RELAXED VERIFICATION FOR CONTINUOUS PROBLEMS

E. Novak
Mathematisches Institut,
Universität Erlangen-Nürnberg
H. Woźniakowski
Department of Computer
Science, Columbia University
and
Institute of Applied Mathematics,
University of Warsaw

CUCS-028-92

October, 1991

Abstract. We analyze the complexity of verifying whether a given element is close to a solution element. Closeness is measured by two nonnegative parameters, ε and α. If $\alpha = 0$, then we get the strong verification problem which usually cannot be solved in the worst case setting, see Woźniakowski [90]. For $\alpha > 0$, we have the relaxed verification problem which is studied in this paper in the worst case setting.

We show that the (ε, α)-verification complexity is roughly equal to the η-computation complexity, where $\eta = \eta(\varepsilon, \alpha)$. Under certain general assumptions we prove that $\eta(\varepsilon, \alpha) = \Theta(\varepsilon\, \alpha^r)$, where r depends on the problem norm, $r \in [0, 1]$. We also show that adaption sometimes helps significantly.

1. Introduction

In information-based complexity, we study the minimal cost of computing an ε-approximation to the solution element for continuous problems. We call such a problem the *computational* problem.

Typeset by $\mathcal{AMS}$-TeX

By *verification*, we mean a different problem. Instead of computing an ε-approximation to the solution element, we wish to verify whether a given element is within ε of the solution element. This "strong" verification problem is studied in Woźniakowski [90], see also this paper for a list of relevant references on information-based complexity. It turns out that for many linear problems, the worst case complexity of the strong verification problem is infinite for all $\varepsilon \geq 0$.

Therefore, in this paper we study a relaxed verification problem. We assume that the solution element is specified by $S(f)$ where S is a given operator, $S : F \to G_1$. Here F is a subset of a linear space F_1 and G_1 is a normed linear space. For given nonnegative parameters ε and α, we want to verify whether an element g from a given set G, $G \subset G_1$, is within ε of the solution element $S(f)$, i.e., whether $\|S(f) - g\| \leq \varepsilon$, or whether $\|S(f) - g\| > (1 + \alpha)\,\varepsilon$. We stress that we do not demand a true answer if

$$\varepsilon < \|S(f) - g\| \leq (1 + \alpha)\,\varepsilon.$$

Thus, for positive $\alpha > 0$ we have a "safety zone". For $\alpha = 0$ we get the strong verification problem.

We assume that the element f is not known and information on f can be gathered by computing certain linear functionals. This information may be *adaptive* since the choice of the successive functional may depend on the element g and on the already computed information on f.

In this paper we study the worst case setting. That is, the cost and error are defined by their worst performance. The complexity is then understood as the minimal cost of solving the problem with the required accuracy.

We show relations between the complexities of the verification and computation problems. These relations depend, in particular, on the set G. We consider two choices $G = S(F) + B_\varepsilon$ and $G = S(F)$, where B_ε is the ball of G_1 of center 0 and radius ε. It turns out that the results for $G = S(F) + B_\varepsilon$ are the same as for any G containing $S(F) + B_\varepsilon$. In particular, this means that the results are the same for $G = S(F) + B_\varepsilon$ and for $G = G_1$.

For small ε, the difference between these two sets $G = S(F) + B_\varepsilon$ and $G = S(F)$ seems insignificant. As we shall see, the results may be, however, quite different. We present examples for which adaption and the parameter α play different roles for these two sets.

We show that the (ε, α)-verification complexity, $\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha)$, is related to the η-computation complexity, $\mathrm{comp}^{\mathrm{com}}(\eta)$, where η is a function of ε and α, i.e., $\eta = \eta(\varepsilon, \alpha)$. For the two choices of G, we show that

$$\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \ \leq\ \mathrm{comp}^{\mathrm{com}}(\varepsilon\,\alpha/2) \ +\ 1.$$

This is sharp for some problems. Indeed, this is the case when S is a linear functional or S is a linear diagonal operator in l_1.

To simplify the presentation of the further results, we present the function $\eta(\varepsilon,\alpha)$ modulo a multiplicative constant which depends only on the norm of the space G_1.

We now take $G = S(F) + B_\varepsilon$. For general S, we prove that if the (ε,α)-verification problem is solved by using information independent of the elements g then its cost is at least as large as the η-computation complexity, where $\eta = \varepsilon\alpha$. Thus, the (ε,α)-verification complexity may be smaller than the $(\varepsilon\,\alpha)$-computation complexity only if *adaption* helps for the verification problem. As we shall see, for some problems this indeed happens and adaption helps significantly.

Let S be a linear diagonal operator in l_p with $p \in [1,\infty]$. For small α we show that (ε,α)-verification complexity is the same as the $(\varepsilon\,\alpha^r)$-computation complexity, where

$$r = \begin{cases} \frac{1}{p} & \text{if } p \in [1,2], \\ \frac{1}{2} & \text{if } p \in [2,\infty), \\ 1 & \text{if } p = \infty. \end{cases}$$

Thus, the dependence on α varies with p. The cases $p = 1$ and $p = \infty$ have the largest complexity, whereas the case $p \in [2,\infty)$ has the smallest complexity.

For $p \in (1,\infty)$, this means that *adaption* helps significantly. If the η-computation complexity is of the form $\Theta(\eta^{-q})$ for some positive q, then adaption is $\Theta(\alpha^{-q(1-r)})$ times more effective than nonadaption. We add that the (ε,α)-verification complexity is obtained by computing adaptive information which consists only of one functional depending on the element g and a number of nonadaptive functionals. Still, this one adaptive functional makes a great difference.

We now turn to the set $G = S(F)$. We show that the (ε,α)-verification complexity is the same as the $(\varepsilon\,\alpha^{1/p})$-computation complexity.

Hence, in this case the (ε,α)-verification complexity decreases monotonically with p. For $p = \infty$, it does not depend on α. This means that for $\alpha = 0$, the strong verification complexity is roughly the same as the ε-computation complexity.

We stress that for $G = S(F)$, adaption does *not* help. The (ε,α)-verification complexity is obtained by computing *nonadaptive* information. This is in a sharp contrast to the previous case, $G = S(F) + B_\varepsilon$, for which adaption helps. Adaption is not needed for $G = S(F)$ since the fact that $g = S(f)$ for some $f \in F$ supplies extra a priori information.

We now compare the (ε,α)-verification complexities for $G = S(F) + B_\varepsilon$ and $G = S(F)$. They are the same for $p \in [1,2]$. For $p > 2$, the case $G = S(F)$ is easier. If the η-computation complexity is of the form $\Theta(\eta^{-q})$ then the ratio of the (ε,α)-verification complexities is

$$\Theta\left(\left(\frac{1}{\alpha}\right)^{q\,a}\right),$$

where $a = 1/2 - 1/p$ if $p \in (2, \infty)$, and $a = 1$ if $p = \infty$.

2. The (ε, α)-verification Problem

For a given subset F of a linear space F_1 and a given normed linear space G_1, consider an arbitrary operator

$$S : F \to G_1.$$

Let G be a nonempty subset of G_1 and let ε and α be nonnegative numbers. By the (ε, α)-*verification* problem we mean to compute the verification operator $\mathrm{VER} : F \times G \to \{\mathrm{YES}, \mathrm{NO}\}$, defined by

$$\mathrm{VER}(f, g) = \begin{cases} \text{YES} & \text{if} \quad \|S(f) - g\| \le \varepsilon, \\ \text{NO} & \text{if} \quad \|S(f) - g\| > (1+\alpha)\,\varepsilon, \\ \text{YES or NO} & \text{otherwise.} \end{cases}$$

That is, we wish to verify whether the elements $S(f)$ and g differ in norm by at most ε or at least $(1+\alpha)\,\varepsilon$. Observe that we allow both answers in the safety zone

$$\varepsilon < \|S(f) - g\| \le (1+\alpha) \cdot \varepsilon.$$

To compute $\mathrm{VER}(f, g)$ we assume that g, as well as the parameters ε and α, are known. The knowledge of the element f can be gathered by computing some information operations L about f. Let Λ be a given set of such information operations L, where $L : F \to \mathbb{R}$. The information which is computed about f may depend on the element g and is of the form

$$N(f; g) = [L_{1,g}(f), L_{2,g}(f), \ldots, L_{n,g}(f)],$$

where $L_{i,g} \in \Lambda$, and the choice of $L_{i,g}$ may also depend on the already computed values $L_{1,g}(f), \ldots, L_{i-1,g}(f)$. In the worst case setting, we can assume that the number n, the *cardinality* of N, does not depend on f or g. If the $L_{i,g}$'s depend on f or g, then N is called *adaptive*, otherwise N is called *nonadaptive*. The operators $N : F \times G \to \mathbb{R}^n$ and $N_g = N(\cdot; g) : F \to \mathbb{R}^n$ are called *information operators.*

Knowing $N_g(f)$ and g, we combine this information by a mapping ϕ, called an *algorithm*, where $\phi : N(F \times G) \times G \to \{\mathrm{YES}, \mathrm{NO}\}$, to get

$$U(f, g) = \phi(N_g(f), g).$$

The approximation operator U may also depend, of course, on the fixed parameters of the verification problem such as S, ε, and α.

By the *solution* of the (ε, α)-verification problem we mean to find an approximation operator U such that

$$U(f,g) = \mathrm{VER}(f,g)$$

for all $f \in F$ and all $g \in G$ for which

$$\|g - S(f)\| \le \varepsilon \quad \text{or} \quad \|g - S(f)\| > (1+\alpha)\,\varepsilon.$$

Observe that for some elements g, the (ε, α)-verification problem may be trivial. Indeed, if

$$\mathrm{dist}(g, S(F)) \, > \, \varepsilon$$

then the condition $\|g - S(f)\| \le \varepsilon$ never happens and $U(f,g) = \mathrm{NO}$ solves the problem. This shows that we get the same results if

$$S(F) \, + \, B_\varepsilon \;\subset\; G \qquad \text{or} \qquad S(F) \, + \, B_\varepsilon \; = \; G,$$

where $S(F) + B_\varepsilon = \{S(f) + h : \; f \in F \text{ and } \|h\| \le \varepsilon\}$.

In this paper we consider two different choices of the set G. The first is

$$G \; = \; S(F) \, + \, B_\varepsilon \qquad\qquad (\text{or } S(F) \, + \, B_\varepsilon \subset G)$$

and the second is

$$G \; = \; S(F).$$

For small ε, it seems that the difference between these two sets is insignificant. As we shall see the results, however, may be quite different.

We shall take the information point of view, i.e., for given S, ε, α and the set G we ask for conditions on N under which there is a ϕ such that $U = (\phi, N)$ solves the (ε, α)-verification problem. As we shall see, these conditions on N will be expressed in terms of the concepts which are used for the computation problem.

Therefore, we first recall for which N we can solve the ε-computation problem. That is, we now have an information operator $N : F \to \mathbb{R}^n$ independent of g and ask whether there exists a $\phi : \mathbb{R}^n \to G_1$ such that $\|S(f) - \phi(N(f))\| \le \varepsilon$ for all $f \in F$. For any S and N, the solution of the ε-computation problem depends on the *radius* of information N which is defined as

$$r(N) = \sup_{y \in N(F)} \mathrm{rad}(SN^{-1}(y)),$$

where the radius $\mathrm{rad}(A)$ of a set A, $A \subset G$, is given by

$$\mathrm{rad}(A) = \inf_{x \in G} \sup_{a \in A} \|x - a\|.$$

Assuming that the infima in $\mathrm{rad}(SN^{-1}(y))$ are attained, the ε-computation problem can be solved using the information N iff

$$r(N) \le \varepsilon.$$

It will be convenient to use also the concept of the *diameter* of the information N which is defined as

$$d(N) = \sup_{y \in N(F)} \mathrm{diam}(SN^{-1}(y)),$$

where the diameter $\mathrm{diam}(A)$ of a set A is given by

$$\mathrm{diam}(A) = \sup_{a,b \in A} \|a - b\|.$$

Obviously, for all $N : F \to \mathbb{R}^n$ we have

$$r(N) \le d(N) \le 2\, r(N).$$

3. Verification for $S(F) + B_\varepsilon \subset G$

In this section we assume that the set G contains $S(F) + B_\varepsilon$. As already explained this is equivalent to assuming that $G = G_1$.

We consider information operators N which may or may not depend adaptively on g. We shall see that adaptive information can be much more powerful for some (ε, α)-verification problems.

3.1. Information Independent of g

We first analyze information which does not depend on g. A simple way to solve the (ε, α)-verification problem for such information is as follows. Assume that the radius $r(N)$ of information $N : F \to \mathbb{R}^n$ is smaller than $\varepsilon\,\alpha/2$. Then we can find an algorithm $\phi : \mathbb{R}^n \to G_1$ such that

$$\|S(f) - \phi(N(f))\| < \varepsilon\,\alpha/2 \quad \forall f \in F.$$

Using this algorithm for the computation problem, we can solve the (ε, α)-verification problem by putting

$$U(f,g) = \begin{cases} \text{YES} & \text{if} \quad \|\phi(N(f)) - g\| \le (1+\alpha/2)\,\varepsilon, \\ \text{NO} & \text{if} \quad \|\phi(N(f)) - g\| > (1+\alpha/2)\,\varepsilon. \end{cases}$$

Indeed, if $\|S(f) - g\| \le \varepsilon$ then $\mathrm{VER}(f,g) = \text{YES}$ and

$$\|\phi(N(f)) - g\| \le \|S(f) - g\| \; + \; \|\phi(N(f)) - S(f)\| \; \le \; \varepsilon \; + \; \varepsilon\,\alpha/2 \; = (1+\alpha/2)\,\varepsilon.$$

Thus, $U(f,g) = \text{YES} = \mathrm{VER}(f,g)$. Similarly, if $\|S(f) - g\| > (1+\alpha)\,\varepsilon$ then $\mathrm{VER}(f,g) =$ NO and

$$\|\phi(N(f)) - g\| \; \ge \; \|S(f) - g\| \; - \; \|S(f) - \phi(N(f))\| \; > \; (1+\alpha)\,\varepsilon \; - \; \varepsilon\,\alpha/2 \; = (1+\alpha/2)\,\varepsilon.$$

Thus, $U(f,g) = \text{NO} = \mathrm{VER}(f,g)$, as claimed.

From the information point of view this result can be slightly strengthened by using the diameter of information instead of its radius.

Theorem 3.1. *The (ε, α)-verification problem can be solved for every $g \in G$ by using a information operator $N : F \to \mathbb{R}^n$ independent of g iff*

$$d(N) \le \varepsilon\,\alpha.$$

Proof. First assume that $d(N) \le \varepsilon\,\alpha$. Define U by

$$U(f,g) = \begin{cases} \text{YES} & \text{if} \quad \inf\{\|S(\tilde{f}) - g\| : \; \tilde{f} \in F \text{ with } N(\tilde{f}) = N(f)\} \; \le \; \varepsilon, \\ \text{NO} & \text{otherwise.} \end{cases}$$

The U approximation solves the (ε, α)-verification problem. Indeed, if $\|S(f) - g\| \le \varepsilon$ then

$$\inf\{\|S(\tilde{f}) - g\| : \; \tilde{f} \in F, \; N(\tilde{f}) = N(f)\} \; \le \; \|S(f) - g\| \; \le \; \varepsilon$$

and $\mathrm{VER}(f,g) = U(f,g) = \text{YES}$.

Assume now that $\|S(f) - g\| > (1+\alpha)\,\varepsilon$. Observe that for any $\tilde{f} \in F$ with $N(\tilde{f}) = N(f)$ we have $\|S(\tilde{f}) - S(f)\| \le d(N) \le \varepsilon\,\alpha$. Therefore

$$\|S(\tilde{f}) - g\| \ge \|S(f) - g\| - \|S(\tilde{f}) - S(f)\| \; > \; (1+\alpha)\varepsilon - \varepsilon\,\alpha \; = \; \varepsilon.$$

Thus, $\mathrm{VER}(f,g) = U(f,g) = \text{NO}$, as claimed.

Consider now the case $d(N) > \varepsilon\,\alpha$. This means that there exist $f_1, f_2 \in F$ such that $N(f_1) = N(f_2)$ and $\|S(f_1) - S(f_2)\| > \varepsilon\,\alpha$. We can find an element $g \in S(F) + B_\varepsilon \subset G$ on the line passing through $S(f_1)$ and $S(f_2)$ with $\|S(f_1) - g\| \le \varepsilon$ and $\|S(f_2) - g\| > (1+\alpha)\varepsilon$. For instance, one can take $g = S(f_1) - \varepsilon\,\|S(f_1) - S(f_2)\|^{-1}\,(S(f_2) - S(f_1))$. From $N(f_1) = N(f_2)$ we have $U(f_1, g) = U(f_2, g)$ for any U using N. Since $\mathrm{VER}(f_1, g) \ne \mathrm{VER}(f_2, g)$ then $\mathrm{VER}(f_i, g) \ne U(f_i, g)$ for some $i \in \{1, 2\}$. Hence we cannot solve the (ε, α)-verification problem with the information N. This completes the proof. $\square$

What is the smallest cardinality n such that the (ε, α)-verification problem can be solved for every $g \in G$ by using $N : F \to \mathbb{R}^n$ independent of g? Obviously, this question has been answered by Theorem 3.1; we just have to choose the smallest n such that there is an information operator $N : F \to \mathbb{R}^n$ with $d(N) \le \varepsilon\alpha$.

In the next subsection we turn to adaptive information $N : F \times G \to \mathbb{R}^n$ and show that for some problems the inequality $d(N_g) \le \varepsilon\,\alpha$ may be significantly relaxed. We will seek the minimal cardinality n for which the (ε, α)-verification problem can be solved by using adaptive information of cardinality n.

3.2. Adaptive Information

We first check which adaptive information N can solve the (ε, α)-verification problem. In what follows, we use the following notation:

$$B(g, \varepsilon) = \{S(f) :\; f \in F \text{ and } \|g - S(f)\| \le \varepsilon\},$$
$$B(g, -(1+\alpha)\varepsilon) = S(F) \;-\; B(g, (1+\alpha)\varepsilon).$$

Theorem 3.2. *The (ε, α)-verification problem can be solved for an element g of G by using an information operator $N_g : F \to \mathbb{R}^n$ iff for any $f \in F$,*

$$B(g, \varepsilon) \cap SN_g^{-1}(N_g(f)) \ne \emptyset \quad \textit{implies} \quad B(g, -(1+\alpha)\varepsilon) \cap SN_g^{-1}(N_g(f)) = \emptyset. \qquad (3.1)$$

Proof. Assume that (3.1) holds. Define U by

$$U(f, g) = \begin{cases} \text{YES} & \text{if } \; B(g, \varepsilon) \cap SN_g^{-1}(N_g(f)) \ne \emptyset, \\ \text{NO} & \text{otherwise.} \end{cases}$$

The U approximation solves the (ε, α)-verification problem. Indeed, if $\|g - S(f)\| \le \varepsilon$ then $S(f) \in B(g, \varepsilon) \cap SN_g^{-1}(N_g(f))$. Thus, $U(f, g) = \mathrm{VER}(f, g) = \text{YES}$.

Assume now that $\|g - S(f)\| > (1+\alpha)\varepsilon$. Then $S(f) \in B(g, -(1+\alpha)\varepsilon) \cap SN_g^{-1}(N_g(f))$. Due to (3.1) this implies that $B(g,\varepsilon) \cap SN_g^{-1}(N_g(f)) = \emptyset$. Hence, $U(f,g) = \mathrm{VER}(f,g) =$ NO, as claimed.

Suppose now that (3.1) does not hold. That is, there exists $f \in F$ such that $\|g - S(f_1)\| \leq \varepsilon$ and $\|g - S(f_2)\| > (1+\alpha)\varepsilon$ for some $f_1, f_2 \in F$ and $N_g(f_1) = N_g(f_2) = N_g(f)$. Then $\mathrm{VER}(f_1,g) \neq \mathrm{VER}(f_2,g)$ but $U(f_1,g) = U(f_2,g)$ for any U that uses N. Hence, $\mathrm{VER}(f_i,g) \neq U(f_i,g)$ for some $i \in \{1,2\}$ and N does not solve the (ε,α)-verification problem. $\square$

Theorem 3.2 states that N solves the problem for all $g \in G$ iff the sets $SN_g^{-1}(N_g(f))$ do not have common elements simultaneously with $B(g,\varepsilon)$ and $B(g,-(1+\alpha)\varepsilon)$. The set $SN_g^{-1}(N_g(f))$ represents solution elements which are indistinguishable if $N_g(f)$ is computed. Observe that (3.1) holds trivially if $\mathrm{dist}(g, S(F)) > \varepsilon$. Thus, we need to check (3.1) only for g such that $\mathrm{dist}(g, S(F)) \leq \varepsilon$. From Theorem 3.2 we easily conclude the following corollary.

Corollary 3.1. *If*

$$d(N_g) \leq \varepsilon\,\alpha \quad \forall\, g \in S(F) + B_\varepsilon$$

then the (ε,α)-verification problem can be solved for every $g \in G_1$ by using N.

Proof. We check (3.1). Let $A = B(g,\varepsilon) \cap SN_g^{-1}(N_g(f)) \neq \emptyset$. Take f_1 from A and arbitrary $f_2 \in SN_g^{-1}(N_g(f))$. Then $N_g(f_1) = N_g(f_2)$, and $\|g - S(f_1)\| \leq \varepsilon$ and $\|S(f_1) - S(f_2)\| \leq d(N_g) \leq \varepsilon\alpha$. Thus

$$\|g - S(f_2)\| \leq \|g - S(f_1)\| + \|S(f_1) - S(f_2)\| \leq \varepsilon + \varepsilon\,\alpha = (1+\alpha)\,\varepsilon.$$

Hence, $B(g, -(1+\alpha)\varepsilon) \cap SN_g^{-1}(N_g(f)) = \emptyset$ and (3.1) holds. $\square$

Observe that for information N independent of g we have $d(N_g) = d(N)$ and Corollary 3.1. coincides with part of Theorem 3.1. By a proper choice of g the condition $d(N) \leq \varepsilon\alpha$ is also necessary as the other part of Theorem 3.1 states.

We now want to check whether $d(N_g) \leq \varepsilon\,\alpha$ can be improved for adaptive information. As we shall see the answer depends on the particular problem. For some problems this inequality can be significantly improved, while for others it cannot.

First we present a problem for which adaption helps significantly. Let F_1 and G_1 be Hilbert spaces and let $S : F_1 \to G_1$ be a diagonal operator, i.e., S is linear and

$$S(e_i) = \lambda_i \tilde{e}_i, \tag{3.2}$$

for some $\{e_i\}$ and $\{\tilde{e}_i\}$ which form complete orthonormal systems of F_1 and G_1, respectively. We order $\{\lambda_i\}$ such that $\lambda_1 \ge \lambda_2 \ge \cdots \ge 0$ and assume that $\lim_i \lambda_i = 0$. Note that (3.2) holds if S is a compact operator. We also assume that $\Lambda = F_1^*$ is the set of all continuous linear functionals and F is the unit ball of F_1.

Define the adaptive information of cardinality n

$$N^*(f,g) = [(S(f),g), (f,e_1), \dots, (f,e_{n-1})], \tag{3.3}$$

where $(\cdot,\cdot)$ stands for the inner product in the corresponding space and n is chosen as the smallest integer for which

$$\lambda_n \le \varepsilon \sqrt{\alpha(2+\alpha)}.$$

For linear problems we have $d(N_g^*) = 2\sup\{\|S(h)\| : h \in F, N_g^*(h) = 0\}$. From this it easily follows that $2\lambda_{n+1} \le d(N_g^*) \le 2\lambda_n$. From the definition of n we get

$$\frac{\lambda_{n+1}}{\lambda_n}\, 2\varepsilon \sqrt{\alpha(2+\alpha)} \le d(N_g^*) \le 2\varepsilon \sqrt{\alpha(2+\alpha)}.$$

Suppose that $\lambda_i \to 0$ so slowly that $\lambda_{i+1}/\lambda_i \to 1$. (This holds, for example, if $\lambda_i = i^{-r}$ with $r > 0$.) Then $d(N_g^*) \simeq 2\varepsilon \sqrt{\alpha(2+\alpha)}$ for small ε or α. This means that for small α we have

$$d(N_g^*) \simeq 2\sqrt{2}\,\varepsilon \sqrt{\alpha}$$

which is much larger than the bound $d(N) \le \varepsilon\alpha$ required for information independent of g. Despite this, we now show that N^* solves the problem.

Theorem 3.3. *The (ε,α)-verification problem can be solved for every $g \in G$ by using the adaptive information operator N^* given by (3.3).*

Proof. For any $f \in F$ and $g \in G$ let $\sigma = \sum_{i=1}^{n-1} (f,e_i)\, e_i$. Then

$$S(\sigma) = \sum_{i=1}^{n-1} \lambda_i (f,e_i)\, \tilde{e}_i$$

and

$$\beta = \|g\|^2 - 2(S(f),g) + \|S(\sigma)\|^2 = \|g\|^2 - 2(S(f),g) + \sum_{i=1}^{n-1} \lambda_i^2\, (f,e_i)^2.$$

Hence, β can be easily computed if $N^*(f,g)$ is known. Define U by

$$U(f,g) = \begin{cases} \text{YES} & \text{if } \beta \le \varepsilon^2, \\ \text{NO} & \text{if } \beta > \varepsilon^2. \end{cases}$$

We prove that this U solves the (ε,α)-verification problem. For each $f \in F$ we have $S(f) = S(\sigma) + S(h)$ with $(S(\sigma), S(h)) = 0$ and $\|S(h)\| \le \lambda_n$. Hence

$$\|g - S(f)\|^2 = \|g\|^2 - 2(S(f), g) + \|S(f)\|^2 = \beta + \|S(h)\|^2.$$

Thus, we obtain

$$\beta \le \|g - S(f)\|^2 \le \beta + \lambda_n^2.$$

If $\|g - S(f)\| \le \varepsilon$ then $\beta \le \varepsilon^2$ and U gives the correct answer 'yes'. If $\|g - S(f)\| > (1+\alpha)\varepsilon$ then

$$\beta > (1+\alpha)^2\varepsilon^2 - \alpha(2+\alpha)\varepsilon^2 = \varepsilon^2$$

and U again gives the right answer 'no'. This completes the proof. $\square$

Theorem 3.3 presents a linear problem in a Hilbert space for which adaption helps. We illustrate this by assuming that $\lambda_i = i^{-q}$ for a positive q. We compare cardinalities of information N independent of g and information N^* which both solve the (ε,α)-verification problem. For N we have to guarantee that $d(N) \le \varepsilon\alpha$ which implies that its cardinality k must be at least equal to $\lceil(\varepsilon\alpha/2)^{-1/q}\rceil - 1$, whereas the cardinality n of N^* is given by $n = \lceil(\varepsilon\sqrt{\alpha(2+\alpha)})^{-1/q}\rceil$. In Section 4 we show that the cardinality of N^* is (almost) minimal among the cardinalities of adaptive information that solve the (ε,α)-verification problem. Neglecting the ceilings we have

$$\frac{k+1}{n} \ge \left(\frac{4(2+\alpha)}{\alpha}\right)^{1/(2q)}.$$

This ratio tends to $+\infty$ as α goes to zero.

3.3. Diagonal Operators in l_p

We now consider diagonal operators in l_p for arbitrary $p \in [1,+\infty]$ with G containing $S(F) + B_\varepsilon$. We show that adaption does not help much if $p = 1$ or $p = \infty$ but does help for all other p. The case $p = 2$ is extremal in the sense that adaption helps most of all.

Let $F_1 = G_1 = l_p$ be the space of sequences $f = [f_1, f_2, \dots]$ with $\|f\| < +\infty$, where $\|f\| = (\sum_{i=1}^{+\infty} |f_i|^p)^{1/p}$ for $p \in [1,+\infty)$ and $\|f\| = \sup_{1\le i<+\infty} |f_i|$ for $p = +\infty$.

Let $S : l_p \to l_p$ be a diagonal operator, i.e., S is linear and

$$S(e_i) = \lambda_i\, e_i,$$

where $e_i = (0,\dots,0,1,0,\dots)$, i.e., $(e_i)_k = \delta_{ik}$. We assume that $\lambda_1 \ge \lambda_2 \ge \cdots \ge 0$. Let $\Lambda = F_1^*$ be the set of all continuous linear functionals on F_1 and let F be the unit ball of

l_p. To guarantee that the (ε, α)-verification problem can be solved for arbitrary positive ε and α we must assume that $\lim_i \lambda_i = 0$.

3.3.1. Necessary Conditions on Cardinality

We now prove necessary conditions on n such that the (ε, α)-verification problem can be solved using adaptive information of cardinality n. For our proof we use Theorem 3.2 with a suitable $g \in G_1$. It turns out that the appropriate choice of g depends on p and is given by

$$g = \varepsilon \sum_{i=1}^{n+1} e_i. \tag{3.4}$$

for $p = \infty$, and

$$g = (n+1)^{-1/p}\, \varepsilon \sum_{i=1}^{n+1} e_i \tag{3.5}$$

for $2 < p < \infty$, and finally

$$g = \varepsilon\, e_1 \tag{3.6}$$

for $1 \le p \le 2$.

Observe that we have $\|g\| = \varepsilon$ in each case. Let

$$X^* = \{f \in l_p : \; f_i = 0 \text{ for } i \ge n+2\}.$$

For any adaptive information N of cardinality n we consider the set

$$X = \{f \in l_p : \; N_g(f) = 0\} \cap X^*.$$

Note that X is a linear space with dimension at least one. Observe that the elements of $F \cap X$ cannot be distinguished from $0 \in F \cap X$ by the information N_g. We use Theorem 3.2 for the element g and the information N_g. Since $\|g\| = \varepsilon$, we have $0 \in B(g, \varepsilon) \cap S N_g^{-1}(0)$. Thus, the (ε, α)-verification problem is solvable (for g using N_g) only if

$$\sup_{f \in F \cap X} \|g - S(f)\| \le (1+\alpha)\, \varepsilon.$$

Since $F \cap X$ is balanced, i.e., $f \in F \cap X$ implies that $-f \in F \cap X$, we can rewrite the last estimate as

$$\sup_{f \in F \cap X} \max\left(\|g + S(f)\|\,,\; \|g - S(f)\|\right) \;\le\; (1+\alpha)\, \varepsilon.$$

Define

$$\beta = \inf_{f \in X^*,\, \|f\|=1} \max\left(\|g + S(f)\|\,,\; \|g - S(f)\|\right). \tag{3.7}$$

Clearly, β is no greater than the right hand side of the previous estimate. Hence, if the (ε,α)-verification problem is solvable for adaptive information of cardinality n then we have

$$\beta \le (1+\alpha)\,\varepsilon. \tag{3.8}$$

Clearly, β may depend on all the eigenvalues $\lambda_1,\dots,\lambda_{n+1}$. We will prove, however, rather sharp lower bounds on β which depend only on λ_{n+1}.

We consider the three cases $p=\infty$, $2<p<\infty$, and $1\le p\le 2$ separately.

Theorem 3.4. *Assume that the (ε,α)-verification problem can be solved for $p=\infty$ by using adaptive information of cardinality n. Then we have*

$$\lambda_{n+1} \le \varepsilon\,\alpha.$$

Proof. We take g as in (3.4) and estimate β given by (3.7). Let $f\in X^*$ with $\|f\|=1$. Then $|f_i|=1$ for some $i\in[1,n+1]$ and we get

$$\max(\|g+S(f)\|,\|g-S(f)\|) \ge \varepsilon+\lambda_i \ge \varepsilon+\lambda_{n+1}.$$

This proves $\beta\ge\varepsilon+\lambda_{n+1}$. Since (3.8) holds, this completes the proof. $\square$

Theorem 3.5. *Assume that the (ε,α)-verification problem can be solved for $2<p<\infty$ by using adaptive information of cardinality n. Then we have*

$$(1+\alpha)^p\,\varepsilon^p \ge \tfrac{1}{2}|\varepsilon-\lambda_{n+1}|^p+\tfrac{1}{2}|\varepsilon+\lambda_{n+1}|^p.$$

A slightly weaker (but more explicit) condition on λ_{n+1} is given by

$$\lambda_{n+1} \;\le\; \varepsilon\,\sqrt{(1+\alpha)^p-1}\,\sqrt{\frac{2}{p\,(p-1)}} \;=\; \varepsilon\,\sqrt{\alpha}\,\sqrt{2/(p-1)}\,(1+o(1)) \quad \text{as } \alpha\to 0.$$

Proof. We consider g as in (3.5) and estimate β of (3.7). We have

$$\beta \;=\; \inf_{h\in S(B)} \max\left(\|g+h\|\,,\,\|g-h\|\right),$$

where $B=\{f\in X^*:\ \|f\|=1\}$.

We now show that we get a lower bound on β if S is replaced by $\lambda_{n+1}\,\mathrm{Id}$. Indeed, note that for any $h^*\in S(B)$ there exists $\gamma\in[0,1]$ such that $h=\gamma\,h^*\in\lambda_{n+1}\,B$. Consider the function $f(x)=\|g+xh^*\|$ for $|x|\le 1$. Since f is convex, we have

$$\max_{|x|\le 1} f(x) \;=\; \max\left(\|g+h^*\|\,,\,\|g-h^*\|\right).$$

Taking $x = \gamma$ we get

$$\max\left(\|g+h\|\,,\,\|g-h\|\right) \,\le\, \max\left(\|g+h^*\|\,,\,\|g-h^*\|\right).$$

This proves that

$$\beta^p \,\ge\, \inf_{f\in B} \max\left(\sum_{i=1}^{n+1} |g_i - \lambda_{n+1}\, f_i|^p,\, \sum_{i=1}^{n+1} |g_i + \lambda_{n+1}\, f_i|^p\right).$$

Observe that all components of g are equal, $g_i = c = (n+1)^{-1/p}$. By compactness of B, the infimum is attained for some f^*. Assume that $f_i^* > 0$ and $f_j^* > 0$ with $f_i^* \ne f_j^*$. Since the function $f_i \mapsto |c - f_i\,\lambda_{n+1}|$ is convex, a modified version of f^* yields a smaller value which contradicts the minimality of f^*. Hence we see that an optimal f^* is of the form

$$f^* = \sum_{i=1}^{m} c_1 e_i - \sum_{i=m+1}^{n+1} c_2 e_i \tag{3.9}$$

for some m and nonnegative c_1 and c_2. By $\|f^*\| = 1$ we get the condition

$$c_1^p\, m + c_2^p\,(n+1-m) = 1 \tag{3.10}$$

The optimal f satisfies the condition

$$\sum_{i=1}^{n+1} |g_i - \lambda_{n+1}\, f_i|^p = \sum_{i=1}^{n+1} |g_i + \lambda_{n+1}\, f_i|^p.$$

This and (3.9) yield

$$m\,|c - \lambda_{n+1}\,c_1|^p + (n+1-m)\,|c + \lambda_{n+1}\,c_2|^p = m\,|c + \lambda_{n+1}\,c_1|^p + (n+1-m)\,|c - \lambda_{n+1}\,c_2|^p. \tag{3.11}$$

Assume, for a moment, that m is an arbitrary real number from $[0, n+1]$. Then by some simple monotonicity arguments we see that $c_1, c_2 \ge 0$ are uniquely determined by (3.10) and (3.11). These values of c_1 and c_2, of course, depend on m and it turns out that both sides of (3.11) are smallest if $m = n+1-m$, i.e., if $2m = n+1$. In this case we get $c_1 = c_2 = (n+1)^{-1/p}$ and both sides of (3.11) take the value

$$\frac{(n+1)}{2}\,|c - \lambda_{n+1}\,(n+1)^{-1/p}|^p + \frac{(n+1)}{2}\,|c + \lambda_{n+1}\,(n+1)^{-1/p}|^p \;=\; \frac{1}{2}|\varepsilon - \lambda_{n+1}|^p + \frac{1}{2}|\varepsilon + \lambda_{n+1}|^p.$$

Therefore we have proved

$$(1+\alpha)^p\,\varepsilon^p \,\ge\, \beta^p \,\ge\, \frac{1}{2}|\varepsilon - \lambda_{n+1}|^p + \frac{1}{2}|\varepsilon + \lambda_{n+1}|^p.$$

Using the binomial series we obtain

$$\lambda_{n+1}^2 \le \left((1+\alpha)^p - 1\right)\cdot \frac{2\varepsilon^2}{p\,(p-1)}$$

which completes the proof. $\square$

Theorem 3.6. *Assume that the (ε, α)-verification problem can be solved for $1 \le p \le 2$ by using adaptive information of cardinality n. Then we have*

$$\lambda_{n+1} \le \varepsilon \left((1+\alpha)^p - 1\right)^{1/p} = \varepsilon\, \alpha^{1/p}\, p^{1/p}\,(1+o(1)) \quad \text{as } \alpha \to 0. \tag{3.12}$$

Proof. We consider $g = \varepsilon\, e_1$ as in (3.6) and estimate β of (3.7). As in the proof of Theorem 3.5 we have

$$\beta^p \ge \inf_{f \in B} \max\left(\sum_{i=1}^{n+1} |g_i - \lambda_{n+1}\, f_i|^p, \sum_{i=1}^{n+1} |g_i + \lambda_{n+1}\, f_i|^p \right).$$

By compactness the infimum is attained for some f^* and because of the special form of g, we have $g_2 = \cdots = g_{n+1} = 0$, we can assume that f^* is of the form

$$f = f_1 e_1 + \sum_{i=2}^{n+1} c e_i$$

for some nonnegative f_1 and c. For such an f we have

$$\sum_{i=1}^{n+1} |g_i + \lambda_{n+1}\, f_i|^p = (f_1\, \lambda_{n+1} + \varepsilon)^p + n\, c^p\, \lambda_{n+1}^p$$

with $f_1^p + n\, c^p = 1$. For simplicity we use the estimate $(f_1\, \lambda_{n+1} + \varepsilon)^p + n\, c^p\, \lambda_{n+1}^p \ge f_1^p\, \lambda_{n+1}^p + \varepsilon^p + n\, c^p\, \lambda_{n+1}^p$, which yields

$$\beta^p \ge \varepsilon^p + \lambda_{n+1}^p.$$

Hence, we obtain the condition

$$(1+\alpha)^p\, \varepsilon^p \ge \varepsilon^p + \lambda_{n+1}^p$$

which completes the proof. $\square$

We stress that the condition (3.12) is necessary for all $1 \le p < \infty$ to solve the (ε, α)-verification problem for the element $g = \varepsilon\, e_1$. This is not important for the set G considered in this section, $S(F) + B_\varepsilon \subset G$, since the estimate of Theorem 3.5 is better for $p > 2$. This remark will be used, however, in Section 4 where we consider the set $G = S(F)$.

3.3.2. Sufficient Conditions on Cardinality

We have proved necessary conditions on n to solve the (ε, α)-verification problem by using adaptive information of cardinality n. We now present similar sufficient conditions on n.

For information independent of g a sufficient condition to solve the (ε, α)-verification problem is that the cardinality n of information is such that

$$\lambda_{n+1} \le \varepsilon\, \alpha/2. \tag{3.13}$$

This follows from Theorem 3.1 and from the known facts that the diameter of the non-adaptive information

$$N^{\mathrm{non}}(f) = [f_1, f_2 \ldots, f_n]$$

is $2\lambda_{n+1}$, and no nonadaptive (or even adaptive but independent of g) information of cardinality n has a smaller diameter. Hence, in this case solvability is directly linked with the diameter of information.

Consider first the extreme cases of p, i.e., $p = \infty$ or $p = 1$. Theorems 3.4 and 3.6 state that for such p's we have to guarantee

$$\lambda_{n+1} \le \varepsilon\, \alpha$$

even if adaptive information of cardinality n is used to solve the (ε, α)-verification problem. The last estimate differs from (3.13) only by a factor of 2. Hence, we have the following corollary.

Corollary 3.2. *Assume that the (ε, α)-verification problem can be solved for $p = \infty$ or for $p = 1$ by using adaptive information of cardinality n. Then there exists nonadaptive information N^{non} of cardinality n such that*

$$d(N^{\mathrm{non}}) \le 2\, \varepsilon\, \alpha$$

and hence the $(\varepsilon, 2\alpha)$-verification problem can be solved by using N^{non} for all $g \in G$. Thus, adaption can help at most by a factor of 2.

For $p = 1$ or $p = \infty$ it can be seen that adaption may help by a factor of 2. Indeed, consider the simple example of $S = \mathrm{Id} : \mathbb{R}^2 \to \mathbb{R}^2$ with $n = 1$ and $\varepsilon = 2$. Note that $d(N) = 2$ for any nonadaptive information of cardinality 1. Thus, we can solve this verification problem for all $g \in G_1$ using nonadaptive information iff $\alpha \ge 1$. We now show that using suitable adaptive information N_g of cardinality 1 the verification problem can be solved for all $g \in G_1$ iff $\alpha \geq 1/2$. Using Theorem 3.2 we need thus to check that

$$A = \{f \in F : N_g(f) = x, \ \|g - f\| \leq 2\} = \emptyset$$

or

$$B = \{f \in F : N_g(f) = x, \ \|g - f\| > 3\} = \emptyset$$

holds for all $g \in G_1$ and $x \in \mathbb{R}$.

We only consider the case $p = \infty$ (in $\mathbb{R}^2$ the p-norms are isometric for $p = 1$ and $p = \infty$) and due to symmetry we may assume that $g = (g_1, g_2)$ with $0 \leq g_1 \leq g_2$. If $g_2 \leq 2$ or $g_2 > 3$ the problem is trivial, i.e., A or B is empty no matter how N_g is defined. Hence, assume that $2 < g_2 \leq 3$.

If $g_1 \leq 2$ we take $N_g(f) = f_2$. Then $A \neq \emptyset$ implies that $B = \emptyset$.

If $g_1 > 2$ we take $N_g(f) = f_1 + f_2$. Assume that $N_g(f) \geq g_1 + g_2 - 4$. Then we have $f_1 \geq g_1 + g_2 - 5$ and $f_1 > g_1 - 3$ and similarly $f_2 > g_2 - 3$. Thus, $\|g - f\| < 3$ and $B = \emptyset$. If $N_g(f) = f_1 + f_2 < g_1 + g_2 - 4$ then $|f_i - g_i| > 2$ for $i \in \{1, 2\}$ and $A = \emptyset$.

Consider now the case $p \in (1, \infty)$. We show that for such p's adaptive information dependent on g helps. We use the following idea. First we compute the nonadaptive information $N_{n-1}^{\text{non}}(f) = [f_1, \ldots, f_{n-1}]$ and approximate $S(f)$ by its first $n-1$ components. Then we choose a suitable linear functional $L_g : F \to \mathbb{R}$ which depends on g and which allows to estimate $\|g - S(f)\|$ with minimal error. This idea was already used in the Hilbert space case, see Theorem 3.3.

Let $h = S(f)$. We have

$$\|g\| - \|h\| \leq \|g - h\| \leq \|g\| + \|h\|$$

and these inequalities can not be improved in general if nothing else is known about h. We want to improve these inequalities by computing $L_g(h)$ for a suitable linear functional L_g. In the case $p = 2$ we take $L_g(h) = (g, h)$ and obtain

$$\|g - h\|^2 = \|g\|^2 - 2L_g(h) + \|h\|^2.$$

Usually we know only an estimate of $\|h\|$ of the form $\|h\| \leq k$, and therefore

$$\|g\|^2 - 2L_g(h) \leq \|g - h\|^2 \leq \|g\|^2 - 2L_g(h) + k^2. \tag{3.14}$$

The estimate (3.14) leads to much better results for the (ε, α)-verification problem, see Theorem 3.3.

A similar improvement does not hold for $p \neq 2$ if we compute $L_g(h) = (g, h)$. Due to the different shape of the unit ball in l_p, it turns out that we should compute

$$L_g(h) = \sum_{n=1}^{\infty} |g_i|^{p-1} \operatorname{sign}(g_i)\, h_i. \tag{3.15}$$

Here $g, h \in l_p$ and $1 < p < \infty$. Note that Hölder's inequality yields

$$|L_g(h)| \le \|h\|_p \cdot \|g\|_p^{p-1}$$

and hence L_g is well defined and continuous. The following lemma contains the inequalities that are analogous to (3.14) for $p \neq 2$.

Lemma 3.7. *Assume that $g \in l_p$ and $L_g : l_p \to \mathbb{R}$ is defined in (3.15). Then for each $h \in l_p$ the following inequalities hold:*

$$\|g\|^p - p\, L_g(h) \le \|g - h\|^p \le \|g\|^p - p\, L_g(h) + 2\, \|h\|^p, \qquad \textit{if } 1 < p \le 2, \tag{3.16}$$

$$\|g\|^p - p\, L_g(h) \le \|g - h\|^p \le \|g\|^p - p\, L_g(h) + (2^p - 1 - p) \cdot (\|h\|^p + \|h\|^2\, \|g\|^{p-2}), \tag{3.17}$$

if $2 \le p < \infty$.

Proof. Let us first address the case $p \in (1, 2]$. Let g and h be any two real numbers. Suppose we can show that

$$|g|^p - p|g|^{p-1}\operatorname{sign}(g)h \le |g - h|^p \le |g|^p - p|g|^{p-1}\operatorname{sign}(g)h + 2|h|^p. \tag{3.18}$$

It is clear that (3.16) follows from (3.18), so we prove (3.18). This holds if $g = 0$ or $h = 0$. Thus, we can assume that both numbers are different from zero.

If $g < 0$ we multiply both g and h by -1 and so we see that it is enough to consider the case $g > 0$. Now dividing both sides of (3.18) by g^p we see that it is enough to consider the case $g = 1$. This means that we need only to check whether

$$0 \le |1 + x|^p - 1 - px \le 2|x|^p. \tag{3.19}$$

For $x \neq 0$, consider the function

$$f(x) = \frac{|1 + x|^p - 1 - px}{|x|^p}.$$

From Bernoulli's inequality, we have $f(x) \ge 0$. Moreover:

a) f is increasing for $x > 0$, hence $0 \le f(x) \le 1$ for $x > 0$.

b) f is decreasing for $-1 \le x < 0$, hence $0 \le f(x) \le 1$ for $-1 \le x < 0$.

c) For $x < -1$ we have

$$f(y) = \frac{(y-1)^p - 1 + py}{y^p},$$

where $y = -x$, i.e., $y > 1$. This means

$$f(y) = \frac{(y-1)^p}{y^p} + \frac{py-1}{y^p}.$$

Again using Bernoulli's inequality, we have

$$\frac{py-1}{y^p} = \frac{p(z+1)-1}{(z+1)^p} \le \frac{p(z+1)-1}{1+pz} = \frac{(p-1)+pz}{1+pz} \le 1,$$

where $z = y - 1 > 0$. Thus, each term of $f(y)$ is at most one. Hence, $f(y) \le 2$ which proves (3.19).

It can easily be seen that the constant 2 on the right side of (3.18) or (3.19) is optimal, i.e., the inequality $0 \le f(x) \le 2$ cannot be improved simultaneously for all $p \in (1,2)$. Indeed, if p tends to 1, the optimal constant on the right side tends to 2.

Consider now the case $p \ge 2$. Note that

$$\sum_{i=1}^{\infty} h_i^2 \cdot |g_i|^{p-2} \le \|h\|_p^2 \cdot \|g\|_p^{p-2}. \tag{3.20}$$

Due to (3.20) we see that (3.17) follows from

$$|g|^p - p|g|^{p-1}\mathrm{sign}(g)h \le |g-h|^p \le |g|^p - p|g|^{p-1}\mathrm{sign}(g)h + (2^p - 1 - p)\cdot(h^2|g|^{p-2} + |h|^p), \tag{3.21}$$

where $g, h \in \mathbb{R}$. To prove (3.21) we first notice that it is enough to prove

$$0 \le |1+x|^p - 1 - px \le (2^p - 1 - p)\cdot(x^2 + |x|^p),$$

where again $x \ne 0$.

So we study the functions

$$f_1(x) = \frac{(1+x)^p - 1 - px}{x^2}$$

for $|x| \le 1$ and

$$f_2(x) = \frac{|1+x|^p - 1 - px}{|x|^p}$$

for $|x| \geq 1$. Both functions are positive. It is then enough to prove that both functions are bounded (on their respective domains) by $2^p - 1 - p$. The first function is increasing and $f(1) = 2^p - 1 - p$. The second function is increasing for $x < 0$ and decreasing for $x > 0$ and therefore it is enough to check $f_2(-1)$ and $f_2(1)$ to get $f_2(x) \leq 2^p - 1 - p$ for all $x \leq -1$ or $x \geq 1$.

The constant $(2^p - 1 - p)$ is clearly not optimal in (3.17) or (3.21) but, of course, the best constant is bigger than $0.5(2^p - 1 - p)$ and it can be shown that 0.5 can be replaced by 0.8; thus, there is not much room for improvement. $\square$

We are ready to prove sufficient conditions on the cardinality of the adaptive information

$$N_g(f) = [f_1, f_2, \dots, f_{n-1}, L_g(S(f))], \tag{3.22}$$

which solves the (ε, α)-verification problem. Here, the functional L_g is given by (3.15). Observe that N_g is only mildly adaptive since only one functional depends on g.

Theorem 3.8.

Assume that $1 < p \leq 2$. Choose n such that

$$2\,\lambda_n^p \leq \varepsilon^p\,((1+\alpha)^p - 1). \tag{3.23}$$

Then the (ε, α)-verification problem can be solved for each $g \in G$ by using N_g of (3.22).

Assume that $2 \leq p < \infty$. Choose n such that

$$(2^p - 1 - p) \cdot (\lambda_n^2\,(\lambda_n + \varepsilon)^{p-2} + \lambda_n^p) \leq \varepsilon^p\,((1+\alpha)^p - 1). \tag{3.24}$$

Then the (ε, α)-verification problem can be solved for $g \in G$ by using N_g of (3.22).

Proof. Let $1 < p \leq 2$. Then the repetitive use of (3.19) yields

$$\gamma \leq \|g - S(f)\|^p \leq \gamma + 2\sum_{i=n}^{\infty} |\lambda_i f_i|^p \leq \gamma + 2\lambda_n^p,$$

where

$$\gamma = \sum_{i=1}^{n-1} |g_i - \lambda_i f_i|^p + \sum_{i=n}^{\infty} |g_i|^p - pL_g(S(f)) + p\sum_{i=1}^{n-1} |g_i|^{p-1}\mathrm{sign}(g_i) f_i \lambda_i.$$

Observe that γ can easily be computed if $N_g(f)$ is known. Define $U(f, g) = \text{YES}$ if $\gamma \leq \varepsilon^p$ and $U(f, g) = \text{NO}$ if $\gamma > \varepsilon^p$. Then U solves the (ε, α)-verification problem if

$$2\lambda_n^p \leq \varepsilon^p((1+\alpha)^p - 1).$$

Indeed, $\|g - S(f)\| \le \varepsilon$ implies $\gamma \le \varepsilon^p$ and $\mathrm{VER}(f,g) = U(f,g) = \mathrm{YES}$. If $\|g - S(f)\| > (1+\alpha)\varepsilon$ then $\gamma > (1+\alpha)^p \varepsilon^p - 2\lambda_n^p \ge \varepsilon^p$, and $\mathrm{VER}(f,g) = U(f,g) = \mathrm{NO}$, as claimed.

Now, let $2 \le p < \infty$. Then the repetitive use of (3.21) yields

$$\gamma \le \|g - S(f)\|^p \le \gamma + (2^p - 1 - p) \cdot \sum_{i=n}^{\infty} (|f_i \lambda_i|^2 |g_i|^{p-2} + |f_i \lambda_i|^p),$$

where

$$\gamma = \sum_{i=1}^{n-1} |g_i - \lambda_i f_i|^p + \sum_{i=n}^{\infty} |g_i|^p - p L_g(S(f)) + p \sum_{i=1}^{n-1} |g_i|^{p-1} \mathrm{sign}(g_i) f_i \lambda_i.$$

If $\mathrm{dist}(g, S(F)) > \varepsilon$ then $U(f,g) = \mathrm{NO}$ solves the problem. So we may assume that

$$g = S(f^*) + h^*, \qquad \|f^*\| \le 1, \quad \|h^*\| \le \varepsilon. \tag{3.25}$$

For such an element g, define $U(f,g) = \mathrm{YES}$ if $\gamma \le \varepsilon^p$ and $U(f,g) = \mathrm{NO}$ if $\gamma > \varepsilon^p$. As before, it is easy to check that U solves the (ε, α)-verification problem if

$$\beta := (2^p - 1 - p) \cdot \sum_{i=n}^{\infty} (|f_i \lambda_i|^2 |g_i|^{p-2} + |f_i \lambda_i|^p) \le \varepsilon^p \left((1+\alpha)^p - 1\right).$$

Using the form (3.25) of g and (3.20) we obtain

$$\beta = (2^p - 1 - p) \cdot \sum_{i=n}^{\infty} (|f_i \lambda_i|^2 |f_i^* \lambda_i + h_i^*|^{p-2} + |f_i \lambda_i|^p) \le (2^p - 1 - p) \cdot (\lambda_n^2 \, (\lambda_n + \varepsilon)^{p-2} + \lambda_n^p).$$

This completes the proof. $\square$

Assume now that $\alpha \ll 1$. Then Theorem 3.5, 3.3 and 3.6 yield asymptotically in α the necessary conditions

$$\begin{aligned} \lambda_{n+1} &\le \varepsilon \, \alpha^{1/p} \, p^{1/p} \, (1 + o(1)) && \text{if } 1 < p \le 2, \\ \lambda_{n+1} &\le \varepsilon \sqrt{\alpha(2+\alpha)} && \text{if } p = 2, \\ \lambda_{n+1} &\le \varepsilon \sqrt{\alpha} \sqrt{2/(p-1)} \, (1 + o(1)) && \text{if } 2 < p < \infty, \end{aligned} \tag{3.26}$$

while Theorems 3.8 and 3.3 yield asymptotically in α the sufficient conditions

$$\begin{aligned} \lambda_n &\le \varepsilon \, \alpha^{1/p} \, (p/2)^{1/p} \, (1 + o(1)) && \text{if } 1 \le p < 2, \\ \lambda_n &\le \varepsilon \sqrt{\alpha(2+\alpha)} && \text{if } p = 2, \\ \lambda_n &\le \varepsilon \sqrt{\alpha} \sqrt{p/(2^p - 1 - p)} \, (1 + o(1)) && \text{if } 2 < p < \infty. \end{aligned} \tag{3.27}$$

Note that the indices of the eigenvalues λ_i in (3.26) and (3.27) differ by one. This is not essential since with one extra evaluation of f_n in (3.22) and (f, e_n) in (3.3), we may replace λ_n in (3.27) by λ_{n+1}.

Hence, modulo multiplicative constants, the necessary and sufficient conditions coincide. This and (3.13) yield the following corollary.

Corollary 3.3. *Adaption helps for diagonal operators in l_p with $p \in (1, \infty)$. More precisely, to solve the (ε, α)-verification problem we need to guarantee that*

$$\lambda_{n+1} \le \varepsilon\, \alpha/2$$

if nonadaptive information of cardinality n is used, and

$$\lambda_n \le \varepsilon\, \alpha^{1/p}\, \beta_p, \qquad \text{if } p \in (1,2],$$
$$\lambda_n \le \varepsilon \sqrt{\alpha}\, \beta_p, \qquad \text{if } p \in [2,\infty)$$

if adaptive information of cardinality n is used. Here,

$$\beta_p/(1+o(1)) \in [(p/2)^{1/p}, p^{1/p}] \qquad \text{if } p \in (1,2],$$
$$\beta_p/(1+o(1)) \in [\sqrt{p/(2^p-1-p)}, \sqrt{2/(p-1)}] \qquad \text{if } p \in [2,\infty).$$

4. Verification for the Solution Set $G = S(F)$

In this section we restrict the choice of the set to the case $G = S(F)$ and check how this choice of G improves the results of Section 3.

In Section 3 we showed that information N independent of g cannot solve the (ε, α)-verification problem for G containing $S(F) + B_\varepsilon$ if

$$d(N) > \varepsilon\, \alpha.$$

One can hope to relax this inequality for smaller sets G. Indeed, for $G = S(F)$ the (ε, α)-verification problem cannot be solved by using information N independent of g with

$$d(N) > (1+\alpha)\, \varepsilon.$$

The proof is easy. It is enough to consider f_1 and f_2 from F for which $N(f_1) = N(f_2)$ and $\|S(f_1) - S(f_2)\| > (1+\alpha)\, \varepsilon$. Then the (ε, α)-verification problem cannot be solved for

$g = S(f_1)$. Indeed, on the one hand, $\mathrm{VER}(f_1, g) = \mathrm{YES}$ and $\mathrm{VER}(f_2, g) = \mathrm{NO}$, while on the other hand, any approximation U that uses N must give the same answer for both f_i.

As we shall see, for some problems with $G = S(F)$ the (ε, α)-verification problem can be solved by using N only if $d(N) \le \varepsilon\,\alpha$, even though information may depend on g. For some other problems, it will be enough to assume that $d(N) \le \varepsilon((1+\alpha)^p - 1)^{1/p}$ for $p \in [1, +\infty)$ or only that $d(N) \le (1+\alpha)\,\varepsilon$.

4.1. Linear Functionals

In this subsection we assume that S is a linear functional, $S : F_1 \to \mathbb{R}$, and F is a symmetric and convex subset of F_1. We also assume that the class Λ consists of linear functionals. Obviously, to make the problem nontrivial we require that $S \notin \Lambda$.

Suppose first that

$$\sup_{f \in F} S(f) \le (1+\alpha)\,\varepsilon/2.$$

Then the (ε, α)-verification problem for $G = S(F)$ is trivial. Indeed, $\mathrm{diam}(S(F)) \le (1+\alpha)\,\varepsilon$ and $|S(f) - g| > (1+\alpha)\,\varepsilon$ cannot happen for $f \in F$ and $g \in G$. Hence the approximation $U(f, g) \equiv \mathrm{YES}$ solves the problem.

For technical reasons we shall assume that

$$\sup_{f \in F} S(f) > \varepsilon + \varepsilon\alpha/2. \tag{4.1}$$

This means that we do not cover the case

$$(1+\alpha)\,\varepsilon/2 < \sup_{f \in F} S(f) \le \varepsilon + \varepsilon\alpha/2.$$

Usually, (4.1) is not restrictive for small ε and α.

We now show that the estimate $d(N) \le \varepsilon\,\alpha$ of Theorem 3.1 cannot be improved by permitting adaptive information N, which in particular may depend on g.

Theorem 4.1. *Assume that the (ε, α)-verification problem can be solved for $G = S(F)$ by using adaptive information N of cardinality n. Then there exists a nonadaptive information operator N^{non} of cardinality n such that*

$$d(N^{\mathrm{non}}) \le \varepsilon\,\alpha$$

and hence the (ε, α)-verification problem can be solved by using N^{non} even for all $g \in G_1$.

Proof. Let $g = \varepsilon + \varepsilon\alpha/2$. Since $S(F)$ is an interval, (4.1) yields that $g \in G = S(F)$. The information $N_g = N(\cdot; g) : F \to \mathbb{R}^n$ is of the form

$$N_g(f) = [L_{1,g}(f), L_{2,g}(f), \dots L_{n,g}(f)],$$

where $L_{i,g} \in \Lambda$ may depend on the already computed values $L_{1,g}(f), \dots, L_{i-1,g}(f)$. For $f = 0 \in F$ we get some $L^0_{i,g}$ from Λ and so we can define the nonadaptive linear information $N^{\rm non}$ of cardinality n,

$$N^{\rm non}(f) = [L^0_{1,g}(f), \dots L^0_{n,g}(f)].$$

It is well known that

$$d(N_g) \ge d(N^{\rm non}) = 2\ \sup\{S(f) :\ f \in F,\ N^{\rm non}(f) = 0\}.$$

Consider the symmetric and convex set

$$A = \{S(f) :\ f \in F,\ N_g(f) = 0\} = \{S(f) :\ f \in F,\ N^{\rm non}_g(f) = 0\}.$$

Note that $\mathrm{diam}(A) = d(N^{\rm non})$. If the diameter of the set A is greater than $\varepsilon\,\alpha$ then the (ε, α)-verification problem cannot be solved for the element g by using the information $N(\cdot; g) = N_g$. Indeed, we can find elements f_1 and f_2 from F such that $N^{\rm non}(f_1) = N^{\rm non}(f_2) = 0$ and $S(f_1) < -\varepsilon\,\alpha/2$ and $S(f_2) = \varepsilon\,\alpha/2$. Then $\mathrm{VER}(f_1, g) = \mathrm{NO}$ and $\mathrm{VER}(f_2, g) = \mathrm{YES}$. Since $U(f_1, g) = U(f_2, g)$ for any U using N, the problem cannot be solved.

Thus, the diameter of the set A is at most $\varepsilon\,\alpha$ and we have $d(N^{\rm non}) \le \varepsilon\,\alpha$. Due to Theorem 3.1 we can solve the verification problem using $N^{\rm non}$ even for all $g \in G_1$. $\square$

Theorem 4.1 means that adaption does not help for the (ε, α)-verification problem for linear functionals for which (4.1) holds.

4.2. Diagonal Operators in l_p

In this subsection we consider diagonal operators in l_p, see Section 3.3, for $p \in [1, +\infty]$ with $G = S(F)$. We show that adaption does not help much for these problems. For nonadaptive information, the dependence on α is a function of p and may be quite different than in the inequality $d(N) \le \varepsilon\,\alpha$ for $S(F) + B_\varepsilon \subset G$. Namely, there exists nonadaptive information of cardinality n that solves the (ε, α)-verification problem if $\lambda_n \le \varepsilon/2\,((1 + \alpha)^p - 1)^{1/p}$ for $p \in [1, +\infty)$, and $\lambda_n \le \varepsilon(1+\alpha)/2$ for $p = +\infty$. For small α and $p \in [1, +\infty)$

we get the condition $\lambda_n \le \varepsilon\, \alpha^{1/p}\, p^{1/p}/2\,(1 + o(1))$. Thus the dependence on α improves with large p.

The dependence on α is especially striking for $p = +\infty$. If G contains $S(F) + B_\varepsilon$ we showed in Theorem 3.4 that adaption does not help much and that $d(N) \le \varepsilon\alpha$ must be assumed to solve the (ε, α)-verification problem by information independent of g. If $G = S(F)$ we can solve the (ε, α)-verification problem by using nonadaptive N of cardinality n if $\lambda_n \le (1 + \alpha)\varepsilon/2$. Thus, even for $\alpha = 0$ we can solve the problem if $\lambda_n \le \varepsilon/2$. This shows that the choice of $G = S(F)$ is a very powerful source of information in this case.

On the other hand, if $p = 1$, then for both cases $G = S(F)$ and $S(F) + B_\varepsilon \subset G$ we get the same dependence on α since we have to guarantee that $\lambda_{n+1} \le \varepsilon\alpha$.

We study diagonal operators in l_p and we use the same notation as in Section 4.1. To avoid the trivial case we require that $\varepsilon \le \lambda_1$.

Theorem 4.2. *If the (ε, α)-verification problem can be solved for $G = S(F)$ by using adaptive information N of cardinality n then*

$$\lambda_{n+1} \le \varepsilon\,((1 + \alpha)^p - 1)^{1/p},$$

if $1 \le p < \infty$ and $\lambda_{n+1} \le \varepsilon(1 + \alpha)$ if $p = \infty$.

The nonadaptive information operator

$$N^{\mathrm{non}}(f) = [f_1, f_2, \dots, f_n]$$

solves the (ε, α)-verification problem if

$$\lambda_{n+1} \le \varepsilon/2((1 + \alpha)^p - 1)^{1/p}$$

in the case $1 \le p < \infty$ and $\lambda_{n+1} \le \varepsilon(1 + \alpha)/2$ if $p = \infty$.

Proof. We have already proved the lower bound on the cardinality of N_g for $g = \varepsilon e_1 \in S(F)$ and $1 \le p < \infty$, see Theorem 3.6 and the remark thereafter. The proof in the case $p = \infty$ is even simpler.

We now show that the (ε, α)-verification problem can be solved for any $g \in S(F)$ by using N^{non} if $\lambda_{n+1} \le \varepsilon/2((1 + \alpha)^p - 1)^{1/p}$ with $1 \le p < \infty$. Indeed, knowing $N^{\mathrm{non}}(f)$ and g we can compute $\beta^p = \sum_{1 \le i \le n} |\lambda_i\, f_i \,-\, g_i|^p$ and define

$$U(f, g) = \begin{cases} \text{YES} & \text{if} \quad \beta \le \varepsilon, \\ \text{NO} & \text{if} \quad \beta > \varepsilon. \end{cases}$$

Then

$$\|g - S(f)\|^p = \beta^p + \sum_{i=n+1}^{\infty} |g_i - \lambda_i\, f_i|^p.$$

Since $g \in S(F)$ we obtain

$$\|g - S(f)\|^p \;\le\; \beta^p \;+\; (2\lambda_{n+1})^p.$$

Hence the (ε, α)-verification problem is solvable if

$$(2\lambda_{n+1})^p \le \varepsilon^p\, (1 + \alpha)^p - \varepsilon^p$$

This completes the proof for the case $p < \infty$.

In the case $p = \infty$ we compute $\beta = \max_{1 \le i \le n} |\lambda_i\, f_i \;-\; g_i|$ and define

$$U(f, g) = \begin{cases} \text{YES} & \text{if} \quad \beta \le \varepsilon, \\ \text{NO} & \text{if} \quad \beta > \varepsilon. \end{cases}$$

Then

$$\|g - S(f)\| = \max(\beta,\; \max_{i \ge n+1} |g_i - \lambda_i\, f_i|).$$

Since $g \in S(F)$ we have $|g_i| \le \lambda_i$ and we obtain

$$\|g - S(f)\| \;\le\; \max(\beta\,,\, 2\lambda_{n+1}).$$

Hence the (ε, α)-verification problem is solvable if

$$2\lambda_{n+1} \le \varepsilon\, (1 + \alpha).$$

This completes the proof. $\square$

5. Complexity

In this section we apply the previous results to derive the complexity bounds for the (ε, α)-verification problem and compare them to the complexity of the computational problem.

The complexity is defined as the minimal cost needed to solve the problem in the worst case setting. The cost is defined by assuming that the evaluation of any functional from Λ costs $c > 0$, and that we can add two elements of G_1, multiply a real number by an element of G_1, and check whether $\|g\| \le a$ for any $g \in G_1$ and any $a \in \mathbb{R}$ with cost taken as unity.

We denote the ε-complexity of the computational problem by $\mathrm{comp}^{\mathrm{com}}(\varepsilon)$ and the (ε, α)-complexity of the verification problem by $\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha)$. We present relations between them. For simplicity, we sometimes ignore additive constants of order 1 as well as we do not distinguish between c and $c+2$. This simplification is denoted by the symbol $\asymp$ instead of the symbol $=$.

Obviously, from Section 3 we conclude that for all problems,

$$\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \ \le \ \mathrm{comp}^{\mathrm{com}}(\varepsilon\, \alpha/2) \ + \ 1.$$

In general, this inequality is sharp. For linear functionals studied in Section 4.1 we have

$$\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \asymp \mathrm{comp}^{\mathrm{com}}(\varepsilon\, \alpha/2).$$

On the other hand, for some special problems we have better bounds. In particular, for diagonal operators in a Hilbert space studied in Section 3.2 we have

$$\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \asymp \mathrm{comp}^{\mathrm{com}}(\varepsilon\, \sqrt{\alpha(2+\alpha)}).$$

The (ε, α)-complexity of the verification problem depends, in particular, on the set G. For G containing $S(F) + B_\varepsilon$ and for diagonal operators in l_p studied in Section 3 we have asymptotically in α,

$$\begin{aligned}
&\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \asymp \mathrm{comp}^{\mathrm{com}}\left(\varepsilon\, \alpha^{1/p}\, \beta_p\right), \qquad && \text{if } 1 \le p \le 2,\\
&\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \asymp \mathrm{comp}^{\mathrm{com}}\left(\varepsilon\, \sqrt{\alpha}\, \beta_p\right), && \text{if } 2 \le p < \infty,\\
&\mathrm{comp}^{\mathrm{ver}}(\varepsilon, \alpha) \asymp \mathrm{comp}^{\mathrm{com}}\left(\varepsilon\, \alpha\, \beta_\infty\right), && \text{if } p = \infty,
\end{aligned}$$

where β_p is given as in Corollary 3.3 for $p \in (1, \infty)$, and $\beta_1, \beta_\infty \in [1/2, 1]$.

This means that the complexity of the (ε, α)-verification problem can have different relations with the complexity of the respective computation problem. In particular, the dependence on the parameter α varies.

For $p \in (1, \infty)$, the (ε, α)-verification complexity is obtained by *adaptive* information (3.22). If nonadaption is used then the (ε, α)-verification problem can be solved in cost at least equal to $\mathrm{comp}^{\mathrm{com}}(\varepsilon\alpha)$. Thus, $\alpha^{1/p}$ or $\sqrt{\alpha}$ for the adaptive case is replaced by α for the nonadaptive case. This proves that adaption helps significantly.

On the other hand, if $G = S(F)$ then for diagonal operators in l_p studied in Section 4 we have asymptotically in α,

$$\begin{aligned} \mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha) &\asymp \mathrm{comp}^{\mathrm{com}}\left(\varepsilon\,\alpha^{1/p}\,p^{1/p}\gamma_p\right), && 1 \le p < \infty, \\ \mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha) &\asymp \mathrm{comp}^{\mathrm{com}}\left(\varepsilon\,\gamma_\infty\right), && p = \infty, \end{aligned}$$

where $\gamma_p/(1+o(1)) \in [1/2, 1]$.

Unlike the previous choice of G, adaption does not help now. Indeed, the (ε,α)-verification complexity is obtained by using *nonadaptive* information of Theorem 4.2. The extra a priori information $G = S(F)$ makes the use of adaption no more powerful than nonadaption.

Comparing the complexity of the (ε,α)-verification problem for these two choices of the set G, we see that they are roughly the same if $p \in [1,2]$. For $p \in (2,\infty)$, the dependence on $\sqrt{\alpha}$ remains for the set G containing $S(F) + B_\varepsilon$, and decreases with increasing p as $\alpha^{1/p}$ for the set $G = S(F)$. The most striking difference is for $p = \infty$. Then α^1 is present for the set G containing $S(F) + B_\varepsilon$, but disappears for the set $G + S(F)$.

We illustrate the difference between the complexities assuming that the eigenvalues λ_i are equal to $i^{-1/q}$ for some positive q. Let $\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;G)$ be the complexity of the (ε,α)-verification problem for the set G. For simplicity we consider two sets, $G = G_1$ and $G = S(F)$. Then we have

$$\begin{aligned} \frac{\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;G_1)}{\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;S(F))} &= \Theta(1) && \text{if } 1 \le p \le 2, \\ \frac{\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;G_1)}{\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;S(F))} &= \Theta\left(\left(\frac{1}{\alpha}\right)^{q\,\frac{p-2}{2p}}\right) && \text{if } 2 < p < \infty, \\ \frac{\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;G_1)}{\mathrm{comp}^{\mathrm{ver}}(\varepsilon,\alpha;S(F))} &= \Theta\left(\left(\frac{1}{\alpha}\right)^{q}\right) && \text{if } p = \infty. \end{aligned}$$

Thus, the ratio of the complexities goes to infinity as α goes to zero for $p > 2$. In this case, the additional information given by $G = S(F)$ makes the (ε,α)-verification problem much easier than the same problem for $G = G_1$ (or $G = S(F) + B_\varepsilon$).

Acknowledgments

We thank A. Papageorgiou, A. G. Werschulz and J. F. Traub for valuable comments.

References

H. Woźniakowski (1990): Complexity of Verification and Computation for IBC Problems, to appear in J. Complexity.