

NONLINEAR MATROID OPTIMIZATION AND EXPERIMENTAL DESIGN*

Yael Berstein[†], Jon Lee[‡], Hugo Maruri-Aguilar[§], Shmuel Onn[†],
Eva Riccomagno[¶], Robert Weismantel^{||}, and Henry Wynn[§]

Abstract. We study the problem of optimizing nonlinear objective functions over matroids presented by oracles or explicitly. Such functions can be interpreted as the balancing of multicriteria optimization. We provide a combinatorial polynomial time algorithm for arbitrary oracle-presented matroids, that makes repeated use of matroid intersection and an algebraic algorithm for vectorial matroids. Our work is partly motivated by applications to minimum-aberration model-fitting in experimental design in statistics, which we discuss and demonstrate in detail.

Key words. matroid, matroid intersection, Binet–Cauchy identity, spanning tree, matching, exact matching, experimental design, aberration, algebraic statistics, learning, interpolation, regression, nonlinear discrete optimization, combinatorial optimization, integer programming

AMS subject classifications. 05A, 15A, 51M, 52A, 52B, 52C, 62H, 62K, 65C, 68Q, 68R, 68U, 68W, 90B, 90C

DOI. 10.1137/070696465

1. Introduction. In this article, partly motivated by applications to minimum-aberration model-fitting in experimental design, which will be discussed briefly at the end of this introduction and in detail in section 5, we study the problem of optimizing an arbitrary nonlinear function over a matroid as follows.

Nonlinear matroid optimization. Given matroid M on ground set $N := \{1, \dots, n\}$, integer weight vectors $w_i = (w_{i,1}, \dots, w_{i,n}) \in \mathbb{Z}^n$ for $i = 1, \dots, d$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$, find a matroid base $B \in \mathcal{B}(M) \subset 2^N$ minimizing the “balancing” by f of

*Received by the editors July 6, 2007; accepted for publication (in revised form) February 11, 2008; published electronically May 16, 2008.

<http://www.siam.org/journals/sidma/22-3/69646.html>

[†]Technion - Israel Institute of Technology, 32000 Haifa, Israel (yaelber@tx.technion.ac.il, onn@ie.technion.ac.il). The first author was supported by an Irwin and Joan Jacobs Scholarship and by a scholarship from the Graduate School of the Technion. The fourth author was partially supported by the Joan and Reginald Coleman-Cohen Exchange Program during a stay of Henry Wynn at the Technion, was partially supported by the Mathematisches Forschungsinstitut Oberwolfach during a stay within the Research in Pairs Programme, and was also supported by the ISF - Israel Science Foundation.

[‡]IBM T.J. Watson Research Center, Yorktown Heights, NY 10598 (jonlee@us.ibm.com). This author was partially supported by the Mathematisches Forschungsinstitut Oberwolfach during a stay within the Research in Pairs Programme.

[§]London School of Economics, London WC2A 2AE, UK (h.maruri-aguilar@lse.ac.uk, h.wynn@lse.ac.uk). The third and last authors were supported by the Research Councils UK (RCUK) Basic Technology grant “Managing Uncertainty in Complex Models.” The last author was partially supported by the Joan and Reginald Coleman-Cohen Exchange Program during a stay of his at the Technion.

[¶]Università degli Studi di Genova, 16146 Genova, Italy (riccomagno@dima.unige.it).

^{||}Otto-von-Guericke Universität Magdeburg, D-39106 Magdeburg, Germany (weismantel@imo.math.uni-magdeburg.de). This author was partially supported by the Mathematisches Forschungsinstitut Oberwolfach during a stay within the Research in Pairs Programme and was also supported by the European TMR Network ADONET 504438.

the d weights $w_i(B) := \sum_{j \in B} w_{i,j}$ of base B ,

$$f(w_1(B), \dots, w_d(B)) = f \left(\sum_{j \in B} w_{1,j}, \dots, \sum_{j \in B} w_{d,j} \right).$$

(All necessary basics about matroid theory are provided in section 2.1. For more details consult [14] or [17].)

Nonlinear matroid optimization can be interpreted as *multicriteria matroid optimization*: the d given weight vectors w_1, \dots, w_d represent d different criteria, where the value of base $B \in \mathcal{B}(M)$ under criterion i is its i th weight $w_i(B) = \sum_{j \in B} w_{i,j}$, and where the objective is to minimize the “balancing” $f(w_1(B), \dots, w_d(B))$ of the d given criteria by the given function f .

In fact, we have a hierarchy of problems of increasing generality, parameterized by the number d of weight vectors. At the bottom of the hierarchy lies standard linear matroid optimization, recovered with $d = 1$ and f being the identity on \mathbb{Z} . At the top of the hierarchy lies the problem of maximizing an arbitrary function over the set of bases, with $d = n$ and $w_i = \mathbf{1}_i$, the i th standard unit vector in \mathbb{Z}^n for all i ; see Proposition 2.4.

It will often be convenient to collect the weight vectors in a $d \times n$ matrix W . Thus, the i th row of this matrix is the i th weight vector $w_i = (w_{i,1}, \dots, w_{i,n})$. For each subset $S \subseteq N$ we define its W -image to be

$$W(S) := (w_1(S), \dots, w_d(S)) := \left(\sum_{j \in S} w_{1,j}, \dots, \sum_{j \in S} w_{d,j} \right) \in \mathbb{Z}^d,$$

which is the vector giving the value of S under each of the d weight vectors. The nonlinear matroid optimization then asks for a matroid base $B \in \mathcal{B}(M)$ minimizing the objective function $f(W(B))$.

The computational complexity of nonlinear matroid optimization depends on the number d of weight vectors, on the representation of weights (binary $\langle w_{i,j} \rangle$ versus unary $|w_{i,j}|$; see section 2.1), on the type of function f and its presentation, and on the type of matroid and its presentation. We will be able to handle an arbitrary function f presented by a *comparison oracle* that, queried on $u, v \in \mathbb{Z}^d$, asserts whether or not $f(u) \leq f(v)$, and an arbitrary matroid presented by an *independence oracle*, that, queried on $I \subseteq N$, asserts whether or not I is *independent* in M , that is, whether $I \subseteq B$ for some base $B \in \mathcal{B}(M)$; see section 2.1. These are very broad presentations that reveal little information (per query) on the function and matroid, making our problem setting rather expressive but difficult for achieving strong complexity results.

Standard linear matroid optimization is well known to be efficiently solvable by the greedy algorithm. Nonlinear matroid optimization with d fixed and f *concave* turns out to be solvable in polynomial time as well [8, 11]. In fact, using sophisticated geometric methods, the nonlinear optimization problem with d fixed and f concave has been recently shown to be efficiently solvable for bipartite matching [4] and for broader classes of combinatorial optimization problems [12]. Therein, maximization rather than minimization form is used; hence, convex rather than concave functions are considered.

However, generally, nonlinear matroid optimization is intractable, even for uniform matroids. In particular, if d is variable, then exponential time is needed even for $\{0, 1\}$ -valued weights, and if the weights are encoded in binary, then exponential

time is needed even for fixed dimension $d = 1$. See Propositions 2.3, 2.4, and 2.5 in what follows for various intractability statements.

In spite of these difficulties, we establish here the efficient solvability of the problem as follows.

THEOREM 1.1. *For every fixed d and p , there is an algorithm that, given a matroid M presented by an independence oracle on the n -element ground set N , integers $a_1, \dots, a_p \in \mathbb{Z}$, weight vectors $w_1, \dots, w_d \in \{a_1, \dots, a_p\}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the nonlinear matroid optimization problem in time that is polynomial in n and $\max\langle a_i \rangle$.*

We also state the following natural immediate corollary concerning $\{0, 1, \dots, p\}$ -valued weights.

COROLLARY 1.2. *For every fixed d and p , there is an algorithm that, given n -element matroid M presented by an independence oracle, $w_1, \dots, w_d \in \{0, 1, \dots, p\}^n$ and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the nonlinear matroid optimization problem in time polynomial in n .*

The algorithm establishing Theorem 1.1 is combinatorial and makes repeated use of matroid intersection (see, e.g., [9] or [10], and see [7] for another recent interesting application of matroid intersection). In fact, it invokes the matroid intersection algorithm roughly n^{p^d} times, and hence it is quite heavy. However, most matroids appearing in practice, including graphic matroids and those arising in the applications to experimental design to be discussed later, are vectorial. Therefore, we also provide another more efficient, linear-algebraic algorithm for vectorial matroids. Moreover, this algorithm applies to weights with an unlimited number (rather than a fixed number p) of different values $w_{i,j}$ of entries.

THEOREM 1.3. *For every fixed d , there is an algorithm that, given integer $m \times n$ matrix A , weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the nonlinear optimization problem over the (real) vectorial matroid of A in time polynomial in $\langle A \rangle$ and $\max |w_{i,j}|$.*

A specific application that can be solved by either the combinatorial algorithm underlying Theorem 1.1 or the more efficient linear-algebraic algorithm underlying Theorem 1.3 is the following example.

Example 1.4 (minimum-norm spanning tree). Fix any positive integer d . Let G be any connected graph with edge set $E = \{e_1, \dots, e_n\}$, and let $w_1, \dots, w_d \in \mathbb{Z}^n$ be weight vectors with $w_{i,j}$ representing the values of edge e_j under the i th criterion. Let A be the vertex-arc incidence matrix of an arbitrary orientation of G . Then the vectorial matroid of A is the graphic matroid of G whose bases are the spanning trees of G . Now fix also any q that is either a positive integer or ∞ , and let $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ be the l_q norm given by $\|u\|_q := (\sum_{i=1}^d |u_i|^q)^{\frac{1}{q}}$ for finite q and $\|u\|_\infty := \max_{i=1}^d |u_i|$. Note that a comparison oracle for $f(u) = \|u\|_q$ is easily and efficiently realizable. Then Theorems 1.1 and 1.3 assure that a spanning tree T of G minimizing the l_q norm of the multicriteria vector, given by

$$\|(w_1(T), \dots, w_d(T))\|_q = \|W(T)\|_q$$

is computable in time polynomial in n and $\max |w_{i,j}|$. Note that if $P \neq NP$, then the problem is *not* solvable in time polynomial in the binary length $\langle w_{i,j} \rangle$ even for the graph obtained from a path by replacing every edge by two parallel copies; see Proposition 2.5.

Experimental design. We conclude the introduction with a brief discussion of the application to experimental design, elaborated in detail in section 5. The general

framework is as follows. We are interested in learning an unknown system whose output y is an unknown function Φ of a multivariate input $x = (x_1, \dots, x_k) \in \mathbb{R}^k$. It is customary to call the input variables x_j *factors* of the system. In order to learn the system, we perform several experiments. Each experiment i is determined by a point $p_i = (p_{i,1}, \dots, p_{i,k})$ and consists of feeding the system with input $x := p_i$ and measuring the corresponding output $y_i = \Phi(p_i)$. Based on these experiments, we wish to *fit a model* for the system, namely, determine an estimation $\hat{\Phi}$ of the function Φ , that satisfies the following properties:

- It lies in a prescribed class of functions.
- It is consistent with the outcomes of the experiments.
- It minimizes the *aberration*—a suitable criterion—among models in the class.

More detailed discussion and precise definitions will be given in section 5. We have the following broad corollary of Theorems 1.1 and 1.3; see section 5 for the precise statement and its various practical specializations to concrete aberration criteria useful in optimal model-fitting in experimental design.

COROLLARY 1.5. *An aberration-minimum multivariate-polynomial model is polynomial time computable.*

The article proceeds as follows. In section 2 we set some notation and preliminaries, make some preparations for the algorithms in the following sections, and demonstrate various intractability limitations on nonlinear matroid optimization. In section 3 we discuss arbitrary matroids presented by oracles, and provide the combinatorial algorithm for nonlinear matroid optimization, thereby establishing Theorem 1.1. In section 4 we provide the more efficient algebraic algorithm for nonlinear optimization over vectorial matroids, thereby proving Theorem 1.3. We conclude in section 5 with a detailed discussion of the experimental design application and prove Corollary 5.2 (a refined version of Corollary 1.5) and its various practical specializations. Readers interested mostly in experimental design can go directly to section 5, where the minimum-aberration model-fitting problem is reduced to nonlinear optimization over a suitable matroid, and where each of the algorithms developed in sections 3 and 4 can be invoked as a black box.

2. Preliminaries, preparation, and limitations.

2.1. Preliminaries. We use \mathbb{R} for the reals, \mathbb{Z} for the integers, and \mathbb{N} for the nonnegative integers. The i th standard unit vector in \mathbb{R}^n is denoted by $\mathbf{1}_i$. The *support* of $x \in \mathbb{R}^n$ is the index set $\text{supp}(x) := \{j : x_j \neq 0\}$ of nonzero entries of x . The integer lattice \mathbb{Z}^n is naturally embedded in \mathbb{R}^n . Vectors will be interpreted as either row or column vectors interchangeably—this will be relevant only when such vectors are multiplied by matrices—in which case the correct interpretation will be clear from the context. We often collect a sequence of vectors designated by a lower-case letter as the rows of a matrix designated by the corresponding upper case letter. Thus, our weight vectors $w_i = (w_{i,1}, \dots, w_{i,n})$, $i = 1, \dots, d$ are arranged in a $d \times n$ matrix W , and our design points $p_i = (p_{i,1}, \dots, p_{i,k})$, $i = 1, \dots, m$ are arranged in an $m \times k$ matrix P . The space \mathbb{R}^n is endowed with the standard inner product which, for $w, x \in \mathbb{R}^n$, is $w \cdot x := \sum_{i=1}^n w_i x_i$. Vectors w in \mathbb{R}^n are also regarded as linear functions on \mathbb{R}^n via the inner product $w \cdot x$. Therefore, we refer to elements of \mathbb{R}^n as points, vectors, or linear functions, as is appropriate from the context. We write $\mathbf{1}$ for the vector with all entries equal to 1, with the dimension being clear from the context.

Our algorithms are analyzed for rational data only, and the time complexity is as in the standard Turing machine model; see, e.g., [1, 6, 16]. The input typically

consists of rational (usually integer) numbers, vectors, matrices, and finite sets of such objects. The *binary length* of an integer number $z \in \mathbb{Z}$ is defined to be the number of bits in its binary representation, $\langle z \rangle := 1 + \lceil \log_2(|z| + 1) \rceil$ (with the extra bit for the sign). The length of a rational number presented as a fraction $r = \frac{p}{q}$ with $p, q \in \mathbb{Z}$ is $\langle r \rangle := \langle p \rangle + \langle q \rangle$. The length of an $m \times n$ matrix A (or a vector) is the sum $\langle A \rangle := \sum_{i,j} \langle a_{i,j} \rangle$ of the lengths of its entries. Note that the length of A is no smaller than the number of entries, $\langle A \rangle \geq mn$. Therefore, when A is, say, part of an input to an algorithm, with m and n not fixed, the length $\langle A \rangle$ already incorporates mn , and so we will typically not account additionally for m, n directly. But sometimes we will also emphasize n as part of the input length. Similarly, the length of a finite set S of numbers, vectors, or matrices is the sum of lengths of its elements and hence, since $\langle S \rangle \geq |S|$, automatically accounts for its cardinality. Some input numbers affect the running time of some algorithms through their unary presentation, resulting in so-called “pseudo-polynomial” running time. The *unary length* of an integer number $z \in \mathbb{Z}$ is the number $|z| + 1$ of bits in its unary representation (again, an extra bit for the sign). The unary length of a rational number, vector, matrix, or finite set of such objects is defined again as the sums of lengths of their numerical constituents, and is again no smaller than the number of such numerical constituents. Often part of the input is presented by oracles. Then the running time counts also the number of oracle queries. An oracle algorithm is *polynomial time* if its running time, including the number of oracle queries, is polynomial in the length of the input.

Next, we make some basic definitions concerning matroids and set some associated notation; for matroid theory, see [14] or [17]. A *matroid* M is described by giving a finite *ground set* $\mathcal{E}(M)$ and a nonempty set $\mathcal{B}(M)$ of subsets of $\mathcal{E}(M)$ called the set of *bases* of M , such that for every $B, B' \in \mathcal{B}(M)$ and $i \in B \setminus B'$ there is an $i' \in B'$ such that $B \setminus \{i\} \cup \{i'\} \in \mathcal{B}(M)$. A subset I of $\mathcal{E}(M)$ is *independent* in M if $I \subseteq B$ for some base $B \in \mathcal{B}(M)$. The set of independent sets of M is denoted by $\mathcal{I}(M)$. Often it is convenient to let $\mathcal{E}(M) = N = \{1, 2, \dots, n\}$ for some positive integer n . The *rank* $\text{rank}(S)$ of a subset $S \subseteq \mathcal{E}(M)$ is the maximum cardinality $|I|$ of an $I \in \mathcal{I}(M)$ that is contained in S . The *rank* of the matroid is $\text{rank}(M) := \text{rank}(\mathcal{E}(M))$ and is equal to the cardinality $|B|$ of every base $B \in \mathcal{B}(M)$. An *independence oracle* for M is one that, queried on $I \subseteq \mathcal{E}(M)$, asserts whether I is in $\mathcal{I}(M)$. An independence oracle allows us to compute the rank of every $S \subseteq \mathcal{E}(M)$ as follows. Start with $I := \emptyset$. For each $j \in S$ (in any order) do: if $I \cup \{j\}$ is in $\mathcal{I}(M)$, then set $I := I \cup \{j\}$. Output $\text{rank}(S) := |I|$.

An important example of a matroid is the *graphic matroid* $M(G)$ of a graph G with $\mathcal{E}(M(G))$ being the edge set of G and $\mathcal{B}(M(G))$ equal to the set of edge sets of spanning forests of G . A further key example is the *vectorial matroid* of an $m \times n$ matrix A (over a field \mathbb{F}) with $\mathcal{B}(M)$ the set of subsets of indices of maximal linearly-independent subsets of columns of A . Throughout, when treating complexity issues, we assume that \mathbb{F} is the field \mathbb{Q} of rationals, that A has integer components, and that we do arithmetic over \mathbb{Q} . A *uniform matroid* is any matroid that is isomorphic to the matroid $\mathcal{U}_{m,n}$ having ground set $N = \{1, \dots, n\}$ and having all m -subsets of N as bases. If M_1 and M_2 are matroids with disjoint ground sets, then their *direct sum* $M_1 \oplus M_2$ has $\mathcal{E}(M_1 \oplus M_2) := \mathcal{E}(M_1) \uplus \mathcal{E}(M_2)$ and $\mathcal{B}(M_1 \oplus M_2) := \{B_1 \uplus B_2 : B_1 \in \mathcal{B}(M_1), B_2 \in \mathcal{B}(M_2)\}$. A *partition matroid* is any matroid that is a direct sum of uniform matroids $\oplus_{i=1}^r \mathcal{U}_{m_i, n_i}$ (with the ground sets of the \mathcal{U}_{m_i, n_i} labeled to be pairwise disjoint). If $m_i = m$ and all $n_i = k$ for all i , then we write $\mathcal{U}_{m,k}^r$ for this r -fold sum of $\mathcal{U}_{m,k}$.

It is well known that all graphic matroids and uniform matroids are vectorial. Furthermore, any partition matroid that is the direct sum $\oplus_{i=1}^r \mathcal{U}_{1,n_i}$ of rank-1 uniform matroids is graphic: it is the matroid of the graph obtained from any forest on r edges by replacing the i th edge by n_i parallel copies for $i = 1, \dots, r$. In particular, $\mathcal{U}_{1,k}^r$ is a graphic matroid for any positive k and r .

2.2. Preparation. Here we provide preparatory ingredients which will be used in algorithms in sections 3 and 4. First, we record for later the following statement, which follows directly from the definitions.

PROPOSITION 2.1. *Consider n -element matroid M , weights $w_1, \dots, w_d \in \mathbb{Z}^n$, and $f : \mathbb{Z}^d \rightarrow \mathbb{R}$. Put*

$$U := \{W(B) : B \in \mathcal{B}(M)\} = \{u \in \mathbb{Z}^d : u = W(B) \text{ for some base } B \in \mathcal{B}(M)\}.$$

Then the optimal objective value of the corresponding nonlinear matroid optimization problem satisfies

$$f^* = \min \{f(u) : u \in U\}.$$

In light of this viewpoint, with respect to the definitions of U and f^* from Proposition 2.1, an *optimal W -image* is any $u \in U$ satisfying $f(u) = f^*$.

Thus, the problem of computing f^* reduces to that of constructing the set U of W -images of bases, and then extracting an optimal W -image from U . This really is the crucial component of the solution of the nonlinear matroid optimization problem. While the cardinality of $U = \{W(B) : B \in \mathcal{B}(M)\}$ may be polynomial under suitable assumptions on the data, its direct computation by computing $W(B)$ for every base is prohibitive since the number of matroid bases is typically exponential in n . Instead, we will construct a finite superset Z of “potential” W -images of bases, satisfying $U \subseteq Z \subseteq \mathbb{Z}^d$, and then filter U out of Z . However, this is not an easy task either: deciding if a given $u \in \mathbb{Z}^d$ satisfies $u = W(B)$ for some base B is NP-complete already for fixed $d = 1$ and uniform matroids or partition matroids that are the direct sums of rank-1 uniform matroids; see Proposition 2.5. The way the filtration of U out of Z is done is precisely the key difference between our two algorithms for nonlinear matroid optimization in sections 3 and 4.

Next, we demonstrate that finding an optimal base for a nonlinear matroid optimization problem can be reduced to finding an optimal W -image for a small number of subproblems. Consider data for a nonlinear matroid optimization problem, consisting of a matroid M , weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$. Each subset $S \subseteq N$ gives a *subproblem* of nonlinear matroid optimization as follows. The matroid of the subproblem is the *restriction* of M to S ; that is, the matroid $M.S$ on ground set S in which a subset $I \subseteq S$ is independent if and only if it is independent in M . Note that an independence oracle for the restriction matroid $M.S$ is realizable at once from that of M . The weight vectors of the subproblem are the restrictions of the original weight vectors to S . The function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ in the subproblem is the same as in the original problem. We have the following useful statement.

LEMMA 2.2. *The nonlinear matroid optimization problem of finding an optimal base of an n -element matroid is reducible in time polynomial in n to finding an optimal W -image for $n + 1$ subproblems.*

Proof. Denote by $u^*(S)$ the optimal W -image for the subproblem on $S \subseteq N$. Now compute an optimal base for the original problem, by computing an optimal W -image for $n + 1$ such subproblems as follows.

```

Start with  $S := N$ ;
Compute  $m := \text{rank}(S)$ ;
Compute an optimal  $W$ -image  $u^* := u^*(N)$  of the original problem;
for  $j=1, 2, \dots, n$  do
    Compute  $\text{rank}(S \setminus \{j\})$ ;
    Compute an optimal  $W$ -image  $u^*(S \setminus \{j\})$ ;
    if  $\text{rank}(S \setminus \{j\}) = m$  and  $f(u^*(S \setminus \{j\})) = f(u^*)$  then set  $S := S \setminus \{j\}$ ;
end
return  $B := S$ ;
    
```

It is not hard to verify that the set B obtained is indeed an optimal base for the original problem. \square

2.3. Limitations. Here we provide various intractability statements about the nonlinear matroid optimization problem and some of its relatives. In particular, we show that, if the weights are encoded in binary, then even the 1-dimensional problem, namely with fixed $d = 1$, over any matroid given explicitly or by an oracle, requires examining the objective value of *every* base, and hence cannot be solved in polynomial time.

It is convenient to define a certain class of rank k matroids on $2k$ elements, so as to generalize the uniform matroid $\mathcal{U}_{k,2k}$ and the partition matroids $\mathcal{U}_{1,2}^k$. For some $r, 1 \leq r \leq k$, partition $K = \{1, \dots, k\}$ into r parts as $\uplus_{i=1}^r K_i$. Correspondingly, let $\bar{K}_i := \{\bar{j} : j \in K_i\}$. Let $k_i = |K_i| = |\bar{K}_i|$. For $i = 1, \dots, r$, let \mathcal{M}_i be a uniform matroid of rank k_i on ground set $K_i \cup \bar{K}_i$ (so $\mathcal{M}_i \cong \mathcal{U}_{k_i,2k_i}$). Let $\mathcal{M}_{r,k} := \oplus_{i=1}^r \mathcal{M}_i$. Observe that $\mathcal{M}_{1,k} \cong \mathcal{U}_{k,2k}$ (which is uniform) and $\mathcal{M}_{k,k} \cong \mathcal{U}_{1,2}^k$ (which is graphic), so *hardness results with respect to the matroid classes $\mathcal{M}_{r,k}$ apply to uniform and graphic matroids*. We note and will soon use that for any $r, 1 \leq r \leq k, |\mathcal{B}(\mathcal{M}_{r,k})|$ is not bounded by any polynomial in $|\mathcal{E}(\mathcal{M}_{r,k})| = 2k$.

PROPOSITION 2.3. *Computing an optimal solution of the 1-dimensional nonlinear matroid optimization problem over any matroid M , given explicitly or by an oracle, on n -element ground sets, and a univariate function f presented by a comparison oracle, cannot be done in polynomial time. In particular, with the single weight vector $w := (1, 2, 4, \dots, 2^{n-1})$, solution of the nonlinear matroid optimization problem requires examining $f(W(B))$ for each of the $|\mathcal{B}(M)|$ bases of M . In particular, for each $r, 1 \leq r \leq k$, the problem cannot be solved in polynomial time for the class of matroids $\mathcal{M}_{r,k}$.*

Proof. The weights $w(S) = \sum_{j \in S} 2^{j-1}$ of the 2^n subsets $S \subseteq N$ attain precisely all 2^n distinct values $0, 1, \dots, 2^n - 1$. Since the function f is arbitrary, this implies that the objective value $f(W(B))$ of each base B can be arbitrary. Therefore, if the value $f(W(B))$ of some base B is not compared against, it may be that this value is the unique minimum one and the nonlinear matroid optimization problem cannot be correctly solved. The final remark of the proposition follows since, for every $r, |\mathcal{B}(\mathcal{M}_{r,k})|$ is not bounded by any polynomial in $|\mathcal{E}(\mathcal{M}_{r,k})| = 2k$. \square

PROPOSITION 2.4. *Computing an optimal solution of the nonlinear matroid optimization problem in variable dimension $d = n$, over any matroid M , with $\{0, 1\}$ -valued weights, the i th weight being the standard unit vector $w_i := \mathbf{1}_i$ in \mathbb{Z}^n for all i , and with $f : \mathbb{Z}^n \rightarrow \mathbb{R}$ a function presented by a comparison oracle, requires examining*

$f(W(B))$ for each of the $|\mathcal{B}(M)|$ bases of M . In particular, for each r , $1 \leq r \leq k$, the problem cannot be solved in polynomial time for the class of matroids $\mathcal{M}_{r,k}$.

Proof. The W -images $W(B) = (w_1(B), \dots, w_n(B))$ of the 2^n subsets $B \subseteq N$ attain precisely all 2^n distinct vectors in $\{0, 1\}^n$. Since the function f is arbitrary, this implies that the objective value $f(W(B))$ of each base can be arbitrary. The rest of the argument is as in the proof of Proposition 2.3. \square

Consider nonlinear matroid optimization with a matroid M , weights $w_1, \dots, w_d \in \mathbb{Z}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$. As explained in section 2.2, a crucial component in solving the problem is to identify W -images of bases; that is, points $u \in \mathbb{Z}^d$ satisfying $u = W(B)$ for some $B \in \mathcal{B}(M)$. The following proposition shows that, with binary-encoded weights, both the nonlinear matroid optimization problem with explicitly given univariate convex quadratic function f and the problem of deciding if a given u is a W -image of some base, are intractable already for fixed $d = 1$ and uniform matroids or partition matroids that are the direct sums of rank-1 uniform matroids.

PROPOSITION 2.5. *Given matroid M , a single nonnegative weight vector $w \in \mathbb{N}^n$, and nonnegative integer $u \in \mathbb{N}$, encoded in binary, the following problems are NP-complete, when already restricted to the class of matroids $\mathcal{M}_{r,k}$, for any r , $1 \leq r \leq k$:*

1. *Determining whether $u = W(B) = \sum_{j \in B} w_j$ for some base $B \in \mathcal{B}(M)$.*
2. *Determining whether the optimal objective value is zero for the 1-dimensional nonlinear matroid optimization problem over M , with the explicit convex univariate function $f(y) := (y - u)^2$.*

Proof. The NP-complete *subset-sum problem* is to decide, given $a_0, a_1, \dots, a_k \in \mathbb{N}$, whether there is a subset $S \subseteq K = \{1, \dots, k\}$ with $\sum_{j \in S} a_j = a_0$. Given such a_i , let $u := a_0$, and let $w := (a_1, \dots, a_k, 0, \dots, 0) \in \mathbb{N}^K \times \mathbb{N}^{\bar{K}}$. Then, for any r , a base B of $\mathcal{M}_{r,k}$ satisfies $W(B) = u$ if and only if $S := B \cap K$ satisfies $\sum_{j \in S} a_j = a_0$. This reduces the subset-sum problem to the problem considered in the first part of the proposition, showing that it is indeed NP-complete.

For the second part, note that the objective value $f(W(B)) = (W(B) - u)^2$ of every base B is nonnegative, and B has $f(W(B)) = 0$ if and only if $W(B) = u$. Thus, the optimal objective value is zero if and only if there is a base with $W(B) = u$. So the problem in the first part of the proposition reduces to the problem in the second part, showing the latter to be NP-complete as well. \square

3. Arbitrary matroids. In this section we develop a combinatorial algorithm for nonlinear matroid optimization that runs in polynomial time for any matroid presented by an independence oracle, provided that the number p of distinct values taken by the entries $w_{i,j}$ of the weight vectors is fixed. In particular, the algorithm applies to $\{0, 1\}$ -valued weight vectors as well as to $\{0, 1, \dots, p\}$ -valued weight vectors for any fixed p .

As explained in section 2.2, we will filter the set $U = \{W(B) : B \in \mathcal{B}(M)\}$ of W -images of bases out of a suitable superset Z . For this, we next show how to efficiently decide if a given $u \in \mathbb{Z}^d$ satisfies $u = W(B)$ for some $B \in \mathcal{B}(M)$. We start with $\{0, 1\}$ -valued W -images with pairwise-disjoint supports.

LEMMA 3.1. *There is an algorithm that, given matroid M presented by an independence oracle on the n -element ground set N , weight vectors $w_1, \dots, w_d \in \{0, 1\}^n$ with pairwise-disjoint supports, and $u \in \mathbb{N}^d$, determines if M has a base B with W -image $W(B) = u$, in time polynomial in n and $\langle u \rangle$.*

Proof. For each base B of M and for each $i = 1, \dots, d$ we have $w_i(B) = |B \cap \text{supp}(w_i)|$. Therefore, a base B has $W(B) = u$ if and only if $|B \cap \text{supp}(w_i)| = u_i$ for $i = 1, \dots, d$. So we may and do assume $\sum_{i=1}^d u_i \leq \text{rank}(M)$ and $u_i \leq |\text{supp}(w_i)|$ for

all i else M has no base with $W(B) = u$. Let

$$\mathcal{B}' := \left\{ B \subseteq N : |B \cap \text{supp}(w_i)| = u_i, \quad i = 1, \dots, d, \right. \\ \left. |B \cap \left(N \setminus \bigcup_{i=1}^d \text{supp}(w_i) \right)| = \text{rank}(M) - \sum_{i=1}^d u_i \right\}.$$

It is easy to see that $\mathcal{B}' = \mathcal{B}(M')$ is the set of bases of a partition matroid M' on ground set N , for which an independence oracle is efficiently realizable. Moreover, M has a base B with $W(B) = u$ if and only if $\mathcal{B}(M) \cap \mathcal{B}(M')$ is nonempty. These observations justify the following algorithm:

```

if  $\sum_{i=1}^d u_i \leq \text{rank}(M)$  or  $u_i > |\text{supp}(w_i)|$  for some  $i = 1, \dots, d$  then return
NO;
Determine if  $\mathcal{B}(M) \cap \mathcal{B}(M')$  is nonempty by computing a max-cardinality
 $S \in \mathcal{I}(M) \cap \mathcal{I}(M')$ ;
if  $|S| = \text{rank}(M)$ ;
then
    return YES and  $B := S$ ;
else
    return NO;
end
    
```

Computing a max-cardinality $S \in \mathcal{I}(M) \cap \mathcal{I}(M')$ can be efficiently carried out using a maximum-cardinality matroid-intersection algorithm; see, e.g., [9] or [10] and the references therein. \square

Next, we consider weight vectors for which the number p of distinct $w_{i,j}$ values is fixed. So, we assume that $w_1, \dots, w_d \in \{a_1, \dots, a_p\}^n$ for arbitrary given integer numbers a_1, \dots, a_p . Note that the a_i can vary and be very large, since they affect the running time through their binary length $\langle a_i \rangle$.

LEMMA 3.2. *For every fixed d and p , there is an algorithm that, given matroid M presented by an independence oracle on ground set N , integers a_1, \dots, a_p , weight vectors $w_1, \dots, w_d \in \{a_1, \dots, a_p\}^n$, and $u \in \mathbb{N}^d$, decides if M has a base B with $W(B) = u$ in time polynomial in n , $\max \langle a_i \rangle$, and $\langle u \rangle$.*

Proof. Let $V := \{a_1, \dots, a_p\}^d$, and let Q be the $d \times p^d$ pattern matrix having columns that are all of the p^d points in V . Let, as usual, W be the $d \times n$ matrix with rows w_1, \dots, w_d . For $j = 1, \dots, n$, let w^j denote the j th column of W . We will exploit the fact that, no matter how large n is, the columns w^j of W all lie in the fixed set V —so the number of distinct columns w^j of W is limited.

Define a $p^d \times n$ selector matrix \widehat{W} , having rows \widehat{w}_v indexed by V , columns \widehat{w}^j indexed by N , and

$$\widehat{w}_{v,j} := \begin{cases} 1 & \text{if } w^j = v, \\ 0 & \text{otherwise,} \end{cases}$$

for $v \in V, j \in N$. Note that each column \widehat{w}^j of \widehat{W} is a standard unit vector, selecting the unique pattern (i.e., column) of V that agrees with the column w^j of W . It should be clear that the rows of \widehat{W} , namely the \widehat{w}_v , lie in $\{0, 1\}^n$ and have pairwise-disjoint supports—this will enable us to appeal to Lemma 3.1. We observe and will make use of the fact that the weight matrix W factors as $W = Q\widehat{W}$. Therefore, the W -image and

\widehat{W} -image of a base B satisfy $W(B) = Q\widehat{W}(B)$. This implies that there exists a base $B \in \mathcal{B}(M)$ with $W(B) = u$ if and only if for some p^d -dimensional vector \widehat{u} satisfying $u = Q\widehat{u}$ there exists a base $B \in \mathcal{B}(M)$ satisfying $\widehat{W}(B) = \widehat{u}$. Since \widehat{W} is $\{0, 1\}$ -valued, any such vector $\widehat{u} = \widehat{W}(B)$ must lie in $\{0, \dots, m\}^{p^d}$, where $m := \text{rank}(M)$. Therefore, checking if there is a base $B \in \mathcal{B}(M)$ with $W(B) = u$ reduces to going over all vectors $\widehat{u} \in \{0, \dots, m\}^{p^d}$, and for each vector \widehat{u} checking if $Q\widehat{u} = u$ and if there is a base B satisfying $\widehat{W}(B) = \widehat{u}$. This justifies the following algorithm:

```

let  $Q$  be the  $d \times p^d$  pattern matrix, and let  $\widehat{W}$  be the selector matrix (both
determined by  $W$ );
for  $\widehat{u} \in \{0, 1, \dots, m\}^{p^d}$  do
  if  $Q\widehat{u} = u$  then
    if there is a base  $B \in \mathcal{B}(M)$  with  $\widehat{W}(B) = \widehat{u}$  then return  $B$ ;
  end
end
return NO;

```

Since d and p are fixed and $m \leq n$, the number $(m+1)^{p^d}$ of such potential vectors \widehat{u} is polynomial in the data. For each such vector \widehat{u} , checking if $Q\widehat{u} = u$ is easily done by direct multiplication; and checking if there exists a base $B \in \mathcal{B}(M)$ satisfying $\widehat{W}(B) = \widehat{u}$ can be done in polynomial time using the algorithm of Lemma 3.1 applied to the matroid M , the $\hat{d} := p^d$ weight vectors \widehat{w}_v , $v \in V$ (the $\{0, 1\}$ -valued rows of the matrix \widehat{W} , having pairwise-disjoint supports), and the vector \widehat{u} . \square

We are now in position to solve the nonlinear optimization problem over a matroid that is presented by an independence oracle.

THEOREM 1.1. *For every fixed d and p , there is an algorithm that, given a matroid M presented by an independence oracle on the n -element ground set N , integers $a_1, \dots, a_p \in \mathbb{Z}$, weight vectors $w_1, \dots, w_d \in \{a_1, \dots, a_p\}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the nonlinear matroid optimization problem in time that is polynomial in n and $\max\langle a_i \rangle$.*

Proof. We have three major steps.

1. First, under the hypotheses of the theorem, assume that in polynomial time we can calculate an optimal W -image for the problem. Then, for every subset $S \subseteq N$, an optimal W -image for the subproblem on S can be computed in polynomial time, since the entries of the restrictions of w_1, \dots, w_d to S also attain values in $\{a_1, \dots, a_p\}$. By Lemma 2.2 this implies that an optimal base can be found and the nonlinear matroid optimization problem solved in polynomial time. So, it remains to show that in polynomial time we can calculate an optimal W -image for the problem.
2. To accomplish this, we first show how to compute the set U of W -images of bases of M , by working with an appropriately defined superset Z of U . Let $m := \text{rank}(M)$. Consider any $i = 1, \dots, d$ and any m -subset B of N . Then, since $w_{i,j} \in \{a_1, \dots, a_p\}$ for all j , we have that, for some nonnegative integers $\lambda_{i,1}, \dots, \lambda_{i,p}$ with $\sum_{k=1}^p \lambda_{i,k} = m$,

$$w_i(B) = \sum_{j \in B} w_{i,j} = \sum_{k=1}^p \lambda_{i,k} a_k.$$

Therefore, we find that the set U of W -images of bases satisfies

$$\begin{aligned} U &= \{W(B) : B \in \mathcal{B}(M)\} \\ &\subseteq \{W(B) : B \subseteq N, |B| = m\} \\ &\subseteq Z := \left\{ \sum_{k=1}^p \lambda_k a_k : \lambda \in \{0, 1, \dots, m\}^p, \sum_{k=1}^p \lambda_k = m \right\}^d. \end{aligned}$$

These observations justify the following algorithm to compute the set U of W -images of bases:

```

Compute  $m := \text{rank}(M)$  and let  $a := (a_1, \dots, a_p)$ ;
Start with  $Z := \emptyset$ ;
for  $\Lambda \in \{0, 1, \dots, m\}^{d \times p}$  do
    if  $\Lambda \mathbf{1} = m \mathbf{1}$  then let  $Z := Z \cup \{\Lambda a\}$ ;
end
Start with  $U := \emptyset$ ;
for  $u \in Z$  do
    if there is a base  $B \in \mathcal{B}(M)$  with  $W(B) = u$  then let
         $U := U \cup \{u\}$ ;
end
return  $U$ ;
    
```

Observe that, since d and p are fixed, $|Z| \leq |\{0, 1, \dots, m\}^{d \times p}| = (m + 1)^{pd}$ is polynomially bounded in $m \leq n$ and hence so are the numbers of iterations in each of the “for” loops of the algorithm. Also note that, in each iteration of the second loop, we can apply the algorithm of Lemma 3.2 to determine, in polynomial time, whether there is a base $B \in \mathcal{B}(M)$ with $W(B) = u$. Therefore, we can efficiently determine U .

3. By repeatedly querying the comparison oracle of f on $|U| - 1$ suitable pairs of points in U , we obtain a $u^* \in U$ that satisfies $f(u^*) = \min\{f(u) : u \in U\}$, which by Proposition 2.1 is an optimal W -image.

Finally, by embedding steps 2 and 3 above as subroutines to solve the $n + 1$ restrictions of the problem to suitable subsets $S \subseteq N$ in step 1, we obtain our desired algorithm. \square

4. Vectorial matroids. In this section we develop an algebraic algorithm for nonlinear matroid optimization over vectorial matroids. It applies to any matroid that is vectorial over an ordered field. For matroids that are vectorial over the rationals \mathbb{Q} , it runs in time polynomial in the binary length $\langle A \rangle$ of the matrix A representing the matroid and in the unary length $\max |w_{i,j}|$ of the weights. It is much more efficient than the combinatorial algorithm of section 3 and applies to weights with an unlimited number of different values $w_{i,j}$ of entries.

First, we show that it suffices to deal with nonnegative weight vectors.

LEMMA 4.1. *The nonlinear matroid optimization problem with arbitrary integer weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$ is polynomial-time reducible to the special case of nonnegative vectors $w_1, \dots, w_d \in \mathbb{N}^n$.*

Proof. Consider a matroid M , integer weights $w_1, \dots, w_d \in \mathbb{Z}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$. Let $m := \text{rank}(M)$ and $\omega := \max |w_{i,j}|$. Define nonnegative weights by $w'_{i,j} := w_{i,j} + \omega$ for all i, j , and define a new function $f' : \mathbb{Z}^d \rightarrow \mathbb{R}$ by $f'(u_1, \dots, u_d) := f(u_1 - m\omega, \dots, u_d - m\omega)$ for every $u = (u_1, \dots, u_d) \in \mathbb{R}^d$. Note that the unary length

of each new weight $w'_{i,j}$ is at most twice the maximum unary length of the original weights $w_{i,j}$, and a comparison oracle for f' is easily realizable from a comparison oracle for f . Then for every base B and for each $i = 1, \dots, d$, we have

$$w'_i(B) = \sum_{j \in B} w'_{i,j} = \sum_{j \in B} (w_{i,j} + \omega) = \left(\sum_{j \in B} w_{i,j} \right) + m\omega = w_i(B) + m\omega,$$

implying the following equality between the new and original objective function values:

$$f'(w'_1(B), \dots, w'_d(B)) = f'(w_1(B) + m\omega, \dots, w_d(B) + m\omega) = f(w_1(B), \dots, w_d(B)).$$

Therefore, a base $B \in \mathcal{B}(M)$ is optimal for the nonlinear matroid optimization problem with data M, w_1, \dots, w_d and f if and only if it is optimal for the problem with M, w'_1, \dots, w'_d and f' . \square

So we assume henceforth that the weights are nonnegative. As explained in section 2.2 and carried out in section 3, we will filter the set $U = \{W(B) : B \in \mathcal{B}(M)\}$ of W -images of bases out of a suitable superset Z . However, instead of checking if $u \in U$ for one point $u \in Z$ after the other, we will filter here the entire set U out of Z at once. We proceed to describe this procedure.

Let A be an $m \times n$ integer matrix of full row rank m , and let M be the vectorial matroid of A . Note that $m = \text{rank}(M)$. Let $w_1, \dots, w_d \in \mathbb{N}^n$ be nonnegative integer weight vectors, and let $\omega := \max w_{i,j}$. Then for each $i = 1, \dots, d$ and each m -subset B of N , we have $w_i(B) \in \{0, 1, \dots, m\omega\}$, and therefore

$$\begin{aligned} U &= \{W(B) : B \in \mathcal{B}(M)\} \subseteq \{W(B) : B \subseteq N, |B| = m\} \\ &\subseteq Z := \{0, 1, \dots, m\omega\}^d \subseteq \mathbb{N}^d. \end{aligned}$$

We will show how to filter the set U out of the above superset Z of potential W -images of bases. For each base $B \in \mathcal{B}(M)$, let $A_{.B}$ denote the nonsingular $m \times m$ submatrix of A consisting of those columns indexed by $B \subseteq N$. Define the following polynomial in d variables x_1, \dots, x_d :

$$(1) \quad g = g(x) := \sum_{u \in Z} g_u x^u := \sum_{u \in Z} g_u \prod_{k=1}^d x_k^{u_k},$$

where the coefficient g_u corresponding to $u \in Z$ is the nonnegative integer

$$(2) \quad g_u := \sum \{ \det^2(A_{.B}) : B \in \mathcal{B}(M), W(B) = u \}.$$

Now, $\det^2(A_{.B})$ is positive for every base $B \in \mathcal{B}(M)$. Thus, the coefficient g_u corresponding to $u \in Z$ is nonzero if and only if there exists a matroid base $B \in \mathcal{B}(M)$ with $W(B) = u$. So the desired set U is precisely the set of exponents of monomials x^u with nonzero coefficient in g . We record this for later use.

PROPOSITION 4.2. *Let M be the vectorial matroid of an $m \times n$ matrix A of rank m , let $w_1, \dots, w_d \in \mathbb{N}^n$, and let $g(x)$ be the polynomial in (1). Then $U := \{W(B) : B \in \mathcal{B}(M)\} = \{u \in Z : g_u \neq 0\}$.*

By Proposition 4.2, to compute U , it suffices to compute all coefficients g_u . Unfortunately, they cannot be computed directly from the definition (2), since this involves again checking exponentially many $B \in \mathcal{B}(M)$ —precisely what we are trying to avoid!

Instead, we will compute the g_u by interpolation. However, in order to do so, we need a way of evaluating $g(x)$ under numerical substitutions. We proceed to show how this can be efficiently accomplished.

Let X be the $n \times n$ diagonal matrix whose j th diagonal component is the monomial $\prod_{i=1}^d x_i^{w_{i,j}}$ in the variables x_1, \dots, x_d , that is, the matrix of monomials defined by

$$X := \text{diag} \left(\prod_{i=1}^d x_i^{w_{i,1}}, \dots, \prod_{i=1}^d x_i^{w_{i,n}} \right).$$

The following lemma will enable us to compute the value of $g(x)$ under numerical substitutions.

LEMMA 4.3. *For any $m \times n$ matrix A of rank m and nonnegative weights $w_1, \dots, w_d \in \mathbb{N}^n$ we have*

$$g(x) = \det(AXA^T).$$

Proof. By the classical Binet–Cauchy identity, for any two $m \times n$ matrices C, D of rank m we have $\det(CD^T) = \sum \{ \det(C_{\cdot B}) \det(D_{\cdot B}) : B \in \mathcal{B}(M) \}$. Applying this to $C := AX$ and $D := A$, we obtain

$$\begin{aligned} \det(AXA^T) &= \sum_{B \in \mathcal{B}(M)} \det((AX)_{\cdot B}) \det(A_{\cdot B}) = \sum_{B \in \mathcal{B}(M)} \prod_{j \in B} \prod_{i=1}^d x_i^{w_{i,j}} \det(A_{\cdot B}) \det(A_{\cdot B}) \\ &= \sum_{B \in \mathcal{B}(M)} \prod_{i=1}^d x_i^{w_i(B)} \det^2(A_{\cdot B}) = \sum_{u \in Z} \sum_{\substack{B \in \mathcal{B}(M): \\ W(B)=u}} \det^2(A_{\cdot B}) \prod_{i=1}^d x_i^{u_i} \\ &= \sum_{u \in Z} g_u x^u = g(x). \quad \square \end{aligned}$$

Lemma 4.3 paves the way for computing the coefficients of the polynomial $g(x) = \sum_{u \in Z} g_u x^u$ by interpolation. We will choose sufficiently many suitable points on the moment curve in \mathbb{R}^Z , substitute each point into x , and evaluate $g(x)$ using the lemma. We will then solve the system of linear equations for the coefficients g_u . The next lemma describes the details and shows that this can be done efficiently.

LEMMA 4.4. *For every fixed d , there is an algorithm that, given any $m \times n$ matrix A of rank m and weights $w_1, \dots, w_d \in \mathbb{N}^n$, computes all coefficients g_u of $g(x)$ in time polynomial in $\max w_{i,j}$ and $\langle A \rangle$.*

Proof. Let $\omega := \max w_{i,j}$ and $s := m\omega + 1$. Then a superset of potential W -images of bases is $Z := \{0, 1, \dots, m\omega\}^d$ and satisfies $|Z| = s^d$. For $t = 1, 2, \dots, s^d$, let $X(t)$ be the numerical matrix obtained from X by substituting $t^{s^{i-1}}$ for x_i , $i = 1, \dots, d$. By Lemma 4.3 we have $g(x) = \det(AXA^T)$, and therefore we obtain the following system of s^d linear equations in the s^d variables g_u , $u \in Z$:

$$\begin{aligned} \det(AX(t)A^T) &= \det \left(A \text{diag}_j \left(\prod_{i=1}^d t^{w_{i,j} s^{i-1}} \right) A^T \right) = \sum_{u \in Z} g_u \prod_{i=1}^d t^{u_i s^{i-1}} \\ &= \sum_{u \in Z} t^{\sum_{i=1}^d u_i s^{i-1}} g_u, \quad t = 1, 2, \dots, s^d. \end{aligned}$$

As u runs through Z , the sum $\sum_{i=1}^d u_i s^{i-1}$ attains precisely all $|Z| = s^d$ distinct values $0, 1, \dots, s^d - 1$. This implies that, under the total order of the points u in Z by increasing value of $\sum_{i=1}^d u_i s^{i-1}$, the vector of coefficients of the g_u in the equation corresponding to t is precisely the point $(t^0, t^1, \dots, t^{s^d-1})$ on the moment curve in $\mathbb{R}^Z \cong \mathbb{R}^{s^d}$. Therefore, the equations are linearly independent and hence the system can be uniquely solved for the g_u .

These observations justify the following algorithm to compute the g_u , $u \in Z$:

```

Compute  $m := \text{rank}(A)$ ;
let  $\omega := \max w_{i,j}$ , and let  $s := m\omega + 1$ ;
let  $X := \text{diag}_j \left( \prod_{i=1}^d x_i^{w_{i,j}} \right)$ ;
for  $t = 1, 2, \dots, s^d$  do
    let  $X(t)$  be the numerical matrix obtained by substituting  $t^{s^{i-1}}$  for  $x_i$ ,
         $i = 1, 2, \dots, d$ , in  $X$ ; Compute  $\det(AX(t)A^T)$ ;
end
let  $Z := \{0, 1, \dots, m\omega\}^d$ ;
Compute and return the unique solution  $g_u$ ,  $u \in Z$ , of the square linear
system:

$$\det(AX(t)A^T) = \sum_{u \in Z} t^{\sum_{i=1}^d u_i s^{i-1}} g_u, \quad t = 1, 2, \dots, s^d.$$


```

We now show that this system can be solved in polynomial time. First, the number of equations and indeterminates is $s^d = (m\omega + 1)^d$ and hence polynomial in the data. Second, for each $i, j = 1, \dots, n$ and $t = 1, 2, \dots, s^d$, it is easy to see that the (i, j) th entry of $AX(t)A^T$ satisfies

$$\left| \sum_{h=1}^n a_{i,h} \prod_{k=1}^d t^{s^{k-1} w_{k,h}} a_{j,h} \right| \leq \sum_{h=1}^n |a_{i,h} a_{j,h}| p^{ds^d \max w_{k,h}},$$

implying that the binary length $\langle AX(t)A^T \rangle$ of $AX(t)A^T$ is polynomially bounded in the data as well.

It follows that $\det(AX(t)A^T)$ can be computed in polynomial time by Gaussian elimination for all t , and the system of equations can indeed be solved for the g_u in polynomial time. We further note that the system of equations is a Vandermonde system, so the number of arithmetic operations needed to solve it is just quadratic in its dimensions. \square

We can now efficiently solve the nonlinear optimization problem over vectorial matroids with unary weights.

THEOREM 1.3. *For every fixed d , there is an algorithm that, given integer $m \times n$ matrix A , weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the nonlinear optimization problem over the (real) vectorial matroid of A in time polynomial in $\langle A \rangle$ and $\max |w_{i,j}|$.*

Proof. Let M be the vectorial matroid of A . Recall that linear-algebraic operations on A can be done in polynomial time, say by Gaussian elimination. Dropping some rows of A if necessary without changing M , we may assume that A has rank m . An independence oracle for M is readily realizable since $S \subseteq N$ is independent in M precisely when the columns of A indexed by S are linearly independent. Applying, if necessary, the procedure of Lemma 4.1 and adjusting the weights while at most doubling the unary length of the maximum weight, we may also assume that the weights are nonnegative.

We will show how to compute an optimal W -image u^* in polynomial time. This will also imply that, for every subset $S \subseteq N$, an optimal W -image for the subproblem on S can be computed in polynomial time. By Lemma 2.2 this will show that an optimal base can be found and the nonlinear matroid optimization problem solved in polynomial time.

Let $\omega := \max w_{i,j}$ and consider the superset $Z := \{0, 1, \dots, m\omega\}^d$ of potential W -images of bases and the polynomial $g(x) = \sum_{u \in Z} g_u x^u$ as defined in (1) and (2). By Proposition 4.2 we have

$$U = \{W(B) : B \in \mathcal{B}(M)\} = \{u \in Z : g_u \neq 0\}.$$

Applying now the algorithm of Lemma 4.4, we can compute in polynomial time the right-hand side and hence the left-hand side, providing the filtration of the set U of W -images of bases out of Z . By repeatedly querying the comparison oracle of f on suitable pairs of points in U , we obtain a $u^* \in U$ satisfying $f(u^*) = \min\{f(u) : u \in U\}$, which by Proposition 2.1 is the desired optimal W -image. \square

5. Experimental design. We now discuss applications of nonlinear matroid optimization to experimental design. For general information on experimental design, see, e.g., the monograph [15] and the references therein. As outlined in the introduction, we consider the following rather general framework. We wish to learn an unknown system whose output y is an unknown function Φ of a multivariate input $x = (x_1, \dots, x_k) \in \mathbb{R}^k$. It is customary to call the input variables x_i *factors* of the system. We perform several experiments. Each experiment i is determined by a point $p_i = (p_{i,1}, \dots, p_{i,k})$ and consists of feeding the system with input $x := p_i \in \mathbb{R}^k$ and measuring the corresponding output $y_i := \Phi(p_i) \in \mathbb{R}$. Based on these experiments, we wish to *fit a model* for the system, namely, determine an estimation $\hat{\Phi}$ of Φ , that:

- lies in a prescribed class of functions;
- is consistent with the outcomes of the experiments;
- minimizes the *aberration*—a suitable criterion—among models in the class.

We concentrate on (multivariate) *polynomial models* defined as follows. Each nonnegative integer vector $\alpha \in \mathbb{N}^k$ serves as an *exponent* of a corresponding monomial $x^\alpha := \prod_{h=1}^k x_h^{\alpha_h}$ in the system input $x \in \mathbb{R}^k$. Each finite subset $B \subset \mathbb{N}^k$ of exponents provides a *model* for the system, namely a polynomial *supported on B* , i.e., having monomials with exponents in B only,

$$\Phi_B(x) = \sum_{\alpha \in B} c_\alpha x^\alpha,$$

where the c_α are real coefficients that need to be determined from the measurements by interpolation.

We assume that the set of design points $\{p_1, \dots, p_m\} \subset \mathbb{R}^k$ is prescribed. Indeed, in practical applications, it may be impossible or too costly to conduct experiments involving arbitrarily chosen points. The problem of choosing the design (termed the *inverse problem* in the statistics literature; see [2] and the references therein), is of interest in its own right, and its computational aspects will be considered elsewhere. We collect the design points in an $m \times k$ *design matrix* P . Thus, the i th row of this matrix is the i th design point p_i . A model $B \subset \mathbb{N}^k$ is *identifiable* by a design P if for any possible measurement values $z_i = \Phi(p_i)$ at the design points, there is a unique polynomial $\Phi_B(x)$ supported on B that interpolates Φ , that is, satisfies $\Phi_B(p_i) = z_i = \Phi(p_i)$ for every design point $p_i = (p_{i,1}, \dots, p_{i,k})$.

Among models identifiable by a given design, we wish to determine one that is best under a suitable criterion. Roughly speaking, common criteria ask for *low degree polynomials*. To make this precise, for each identifiable model B , consider the following *total degree vector* whose i th entry is the total degree of variable x_i over all monomials supported on B :

$$\sum_{\alpha \in B} \alpha = \left(\sum_{\alpha \in B} \alpha_1, \dots, \sum_{\alpha \in B} \alpha_k \right).$$

Now, given any function $f : \mathbb{Z}^k \rightarrow \mathbb{R}$, the *aberration* of model B induced by f is defined to be

$$\mathcal{A}(B) := f \left(\sum_{\alpha \in B} \alpha \right).$$

The term *aberration* is the one used in the statistics literature in this context; see, e.g., [5, 18] and the references therein. We now give some concrete examples of functions providing useful aberrations.

Example 5.1 (some concrete useful aberrations).

- Consider the function $f(u) := \frac{1}{|B|}(u_1 + \dots + u_k)$. Then the aberration of model B is

$$\mathcal{A}(B) = \frac{1}{|B|} \sum_{\alpha \in B} \alpha_1 + \dots + \frac{1}{|B|} \sum_{\alpha \in B} \alpha_k = \frac{1}{|B|} \sum_{\alpha \in B} \sum_{i=1}^k \alpha_i,$$

which is the average total degree of monomials supported on B .

- Consider $f(u) := \frac{1}{|B|}(\pi_1 u_1 + \dots + \pi_k u_k)$ for some real weights π_1, \dots, π_k . Then

$$\mathcal{A}(B) = \pi_1 \frac{1}{|B|} \sum_{\alpha \in B} \alpha_1 + \dots + \pi_k \frac{1}{|B|} \sum_{\alpha \in B} \alpha_k$$

is the weighted average degree, allowing for preferences of some variables over others.

- Consider the function $f(u) := \frac{1}{|B|}(\max\{u_1, \dots, u_k\})$. Then the aberration of B is

$$\mathcal{A}(B) = \max \left\{ \frac{1}{|B|} \sum_{\alpha \in B} \alpha_1, \dots, \frac{1}{|B|} \sum_{\alpha \in B} \alpha_k \right\},$$

and is the maximum over variables of the average variable degree of monomials supported on B .

- More generally, consider $f(u) := \frac{1}{|B|}(\|\pi \cdot u\|_q) = \frac{1}{|B|} \left(\left(\sum_{i=1}^k |\pi_i u_i|^q \right)^{\frac{1}{q}} \right)$. Then the aberration of B is

$$\mathcal{A}(B) = \left\| \pi \cdot \left(\frac{1}{|B|} \sum_{\alpha \in B} \alpha \right) \right\|_q,$$

which is the l_q -norm of the weighted average degree vector of monomials supported on B .

We can now formally define the minimum-aberration model-fitting problem.

Minimum-aberration model-fitting problem. Given a design $P = \{p_1, \dots, p_m\}$ of m points in \mathbb{R}^k , a set $N = \{\beta_1, \dots, \beta_n\}$ of n potential exponents in \mathbb{N}^k , and a function $f : \mathbb{Z}^k \rightarrow \mathbb{R}$, find a model $B \subseteq N$ that is identifiable by P and is of minimum aberration

$$\mathcal{A}(B) = f \left(\sum_{\beta_j \in B} \beta_j \right).$$

Next, we demonstrate how to formulate the minimum-aberration model-fitting problem as a nonlinear matroid optimization problem. Consider the following $m \times n$ matrix A having rows indexed by P and columns indexed by N , defined by

$$a_{i,j} := p_i^{\beta_j} = \prod_{h=1}^k p_{i,h}^{\beta_{j,h}}, \quad i = 1, \dots, m, j = 1, \dots, n.$$

It can be verified that a model $B \subseteq N$ is identifiable by a design P if and only if the $m \times m$ matrix $A_{.B}$ is invertible. (In the terminology of algebraic geometry, the model B is identifiable if the congruence classes of the monomials $x^{\beta_1}, \dots, x^{\beta_m}$ form a basis for the quotient of the algebra of polynomials $\mathbb{R}[x_1, \dots, x_k]$ modulo the ideal of polynomials vanishing on the design points; see [3, 13] and the references therein for more on this.) If B is identifiable, then, given any vector of measurements $y \in \mathbb{R}^m$ at the design points, the vector of coefficients $c \in \mathbb{R}^m$ of the unique polynomial $\Phi_B(x) = \sum_{j=1}^m c_j \prod_{h=1}^k x_h^{\beta_{j,h}}$ supported on B that is consistent with the measurements is given by $c := (A_{.B})^{-1} y$.

If the rank of A is less than m , then no $B \subseteq N$ is identifiable, and the set N of potential exponents should be augmented with more exponents. So assume that A has rank m . Let M be the vectorial matroid of A , so that

$$\mathcal{B}(M) := \{B \subseteq N : B \text{ is identifiable by } P\}.$$

Now define k weights vectors $w_1, \dots, w_k \in \mathbb{N}^n$ by $w_{i,j} := \beta_{j,i}$ for $i = 1, \dots, k, j = 1, \dots, n$. Then the aberration of model B is

$$\mathcal{A}(B) = f \left(\sum_{\beta_j \in B} \beta_j \right) = f \left(\sum_{\beta_j \in B} w_{1,j}, \dots, \sum_{\beta_j \in B} w_{k,j} \right).$$

Thus, the aberration of a model B identifiable by the design P is precisely the objective function value of the base B in the nonlinear matroid optimization problem over the matroid M above, with $d := k$ and the weights $w_1, \dots, w_k \in \mathbb{N}^n$ as above, and with the given function $f : \mathbb{Z}^k \rightarrow \mathbb{R}$. Assuming that a comparison oracle for the function f can be realized, which is practically always true, and that the design points are rational so that they can be input and processed on a digital computer, we obtain the following corollary of Theorems 1.1 and 1.3.

COROLLARY 5.2. *For every fixed k , there is an algorithm that, given a rational design $P = \{p_1, \dots, p_m\}$ in \mathbb{R}^k , a set $N = \{\beta_1, \dots, \beta_n\}$ in \mathbb{N}^k , and a function $f : \mathbb{Z}^k \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the minimum-aberration model-fitting problem in time polynomial in $m, n, \langle P \rangle$, and $\max \beta_{i,j}$.*

It is very natural and common in practice to consider *hierarchical models*; that is, models B with the property that $\beta \leq \alpha \in B$ implies $\beta \in B$. In [3, 13], in the

context of the theory of Gröbner bases in commutative algebra, it was shown that the smallest set containing all m -point hierarchical models B (termed *staircases* therein) in \mathbb{N}^k is the following set, consisting of roughly $O(m \log m)$ points,

$$N := \left\{ \alpha \in \mathbb{N}^k : \prod_{h=1}^k (\alpha_h + 1) \leq m \right\}.$$

Thus, Corollary 5.2 will be typically applied with this set N as the set of potential monomial exponents.

We proceed to describe a more general useful class of aberrations that can be treated, which is naturally suggested by the nonlinear matroid optimization formulation. As before, we are given a design $P = \{p_1, \dots, p_m\}$ in \mathbb{R}^k and a set $N = \{\beta_1, \dots, \beta_n\}$ of potential exponents in \mathbb{N}^k . But now we are also given d weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$. The function f is now defined on \mathbb{R}^d rather than \mathbb{R}^k . The aberration induced by the weights and the function is now simply the objective function of the nonlinear matroid optimization problem, which for an identifiable model $B \subseteq N$ is given by

$$\mathcal{A}(B) := f(W(B)),$$

where W is the matrix with rows w_i . Note that aberrations of the type considered before can be recovered as a special case with $d := k$ and $w_{i,j} := \beta_{j,i}$ for all i, j . Here are a few useful examples.

Example 5.3 (some concrete useful generalized aberrations). Let $N = \{\beta_1, \dots, \beta_n\} \subset \mathbb{N}^k$ be any set of exponents. Let θ be a small positive integer, say $\theta = 1$ or $\theta = 2$, that will serve as a desired bound on the degrees of variables in monomials of the sought after models B contained in N .

- Let $d := 1$, and define the single weight vector $w_1 \in \mathbb{N}^n$ by

$$w_{1,j} := \begin{cases} 0 & \text{if } \beta_{j,i} \leq \theta \text{ for every } i = 1, \dots, k, \\ 1 & \text{otherwise,} \end{cases}$$

for $j = 1, \dots, n$. Then $\sum_{\beta_j \in B} w_{1,j}$ is the number of monomials supported on $B \subseteq N$ that do *not* meet the degree bound; in particular, for $\theta = 1$ it is the number of non square-free monomials. Taking $f : \mathbb{Z} \rightarrow \mathbb{R}$ to be the identity $f(u) := u$, the aberration $\mathcal{A}(B)$ of model B is the number of undesired monomials. In particular, an optimal model B has $\mathcal{A}(B) = 0$ if and only if the design admits an identifiable model with all variables in all monomials having degree at most θ .

- Now let $d := k$, and define weight vectors $w_1, \dots, w_k \in \mathbb{N}^n$ by

$$w_{i,j} := \begin{cases} 0 & \text{if } \beta_{j,i} \leq \theta, \\ 1 & \text{otherwise,} \end{cases}$$

for $i = 1, \dots, k$, $j = 1, \dots, n$. Then $\sum_{\beta_j \in B} w_{i,j}$ is the number of monomials supported on model $B \subseteq N$ for which variable x_i violates the degree bound θ . Defining $f : \mathbb{Z}^k \rightarrow \mathbb{R}$ by $f(u) := \max_{i=1}^k u_i$, we get that the aberration $\mathcal{A}(B)$ of model B is the maximum over variables of the number of monomials having x_i violating the degree bound θ . The optimal model will minimize the maximum violation.

We have the following generalized minimum-aberration model-fitting problem and corollary.

Generalized minimal-aberration model-fitting problem. Given a design $P = \{p_1, \dots, p_m\}$ in \mathbb{R}^k , a set $N = \{\beta_1, \dots, \beta_n\}$ of potential exponents in \mathbb{N}^k , weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$, and a function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$, find a model $B \subseteq N$ that is identifiable by P and is of minimum aberration

$$A(B) = f(W(B)) = f\left(\sum_{\beta_j \in B} w_{1,j}, \dots, \sum_{\beta_j \in B} w_{d,j}\right).$$

COROLLARY 5.4. *For every fixed k and d , there is an algorithm that, given any rational design $P = \{p_1, \dots, p_m\}$ in \mathbb{R}^k , any set $N = \{\beta_1, \dots, \beta_n\}$ of potential exponents in \mathbb{N}^k , weight vectors $w_1, \dots, w_d \in \mathbb{Z}^n$, and function $f : \mathbb{Z}^d \rightarrow \mathbb{R}$ presented by a comparison oracle, solves the generalized minimum-aberration model-fitting problem in time polynomial in $m, n, \langle P \rangle, \max \beta_{j,i}$, and $\max |w_{i,j}|$.*

REFERENCES

- [1] A. V. AHO, J. E. HOPCROFT, AND J. D. ULLMAN, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, MA, 1975.
- [2] A. C. ATKINSON, A. DONEV, AND R. TOBIAS, *Optimum experimental designs, with SAS*, Oxford Statistical Science Series, 34, Oxford University Press, Oxford, 2007.
- [3] E. BABSON, S. ONN, AND R. THOMAS, *The Hilbert zonotope and a polynomial time algorithm for universal Gröbner bases*, Adv. in Appl. Math., 30 (2003), pp. 529–544.
- [4] Y. BERSTEIN AND S. ONN, *Nonlinear bipartite matching*, Discrete Optim., 5 (2008), pp. 53–65.
- [5] A. FRIES AND W. G. HUNTER, *Minimum aberration 2^{k-p} designs*, Technometrics, 22 (1980), pp. 601–608.
- [6] M. R. GAREY AND D. S. JOHNSON, *Computers and Intractability*, W. H. Freeman, San Francisco, 1979.
- [7] R. HASSIN AND A. LEVIN, *An efficient polynomial time approximation scheme for the constrained minimum spanning tree problem using matroid intersection*, SIAM J. Comput., 33 (2004), pp. 261–268.
- [8] R. HASSIN AND A. TAMIR, *Maximizing classes of two-parameter objectives over matroids*, Math. Oper. Res., 14 (1989), pp. 362–375.
- [9] J. LEE, *A First Course in Combinatorial Optimization*, Cambridge Texts in Applied Mathematics, Cambridge University Press, Cambridge, UK, 2004.
- [10] J. LEE AND J. RYAN, *Matroid applications and algorithms*, INFORMS (formerly ORSA) J. Comput., 4 (1992), pp. 70–98.
- [11] S. ONN, *Convex matroid optimization*, SIAM J. Discrete Math., 17 (2003), pp. 249–253.
- [12] S. ONN AND U. G. ROTHBLUM, *Convex combinatorial optimization*, Discrete Comput. Geom., 32 (2004), pp. 549–566.
- [13] S. ONN AND B. STURMFELS, *Cutting corners*, Adv. in Appl. Math., 23 (1999), pp. 29–48.
- [14] J. G. OXLEY, *Matroid Theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1992.
- [15] G. PISTONE, E. RICCOMAGNO, AND H. P. WYNN, *Algebraic Statistics*, Monographs on Statistics and Applied Probability 89, Chapman & Hall/CRC, Boca Raton, FL, 2001.
- [16] A. SCHRIJVER, *Theory of Linear and Integer Programming*, John Wiley and Sons, Chichester, UK, 1986.
- [17] D. J. A. WELSH, *Matroid Theory*, Academic Press, London, 1976.
- [18] H. WU AND C. F. J. WU, *Clear two-factor interactions and minimum aberration*, Ann. Statist., 30 (2002), pp. 1496–1511.