Quadratic Programming is in NP*

Stephen A. Vavasis

TR 90-1099
February 1990

Department of Computer Science
Cornell University
Ithaca, NY 4853-7501

*This work supported by the Applied Mathematical Sciences Program (KC-04-02) of the Office of Energy Research of the U.S. Department of Energy under grant DE-FG02-86ER25013.A000 and in part by the U.S. Army Research Office through the Mathematical Sciences Institute at Cornell University.

Quadratic programming is in NP *

Stephen A. Vavasis
Department of Computer Science
Cornell University

February 16, 1990

Abstract

Quadratic programming is an important example of optimization with applications to engineering design, combinatorial optimization, game theory, and economics. Garey and Johnson [1979] state that quadratic programming is **NP**-hard. In this report we show that it lies in **NP**, thereby proving that it is **NP**-complete.

1 Quadratic programming is NP-hard.

Quadratic programming is the following problem. The input data is an $n \times n$ symmetric matrix H, an n-vector $\mathbf{c}$, an $m \times n$ matrix A and an n-vector $\mathbf{b}$. The problem is to find $\mathbf{x} \in \mathbb{R}^n$ to

$$\begin{array}{rl} \text{minimize} & \mathbf{x}^T H\mathbf{x} + \mathbf{c}^T\mathbf{x} \\ \text{subject to} & A\mathbf{x} \geq \mathbf{b}. \end{array}$$

In order to formulate this as a Turing Machine language-recognition problem, we assume that all of the numerical data (namely, H, $\mathbf{c}$, A, and $\mathbf{b}$)

*This work supported by the Applied Mathematical Sciences Program (KC-04-02) of the Office of Energy Research of the U.S. Department of Energy under grant DE-FG02-86ER25013.A000 and in part by the U.S. Army Research Office through the Mathematical Sciences Institute of Cornell University.

have integer entries. We also assume that a rational number K is part of the input. Then we ask the question, does there exist a point $\mathbf{x} \in \mathbb{R}^n$ such that $A\mathbf{x} \geq \mathbf{b}$ and $\mathbf{x}^T H\mathbf{x} + \mathbf{c}^T\mathbf{x} \leq K$? We call this problem QPL, for "quadratic programming language." We use the term "yes-instance" to denote a 5-tuple $(H, \mathbf{c}, A, \mathbf{b}, K)$ that is in the language, i.e., an instance for which the answer to the above question is "yes."

It was proved by Sahni [1974] that QPL is an **NP**-hard problem. It has apparently never been proved that QPL actually lies in **NP** (problem MP2 of Garey and Johnson [1979]. The purpose of this report is to provide that proof. For the remainder of this section, however, we give the proof that QPL is **NP**-hard by polynomially transforming SAT to QPL.

Let Q be an instance of conjunctive normal SAT, that is, a boolean formula with n variables $x_1, \ldots, x_n$ and m clauses. We produce a quadratic program $(H, \mathbf{c}, A, \mathbf{b})$ as follows. We denote the variables of the quadratic program by $y_1, \ldots, y_n$, one for each boolean variable. Linear constraints of the form $y_i \leq 1$ and $y_i \geq 0$ will make up the first $2n$ rows of A and $\mathbf{b}$. The goal is to force the y_i's to be either 0 or 1. For this purpose we define an objective function $f(\mathbf{y})$ by

$$f(y_1, \ldots, y_n) = y_1(1 - y_1) + \cdots + y_n(1 - y_n).$$

Notice that formula is quadratic—indeed it implies that

$$H = \mathrm{diag}(-1, \ldots, -1)$$

and $\mathbf{c} = (1, 1, \ldots, 1)^T$.

We have specified all of $(H, \mathbf{c})$ and the first $2n$ rows of $(A, \mathbf{b})$. Matrix A actually has $2n + m$ rows: the last m rows will contain one inequality for each clause of Q. The inequality will be a sum of terms, one term per literal of the clause. If x_i occurs as a literal, then the corresponding term of the inequality will be y_i. If $\neg x_i$ occurs as a literal, then the term of the inequality will be $(1 - y_i)$. The right hand side of the inequality will be 1. Thus, the clause $(x_1 \vee \neg x_2 \vee \neg x_3)$ will translate to the inequality $y_1 + (1 - y_2) + (1 - y_3) \geq 1$.

The claim is that the SAT formula is satisfiable if and only if the instance QP achieves an objective function less than or equal to 0. First, suppose that the SAT formula is satisfiable, i.e., there is a setting of the variables such that each clause has at least one literal set to 1. We must show that the global min of the QP is 0. Set each variable y_i equal to the corresponding variable x_i (i.e., 0 or 1). For this setting, $f(\mathbf{y}) = 0$, the first $2n$ inequalities are clearly satisfied, and the last m inequalities are satisfied because at least one term on the left-hand side of each inequality is set to 1.

For the other direction, suppose that the global minimum of the QP is 0. Since the objective function is the sum of terms that are nonnegative on the domain, this implies that each term is zero, i.e., each y_i is 0 or 1. Then we claim that by setting each x_i equal to the corresponding y_i we have a satisfying assignment for the formula Q.

2 NP membership when the minimum exists

To show membership in NP it is necessary to exhibit a succinct certificate for every **yes**-instance. The certificate in all cases will be the vector $\mathbf{x}$ such that $\mathbf{x}$ satisfies the decision problem of QPL. It is clear that plugging $\mathbf{x}$ into the inequalities $\mathbf{x}^T H\mathbf{x} + \mathbf{c}^T\mathbf{x} \leq K$ and $A\mathbf{x} \geq \mathbf{b}$ can be done in polynomial time. Accordingly, the main hurdle is to put an upper bound on the number of digits in the entries of vector $\mathbf{x}$.

It is important to stress that the proof is purely existential. In particular, there is no need in this or the following section to describe how the relevant $\mathbf{x}$ is computed, although at times part of our arguments will be computational.

We introduce more notation. Define $f : \mathbb{R}^n \to \mathbb{R}$ by

$$f(\mathbf{x}) = \mathbf{x}^T H\mathbf{x} + \mathbf{c}^T\mathbf{x}.$$

Define the feasible region Π by

$$\Pi = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \geq \mathbf{b}\}.$$

In this section we shall assume that the optimization problem has a global minimum, that is, there is a point $\mathbf{x}^* \in \Pi$ such that $f(\mathbf{x}^*) \leq f(\mathbf{x})$ for all $\mathbf{x} \in \Pi$. This assumption is dropped in the next section. For a **yes**-instance of QPL, a global minimum $\mathbf{x}^*$ for the problem (if it exists) will always serve as a certificate. Therefore, it is enough to show that there exists a global minimum with rational number entries, such that each entry has a number of digits bounded by a polynomial in the length of the input.

It is possible for there to be more than one global minimum. Among all global minima, let $\mathbf{x}^*$ be the global minimum such that the most number of the m inequalities $A\mathbf{x} \geq \mathbf{b}$ are *active*. Here, an *active* inequality is one that is satisfied exactly. If there is more than one global minimum with the maximum number of active inequalities, then we further break ties by selecting the global minimum with the most number of coordinates equal to zero. If there are still ties, they can be broken arbitrarily.

We claim that this particular $\mathbf{x}^*$ is the solution to a nonsingular system of linear equations. The remainder of the proof will expand on this claim. Suppose k constraints are active at $\mathbf{x}^*$ and suppose l entries of $\mathbf{x}^*$ are equal to zero. Then $\mathbf{x}^*$ satisfies the system of equations $M\mathbf{x}^* = \mathbf{b}'$, where M is the $(k+l) \times n$ matrix whose first k rows are equal to the active rows of A and whose last l rows express the constraints that certain coordinates are zero (i.e., these rows are rows of the identity matrix). Note that the entries of M and $\mathbf{b}'$ are either the original entries of A and $\mathbf{b}$ or 1's and 0's. Let r be the rank of matrix M. Then the equation $M\mathbf{x} = \mathbf{b}'$ denotes an $n-r$ dimensional affine subspace of $\mathbb{R}^n$. Call this subspace Y.

We can use elementary row operations to solve for r of the variables in $M\mathbf{x} = \mathbf{b}'$. Let $\hat{\mathbf{x}}$ denote the r variables that have been solved for. Then we can rewrite the constraints defining Y as $\hat{\mathbf{x}} = M'\bar{\mathbf{x}} + \mathbf{b}''$, where $\bar{\mathbf{x}}$ is the vector of the remaining $n-r$ variables; these variables can be chosen arbitrarily. This relationship sets up a linear bijection between $\mathbb{R}^{n-r}$ and Y. In particular, the map B from Y to $\mathbb{R}^{n-r}$ is the function that projects $\mathbf{x}$ onto $n-r$ of its coordinates. The inverse map B^{-1} sends $\bar{\mathbf{x}}$ to the vector $(\bar{\mathbf{x}}, M'\bar{\mathbf{x}} + \mathbf{b}'')$ with the entries permuted into the proper order.

It may be the case that $r = n$, i.e., Y is a 0-dimensional space with a unique point. Then $\mathbf{x}^*$ must be this unique solution since we already know that $\mathbf{x}^* \in Y$. Thus, in this case $\mathbf{x}^*$ is the solution to a nonsingular system of linear equations.

Otherwise, restrict the initial objective function $f(\mathbf{x}) = \mathbf{x}^T H\mathbf{x} + \mathbf{c}^T\mathbf{x}$ to Y; by the bijection described above this defines a quadratic function of $\bar{\mathbf{x}}$ in $\mathbb{R}^{n-r}$. In particular, we substitute the formula $M'\bar{\mathbf{x}} + \mathbf{b}''$ for $\hat{\mathbf{x}}$. This objective function on $\mathbb{R}^{n-r}$ will be denoted $\bar{f}(\bar{\mathbf{x}}) = \bar{\mathbf{x}}^T\bar{H}\bar{\mathbf{x}} + \bar{\mathbf{c}}^T\mathbf{x} + f_0$. Let $\bar{\mathbf{x}}^*$ denote the point $B(\mathbf{x}^*)$.

We claim that $\bar{H}$ must be a positive definite matrix. First, we argue that it is positive semidefinite. Suppose, for example, that there were a vector $\bar{\mathbf{d}}$ such that $\bar{\mathbf{d}}^T\bar{H}\bar{\mathbf{d}} < 0$; we want to show a contradiction. If such a vector $\bar{\mathbf{d}}$ exists, then for some choice of $\sigma = \pm 1$ it can be proved that $\bar{f}(\bar{\mathbf{x}}^* + \sigma\epsilon\bar{\mathbf{d}}) < \bar{f}(\bar{\mathbf{x}})$ for any $\epsilon > 0$. (To show this, write out the formula for the average of $\bar{f}(\bar{\mathbf{x}} - \epsilon\bar{\mathbf{d}})$ and $\bar{f}(\bar{\mathbf{x}} + \epsilon\bar{\mathbf{d}})$.) The point $\bar{\mathbf{x}}^* + \sigma\epsilon\bar{\mathbf{d}}$ can be mapped back to Y by B^{-1}. This point would then lie in the feasible region for ϵ small enough and would have a smaller value of the objective function f than $\mathbf{x}^*$, contradicting the global minimality of $\mathbf{x}^*$. Such a $\bar{\mathbf{d}}$ would be called a *feasible descent direction.*

Therefore, $\bar{H}$ must be positive semidefinite. In fact, it must be positive definite. To see this, suppose there were a nonzero vector $\bar{\mathbf{d}}$ such that $\bar{\mathbf{d}}^T\bar{H}\bar{\mathbf{d}} = 0$. Then it must be the case that $\bar{\mathbf{c}}^T\bar{\mathbf{d}} = 0$ also, otherwise we would have a descent direction as in the previous paragraph. Accordingly, we know that $\bar{f}(\bar{\mathbf{x}}^* + t\bar{\mathbf{d}}) = \bar{f}(\bar{\mathbf{x}}^*)$ for any value of the real number t. Pulling this back to $\mathbb{R}^n$ via B^{-1} gives a direction $\mathbf{d}$ such that $f(\mathbf{x}^* + t\mathbf{d}) = f(\mathbf{x}^*)$ for all t. But we claim that this contradicts the choice of $\mathbf{x}^*$. First, observe that $\mathbf{x}^* + t\mathbf{d} \in Y$, so at least as many inequalities are active for $\mathbf{x}^* + t\mathbf{d}$ as were for $\mathbf{x}^*$, and at least as many coordinates are zero. By choosing t large or small enough we can either make one additional inactive inequality become active or we can drive one additional coordinate to zero. This contradicts the choice of $\mathbf{x}^*$, which was supposed to have the maximum number of active constraints, and for this number of constraints, the maximum number of zero entries.

Therefore, we conclude that $\bar{H}$ is a positive definite matrix. This means that $\bar{f}$ has an (unconstrained) unique global minimum in $\mathbb{R}^{n-r}$, namely the point $\bar{\mathbf{x}}_o = -\bar{H}^{-1}\bar{\mathbf{c}}/2$. We claim that it must be the case that $\bar{\mathbf{x}}_o = \bar{\mathbf{x}}^*$. If not, there would be a feasible descent direction in $\mathbb{R}^{n-r}$, namely $\bar{\mathbf{d}} = \bar{\mathbf{x}}_o - \bar{\mathbf{x}}^*$.

Thus, the formula for $\mathbf{x}^*$ is as follows. If we know which variables are active at $\mathbf{x}^*$, then we can derive the matrix M' and the vector $\mathbf{b}''$. Then we substitute for some of the variables in $f(\mathbf{x})$ to get the restricted objective function coefficients, namely, $\bar{H}$ and $\bar{\mathbf{c}}$. Next, we compute $\bar{\mathbf{x}}^*$ by solving the linear system $\bar{H}\bar{\mathbf{x}}^* = -\bar{\mathbf{c}}/2$. This system always has a solution since $\bar{H}$ is positive definite.

Thus, $\mathbf{x}^*$ is determined entirely by solving two consecutive systems of equations. Edmonds [1967] proved that the solution to a system of equations with rational coefficients can be expressed with a number of digits that is polynomial in the length of the original problem. Since we are solving two systems of equations, we apply Edmonds' theorem twice to conclude that $\mathbf{x}^*$ has a polynomial number of digits.

3 NP membership when the minimum does not exist

In the preceding section we showed the existence of global minimum whose length is polynomial in the length of the input. The assumption made was that the global minimum exists. In this section we assume that the global minimum does not exist. This either means that the feasible region is empty or that it is noncompact. If it is empty, then the instance of QPL is not a yes-instance, so there is no need to discuss this case further. If the region is noncompact, then it must be unbounded since we already know it is closed.

Since the global minimum does not exist, there is a sequence of points $\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \ldots$ such that $f(\mathbf{x}^{(k)})$ either diverges to $-\infty$ or converges to the greatest lower bound of the values of $f(\mathbf{x})$ on the domain. In fact, the following proof will show that it is impossible for f to be bounded below and for the minimum not to exist, but at this point of the argument we cannot exclude that case.

For each k define $v_k = \|\mathbf{x}^{(k)}\|_\infty$. The sequence $v_1, v_2, \ldots$ cannot have an upper bound; if it did, then the sequence $\mathbf{x}^{(k)}$ would lie in a compact set, contradicting our assumption that the minimum fails to exist. Now consider the sequence of quadratic programming problems QP_k given by

$$\begin{array}{rl} \text{minimize} & \mathbf{x}^T H\mathbf{x} + \mathbf{c}^T\mathbf{x} \\ \text{subject to} & A\mathbf{x} \geq \mathbf{b}, \\ & x_i \leq v_k, \text{ for } i = 1, \ldots, n, \\ & x_i \geq -v_k, \text{ for } i = 1, \ldots, n. \end{array}$$

Notice that $\mathbf{x}^{(k)}$ is feasible for this problem.

We redefine $\mathbf{x}^{(k)}$ now to be the global minimum of QP_k. Such a minimum exists since the feasible region of QP_k is nonempty and compact. Moreover, we know that under this new definition $f(\mathbf{x}^{(k)})$ still either tends to the greatest lower bound or diverges to $-\infty$. By passing to a subsequence, we can assume without loss of generality that $f(\mathbf{x}^{(k)})$ is strictly decreasing.

Suppose there is more than one global minimum of QP_k. Then among all choices we select the minimum as in the previous section. Specifically, we select the minimum with the most number of active inequalities. If there is still more than one minimum, we select the one with the most number of zero coordinates. Further ties are broken arbitrarily.

Note that QP_k has exactly $m + 2n$ inequality constraints; assume they are numbered in some canonical order (say the order listed above). Let the *signature* of a particular $\mathbf{x}^{(i)}$ be the list indicating which of the $m + 2n$ inequalities are active and which coordinates are equal to zero. There are at most 2^{m+3n} possible signatures that a point could have. Since there are only a finite number, there must be at least one signature that occurs infinitely often in the sequence $\mathbf{x}^{(k)}$. By passing to a subsequence, we can assume (without loss of generality) that all the points in the sequence have the same signature.

As in the previous section, we construct a sequence of affine spaces Y_k based on the active inequalities. As before,

$$Y_k = \{x \in \mathbb{R}^n : M\mathbf{x} = \mathbf{b}_k\}.$$

Notice that the coefficient matrix M for Y_k will be independent of k; this follows from the assumption that all the points have the same signature. The right-hand-side $\mathbf{b}_k$ depends on k; in particular, its entries will either be coefficients from the original QP or they will be v_k or $-v_k$. This is because some of the constraints $x_i \leq v_k$ or $x_i \geq -v_k$ will be active.

Next, we solve for the first r variables as in the previous section so that we can write $\hat{\mathbf{x}}^{(k)} = M'\bar{\mathbf{x}}^{(k)} + \mathbf{b}'_k$, where $\mathbf{b}'_k$ depends on k, and, specifically, varies linearly with v_k.

Next, we compute the reduced $\bar{f}_k(\bar{\mathbf{x}})$. This function will have the form:

$$\bar{f}_k(\bar{\mathbf{x}}) = \bar{\mathbf{x}}^T \bar{H} \bar{\mathbf{x}} + v_k \bar{\mathbf{c}}_1^T \bar{\mathbf{x}} + \bar{\mathbf{c}}_2^T \bar{\mathbf{x}} + q_0(v_k) + f_0$$

where $\bar{H}$, $\bar{\mathbf{c}}_1$, $\bar{\mathbf{c}}_2$ and f_0 are independent of k, and $q_0(v_k)$ is a real-valued quadratic function of one variable.

As in the previous section $\bar{H}$ must be a positive definite matrix. Therefore, as in the previous section,

$$\bar{\mathbf{x}}^{(k)} = -\bar{H}^{-1}(v_k \bar{\mathbf{c}}_1 + \bar{\mathbf{c}}_2)/2.$$

Thus, we see that $\bar{\mathbf{x}}^{(k)}$ is a linearly varying function of v_k. Moreover, the coefficients of this linear variation can be written down in polynomial space, because they arise from solving linear systems involving only the original coefficients of the quadratic program. Therefore, we can write $\bar{\mathbf{x}}^{(k)} = \bar{\mathbf{x}}_0 + v_k\bar{\mathbf{x}}_1$ where $\bar{\mathbf{x}}_0$ and $\bar{\mathbf{x}}_1$ are rational vectors with a polynomial number of digits. By calculating the other coefficients, we reach a similar conclusion about $\mathbf{x}^{(k)}$, namely, that $\mathbf{x}^{(k)} = \mathbf{x}_0 + v_k\mathbf{x}_1$.

Finally, substituting the formula for $\bar{\mathbf{x}}^{(k)}$ into the objective function, we arrive at the conclusion that $f(\mathbf{x}^{(k)}) = q(v_k)$ where $q(v_k)$ is a real-valued quadratic function of one variable whose coefficients require polynomial space. Since this holds for v_k arbitrarily large, we can define a ray $\mathbf{x}(v) = \mathbf{x}_0 + v\mathbf{x}_1$ which is feasible for the original QP for all v large enough and which has a decreasing objective function.

How large must v be in order for $\mathbf{x}(v)$ to be feasible for the original QP? Let v^* be the minimum value of v such that $\mathbf{x}(v)$ is feasible on $[v^*, +\infty)$, or zero, whichever is larger. If v^* is nonzero, then there must be an i that $\mathbf{a}_i^T\mathbf{x}(v^*) = b_i$ and such that $\mathbf{a}_i^T\mathbf{x}(v) < b_i$ for $v < v^*$. Therefore, the equation $\mathbf{a}_i^T\mathbf{x}(v^*) = b_i$ is a nondegenerate linear equation of one variable. Solving for v^* shows that it can be expressed as a rational number whose number of digits is polynomial in the length of the input. Therefore, we can translate the parameterization of $\mathbf{x}(v)$ so that without loss of generality it is feasible for all $v \geq 0$.

Now finally we have reduced the original problem of showing the existence of a polynomial-length $\mathbf{x}$ to the following problem. Given a decreasing real-valued quadratic function $q(v)$ whose coefficients are rational and given a rational number K, find a point $v^* \geq 0$ such that $q(v^*) \leq K$.

This is a simple problem to solve; we now indicate the argument. The only trick is to show that we need not take a square root. If the leading coefficient of q is zero, then q is linear and we simply solve the linear equation. If the leading coefficient of q is not zero, then we write $q(v)$ as $q(v) = a(v - v_0)^2 + q_0$. This requires only rational operations. Notice that a must be negative in this case, since q is decreasing. Then the problem is to solve $(v - v_0)^2 \geq (K - q_0)/a$. Now, if $(K - q_0)/a \leq 1$ then we can take $v^* = \max(v_0 + 1, 0)$. If $(K - q_0)/a \geq 1$, then we take $v^* = \max(v_0 + (K - q_0)/a, 0)$. In all cases, we find a rational number v^* with a polynomial number of digits such that $v^* \geq 0$ and $q(v^*) \leq K$.

Once this v^* is known, we can determine the certificate $\mathbf{x}$ for the original problem, namely $\mathbf{x} = \mathbf{x}(v^*)$. This requires only a polynomial number of digits.

This concludes the proof that quadratic programming is in **NP**.

Theorem 1 *Problem QPL is* **NP***-complete.*

PROOF. Sahni's reduction or the reduction in the first section shows that any problem in **NP** can be polynomially transformed to QPL. In the last two sections we have argued that there is a polynomial-length certificate for **yes**-instances of QPL, showing that the problem is in **NP**. ∎

Notice that as a byproduct of this proof we have shown the following theorem. There seems to be no way to prove this theorem simpler than setting up all the machinery of this report.

Theorem 2 *Consider the problem of minimizing a quadratic objective function subject to a finite number of linear constraints. Then the possible outcomes are: (a) the constraints are infeasible, (b) a global minimum exists, or (c) the objective function is unbounded from below in the feasible region. In particular, the following case is not possible: the objective function is bounded below but does not achieve its minimum.*

PROOF. The preceding argument shows that for a feasible QP that does not attain its minimum, there must exist a ray such that every point on the ray is feasible, and the objective function is a decreasing quadratic function on the ray. Such a function must tend to $-\infty$. ∎

References

J. Edmonds [1967] Systems of Distinct Representatives and Linear Algebra, *J. Res. Nat. Bur. Standards Ser. B,* 71:241-245.

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

S. Sahni [1974], Computationally related problems, *SIAM J. Comp.* 3:262-279.