_\beta$  is invertible. In fact, if  $\beta$  happens to be a unit, then  $\beta^{-1}$  is associated with the inverse matrix  $M_\beta^{-1}$ .

As in [20, §4.2], we consider the case when the group  $G$  is metacyclic and coefficients in a field  $F$  are used. We will assume, however, that the field  $F$  is finite. When  $G$  is metacyclic, it admits a presentation of the form  $\langle \sigma, \tau \mid \sigma^m = 1, \tau^s = \sigma^t, \tau^{-1}\sigma\tau = \sigma^u \rangle$  for integers  $m, t, u, s$  with  $u \leq m, t \leq m, u^s \equiv 1 \pmod t$ , and  $ut \equiv t \pmod m$ . The order of  $G$  is  $n = ms$ . If we list the elements of  $G$  as

$$1, \tau, \dots, \tau^{s-1}, \sigma, \sigma\tau, \dots, \sigma\tau^{s-1}, \dots, \sigma^{m-1}, \sigma^{m-1}\tau, \dots, \sigma^{m-1}\tau^{s-1}$$

then the matrix  $M(G)$  is block Toeplitz with blocks of size  $s \times s$ . Therefore each matrix  $M_\beta$  for  $\beta \in F[G]$  is also block Toeplitz, so its invertibility can be tested with  $\tilde{O}(s^\omega m)$  operations in  $F$ . As observed in [20, §4.2], it is equally possible to exchange the roles of  $\sigma$  and  $\tau$  so that we obtain a block Toeplitz matrix with blocks of size  $m \times m$  instead.

► **Theorem 26.** *For a finite field  $F$  and a finite group  $G$  with a normal subgroup which is cyclic of order  $m$  and cyclic quotient of order  $s$ , determining if an element  $\beta \in F[G]$  is invertible and, if so, computing the set  $\{g\beta^{-1}\}_{g \in G}$  explicitly can be done in expected time  $O(\omega(\min\{\log_n m, \log_n s\}))$ .*

**Proof.** The  $G$ -orbit  $\{g\beta^{-1}\}_{g \in G}$  corresponds to the rows of the inverse matrix  $M_\beta^{-1}$ . Since  $M_\beta$  is block Toeplitz, the result follows from Theorem 13. ◀

Theorem 26 yields approximately quadratic running time, since one of  $m$  or  $s$  is smaller than or equal to  $\sqrt{n}$ , and  $\omega(0.5) = 2.0442$  according to [19]. For a field  $F$  of characteristic zero, the running time given in [20, Proposition 4.13] is  $\hat{O}(n^{(\omega+1)/2})$  in order to check invertibility of  $M_\beta$  and obtain  $\beta^{-1}$ , while the  $G$ -orbit of  $\beta$  can be written down in  $\hat{O}(n^{(\omega+3)/2}) = O(n^{2.6864})$ .

---

**References**

---

- 1 Josh Alman and Virginia Vassilevska Williams. A refined laser method and faster matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 522–539. SIAM, 2021.
- 2 Bernhard Beckermann and George Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3):804–823, 1994. Publisher: SIAM.
- 3 Robert R. Bitmead and Brian DO Anderson. Asymptotically fast solution of Toeplitz and related systems of linear equations. *Linear Algebra and its Applications*, 34:103–116, 1980. Publisher: Elsevier.
- 4 Nicholas Bonello, Sheng Chen, and Lajos Hanzo. Low-density parity-check codes and their rateless relatives. *IEEE Communications Surveys & Tutorials*, 13(1):3–26, 2010. Publisher: IEEE.
- 5 Alin Bostan, Claude-Pierre Jeannerod, and Éric Schost. Solving Toeplitz- and Van-dermonde-like linear systems with large displacement rank. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 33–40, 2007.
- 6 David G. Cantor and Erich Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28:693–701, 1991.
- 7 Chao Chen and Michael Kerber. An output-sensitive algorithm for persistent homology. *Computational Geometry*, 46(4):435–447, 2013. Publisher: Elsevier.
- 8 Michael B. Cohen, Yin Tat Lee, and Zhao Song. Solving linear programs in the current matrix multiplication time. *Journal of the ACM (JACM)*, 68(1):1–39, 2021. Publisher: ACM New York, NY, USA.
- 9 Henry Cohn and Christopher Umans. Fast matrix multiplication using coherent configurations. In *Proceedings of the 24th annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1074–1087. SIAM, 2013.
- 10 Don Coppersmith. Solving homogeneous linear equations over  $\text{GF}(2)$  via block Wiedemann algorithm. *Mathematics of Computation*, 62(205):333–350, 1994.
- 11 Don Coppersmith and Shmuel Winograd. On the asymptotic complexity of matrix multiplication. *SIAM Journal on Computing*, 11(3):472–492, 1982. Publisher: SIAM.
- 12 James Demmel, Ioana Dumitriu, Olga Holtz, and Robert Kleinberg. Fast matrix multiplication is stable. *Numerische Mathematik*, 106(2):199–224, 2007. Publisher: Springer.
- 13 John D. Dixon. Exact solution of linear equations using  $p$ -adic expansions. *Numerische Mathematik*, 40(1):137–141, 1982. Publisher: Springer.
- 14 Wayne Eberly, Mark Giesbrecht, Pascal Giorgi, Arne Storjohann, and Gilles Villard. Solving sparse rational linear systems. In *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 63–70, 2006.
- 15 Wayne Eberly, Mark Giesbrecht, Pascal Giorgi, Arne Storjohann, and Gilles Villard. Faster inversion and other black box matrix computations using efficient block projections. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 143–150, 2007.
- 16 Herbert Edelsbrunner and John Harer. Persistent homology – a survey. *Contemporary Mathematics*, 453:257–282, 2008. Publisher: Providence, RI: American Mathematical Society.
- 17 Herbert Edelsbrunner, David Letscher, and Afra Zomorodian. Topological persistence and simplification. In *Proceedings 41st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 454–463. IEEE, 2000.
- 18 François Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 296–303, 2014.
- 19 François Le Gall and Florent Urrutia. Improved rectangular matrix multiplication using powers of the Coppersmith-Winograd tensor. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1029–1046. SIAM, 2018.

- 20 Mark Giesbrecht, Armin Jamshidpey, and Éric Schost. Subquadratic-Time Algorithms for Normal Bases. *arXiv preprint arXiv:2005.03497*, 2020.
- 21 Pascal Giorgi, Claude-Pierre Jeannerod, and Gilles Villard. On the complexity of polynomial matrix computations. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 135–142, 2003.
- 22 Israel Gohberg and Georg Heinig. Inversion of finite Toeplitz matrices made of elements of a non-commutative algebra. *Rev. Roumaine Math. Pures Appl.*, XIX(5):623–663, 1974.
- 23 Israel Gohberg and Naum Ya Krupnik. A formula for the inversion of finite Toeplitz matrices. *Mat. Issled.*, 7(2):272–283, 1972.
- 24 Israel Gohberg and Arkadii Semencul. On the inversion of finite Toeplitz matrices and their continuous analogs. *Mat. Issled.*, 7(12):201–233, 1972.
- 25 Magnus Rudolph Hestenes and Eduard Stiefel. *Methods of conjugate gradients for solving linear systems*, volume 49. NBS Washington, DC, 1952.
- 26 Xiaohan Huang and Victor Y. Pan. Fast rectangular matrix multiplication and applications. *Journal of Complexity*, 14(2):257–299, 1998. Publisher: Elsevier.
- 27 Yufan Huang and Richard Peng. Laplacians are Complete for Linear System over  $\mathbb{Z}_p$ , 2020.
- 28 Ted Hurley. Group rings and rings of matrices. *Int. J. Pure Appl. Math.*, 31(3):319–335, 2006.
- 29 Edmund Jonckheere and Chingwo Ma. A simple Hankel interpretation of the Berle-kamp-Massey algorithm. *Linear Algebra and its Applications*, 125:65–76, 1989. Publisher: Elsevier.
- 30 Antoine Joux and Cécile Pierrot. Nearly sparse linear algebra and application to discrete logarithms computations. In *Contemporary Developments in Finite Fields and Applications*, pages 119–144. World Scientific, 2016.
- 31 Thomas Kailath, Sun-Yuan Kung, and Martin Morf. Displacement ranks of matrices and linear equations. *Journal of Mathematical Analysis and Applications*, 68(2):395–407, 1979. Publisher: Elsevier.
- 32 Erich Kaltofen. Analysis of Coppersmith’s block Wiedemann algorithm for the parallel solution of sparse linear systems. *Mathematics of Computation*, 64(210):777–806, 1995.
- 33 Erich Kaltofen and B. David Saunders. On Wiedemann’s method of solving sparse linear systems. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 29–38. Springer, 1991.
- 34 Rasmus Kyng, Di Wang, and Peng Zhang. Packing LPs are hard to solve accurately, assuming linear equations are hard. In *Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 279–296. SIAM, 2020.
- 35 Rasmus Kyng and Peng Zhang. Hardness Results for Structured Linear Systems. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 684–695. IEEE, 2017.
- 36 George Labahn and Stan Cabay. Matrix Padé fractions and their computation. *SIAM Journal on Computing*, 18(4):639–657, 1989. Publisher: SIAM.
- 37 George Labahn, Dong Koo Choi, and Stan Cabay. The inverses of block Hankel and block Toeplitz matrices. *SIAM Journal on Computing*, 19(1):98–123, 1990. Publisher: SIAM.
- 38 Brian A. LaMacchia and Andrew M. Odlyzko. Solving large sparse linear systems over finite fields. In *Conference on the Theory and Application of Cryptography*, pages 109–133. Springer, 1990.
- 39 Cornelius Lanczos. *An iteration method for the solution of the eigenvalue problem of linear differential and integral operators*. United States Governm. Press Office Los Angeles, CA, 1950.
- 40 Nikola Milosavljević, Dmitriy Morozov, and Primoz Skraba. Zigzag persistent homology in matrix multiplication time. In *Proceedings of the 27th Annual Symposium on Computational Geometry*, pages 216–225, 2011.
- 41 Cameron Musco, Christopher Musco, and Aaron Sidford. Stability of the Lanczos method for matrix function approximation. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1605–1624. SIAM, 2018.

- 42 Zipei Nie. Matrix anti-concentration inequalities with applications. *arXiv preprint arXiv:2111.05553*, 2021.
- 43 Vadim Olshevsky and Amin Shokrollahi. A displacement approach to efficient decoding of algebraic-geometric codes. In *Proceedings of the 31st annual ACM Symposium on Theory of Computing (STOC)*, pages 235–244, 1999.
- 44 Peter J. Olver. On multivariate interpolation. *Studies in Applied Mathematics*, 116(2):201–240, 2006. Publisher: Wiley Online Library.
- 45 Nina Otter, Mason A. Porter, Ulrike Tillmann, Peter Grindrod, and Heather A. Harrington. A roadmap for the computation of persistent homology. *EPJ Data Science*, 6:1–38, 2017. Publisher: Springer.
- 46 Victor Pan. New fast algorithms for matrix operations. *SIAM Journal on Computing*, 9(2):321–342, 1980. Publisher: SIAM.
- 47 Victor Pan. On computations with dense structured matrices. *Mathematics of Computation*, 55(191):179–190, 1990.
- 48 Victor Pan. *Structured matrices and polynomials: unified superfast algorithms*. Springer Science & Business Media, 2001.
- 49 Richard Peng and Santosh Vempala. Solving sparse linear systems faster than matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 504–521. SIAM, 2021.
- 50 Yousef Saad. *Iterative methods for sparse linear systems*. SIAM, 2003.
- 51 Daniel A. Spielman and Shang-Hua Teng. Nearly linear time algorithms for preconditioning and solving symmetric, diagonally dominant linear systems. *SIAM Journal on Matrix Analysis and Applications*, 35(3):835–885, 2014. Publisher: SIAM.
- 52 Arne Storjohann. The shifted number system for fast linear algebra on integer matrices. *Journal of Complexity*, 21(4):609–650, 2005. Publisher: Elsevier.
- 53 Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969. Publisher: Springer.
- 54 Volker Strassen. The asymptotic spectrum of tensors and the exponent of matrix multiplication. In *27th Annual Symposium on Foundations of Computer Science (FOCS 1986)*, pages 49–54. IEEE, 1986.
- 55 William F. Trench. An algorithm for the inversion of finite Toeplitz matrices. *Journal of the Society for Industrial and Applied Mathematics*, 12(3):515–522, 1964. Publisher: SIAM.
- 56 Virginia Vassilevska Williams. Multiplying matrices faster than Coppersmith-Winograd. In *Proceedings of the 44th annual ACM Symposium on Theory of Computing (STOC)*, pages 887–898, 2012.
- 57 Douglas Wiedemann. Solving sparse linear equations over finite fields. *IEEE Transactions on Information Theory*, 32(1):54–62, 1986. Publisher: IEEE.
- 58 James Hardy Wilkinson. Error analysis of direct methods of matrix inversion. *Journal of the ACM (JACM)*, 8(3):281–330, 1961. Publisher: ACM New York, NY, USA.
- 59 Afra Zomorodian and Gunnar Carlsson. Computing persistent homology. *Discrete & Computational Geometry*, 33(2):249–274, 2005. Publisher: Springer.
- 60 Uri Zwick. All pairs shortest paths using bridging sets and rectangular matrix multiplication. *Journal of the ACM (JACM)*, 49(3):289–317, 2002. Publisher: ACM New York, NY, USA.