Norms of Matrices and Convergence of Iterative Processes

Pták, Vlastimil
1996

INSTITUTE OF COMPUTER SCIENCE

ACADEMY OF SCIENCES OF THE CZECH REPUBLIC

Norms of matrices and convergence of iterative processes

Vlastimil Pták

Technical report No. 658

March 11, 1996

Institute of Computer Science, Academy of Sciences of the Czech Republic
Pod vodárenskou věží 2, 182 07 Prague 8, Czech Republic
phone: (+422) 66414244 fax: (+422) 8585789
e-mail: uivt@uivt.cas.cz

INSTITUTE OF COMPUTER SCIENCE

ACADEMY OF SCIENCES OF THE CZECH REPUBLIC

Norms of matrices and convergence of iterative processes

Vlastimil Pták

Technical report No. 658

March 11, 1996

Abstract

The critical exponent of a Banach space E is the smallest integer q with the following property: if T is a contractive on E then the spectral radius of T is less than one if and only if $|T^q| < 1$. If q is the critical exponent of a finite-dimensional Banach space E then, it follows from compacturs that, for each $r < 1$, then maximum of $|T^q|$ under the constraints $|T| \leq 1$, $r(T) \leq r$ is less.

In the case of Hilbert space of dimension n the critical exponent equals n and it is possible to evaluate the above maxinimu for every $r \leq 1$. This is a particular case of a general maximum problem in a Banach algebra A. To compute the supremum of $|h(a)|$ as a ranges over all $a \in A$ with $|a| \leq 1$ such that the spectrum of a is contained in a given compact set F; here h is an arbitrary function holomorphic in a neighbourhood of F.

Keywords

Spectral radius, convergence of iterative procedures

1 Introduction

The motivation of the investigatons to be reported about was an attempt to give a mathematical formulation to a general problem in the theory of iterative processes. In many cases theoretical convergence criteria are available, mostly in the form of inequalities to be satisfied by certain data concerning the process, such as norms of certain operators or bounds for certain derivatives; however, such data are not always readily available and, for a variety of other reasons, the verification of the criteria may turn out to be far from easy. Thus the following question presents itself: is it possible to disregard the theoretical criteria and test the convergence on the basis of the behaviour of a finite number of initial steps?

In this case, the crucial point is the number of steps needed to distinguish between convergence and divergence.

Formulated in a somewhat loose manner we are looking for a number q with the following property: the process either starts converging before the q-th step or it does not converge at all.

We shall be concerned with the particular case of iterative processes of the form $x^{k+1} = Ax^k + y$ where A is a given bounded linear operator on a Banach space E. It was in the case of these iteration processes that the first rigorous formulation was given. It is well known that this process converges (for each y and each initial vector x^0) if and only if the spectral radius $r(A)$ of A is less than one.

In 1959 J. Mařík and the present author proved the following theorem. Consider, for n by n complex matrices B the norm $|B| = \max_i \sum_k |b_{ik}|$ so that $|B|$ is the norm of B taken as operator on C^n equipped with the l_∞ norm $|x| = \max |x_j|$.

1.1 *Let $q = n^2 - n + 1$. Given an n by n matrix A such that $|A| = |A^q| = 1$ then $r(A) = 1$. Furthermore q is the smallest integer of this property.*

Thus, for a matrix A with $|A| \leq 1$ convergence of the process manifests itself within the first $n^2 - n + 1$ steps.

Later, the author realized that a similar question may be raised in an arbitrary Banach space and formulated [11] the following definition.

1.2 *The critical exponent of a Banach space E is the smallest integer with the following property.*

If A is a linear operator on E such that $|A| = |A^q| = 1$ then $r(A) = 1$.

An equivalent formulation

If $|A| \leq 1$ then $r(A) < 1$ if and only if $|A^q| < 1$.

In the same paper [11] the author proved that the critical exponent of n-dimensional Hilbert space equals n. The previous result of Mařík and the author appears in the form of the statement that the critical exponent of the n-dimensional l_∞ space equals $n^2 - n + 1$.

The following chapter represents a careful analysis of the spectral radius of an element in Banach algebras and its connection with the convergence of the series

$$1 + \lambda a + \lambda^2 a^2 + \dots$$

We then proceed to prove that the critical exponent of a Hilbert space equals its dimension. The following two chapters are of a technical character; we use this opportunity to present a nontraditional treatment of a classical subject, the representation of operators by matrices together with the geometry of these representations, tools to be used the in solution of the first maximum problem.

Section 6 reproduces the author's original solution of the first maximum problem: find the maximum of $|f(A)|$ as A ranges over all contractions on H_n annihilated by a given polynomial. In spite of the fact that technically simpler solutions were found later, the original one has the advantage of suggesting, in a natural manner, the consideration of dilations and presents an opportunity to explain the connections with the theory of complex functions. This presents a natural introduction to function theoretic considerations to be treated in more detail in Section 9.

The author's original solution of the first maximum problem was followed by a paper of Sz-Nagy [21] in which dilation theory was used explicitly; his proof is reproduced in Section 10. The following chapter describes the relations between the first maximum problem and dilation theory in more detail – this presents are opportunity to explain the connections with the interpolation theory of D. Sarason, Hankel operators and the von Neumann inequality. In particular, the role of (operator valued) Möbius functions in the theory as well as in concrete representations of extremal operators becomes evident.

2 The Spectrum

In the whole lecture A will be a normed algebra over the complex field. We assume that A has a unit e and identify the scalar multiple λe with the complex number λ. The norm $x \to |x|$ is submultiplicative, $|xy| \leq |x|\ |y|$ and we assume that $|e| = 1$.

The spectrum of an element $a \in A$, denoted by $\sigma(a)$ is defined as the set of all complex λ for which $\lambda - a$ is not invertible.

The main result of this section is a deep one: the spectrum of an arbitrary element of A is nonvoid. If the algebra A is complete, it can be shown that the set $\sigma(a)$ is bounded (in fact compact) and we shall show how to compute the radius of the smallest circle around the origin that contains $\sigma(a)$.

We start by proving a particular case of what is known as the spectral mapping theorem

2.1 *Let A be a normed algebra, $a \in A$. If p is an arbitrary polynomial then*

$$\sigma(p(a)) = p(\sigma(a))$$

Proof. Since we do not yet know that spectra are nonvoid, the assertion to be proved reads as follows. If one of the sets $\sigma(p(a))$ and $p(\sigma(a))$ is nonvoid then so is the other and they are equal.

1. Suppose first that $\lambda \in \sigma(a)$. The polynomial $p(z) - p(\lambda)$ being divisible by $(z - \lambda)$, there exists a polynomial $q(z)$ such that

$$p(z) - p(\lambda) = (z - \lambda)q(z).$$

If b stands for $q(a)$ we have

$$p(a) - p(\lambda) = (a - \lambda)b = b(a - \lambda).$$

Suppose that $p(a) - p(\lambda)$ has an inverse, w say. Then

$$wb(a - \lambda) = 1 \qquad \text{and} \qquad (a - \lambda)bw = 1$$

so that $\lambda - a$ is invertible, a contradiction. It follows that $p(\lambda) \in \sigma(p(a))$.

2. Suppose that $\lambda \in \sigma(p(a))$ so that $\lambda - p(a)$ is not invertible. Consider the polynomial $p(z) - \lambda$; it can be expressed as the product of n linear factors

$$p(z) - \lambda = (z - \alpha_1) \dots (z - \alpha_n).$$

It follows that

$$p(a) - \lambda = (a - \alpha_1) \dots (a - \alpha_n).$$

If all $a - \alpha_j$ were invertible, so would be $p(a) - \lambda$. Thus there exists an index k such that $a - \alpha_k$ is not invertible, in other words $\alpha_k \in \sigma(a)$. Since $p(\alpha_k) - \lambda = 0$ we have $\lambda = p(\alpha_k) \in p(\sigma(a))$. $\square$

2.2 *Let A be a Banach algebra, $a \in A$. If $\lambda \in \sigma(a)$ then $|\lambda| \le \inf |a^n|^{1/n}$.*

Proof. We prove first that $|\lambda| \le |a|$. Indeed, suppose $|\lambda| > |a|$. Then $|\frac{a}{\lambda}| < 1$, the series $1 + \frac{a}{\lambda} + (\frac{a}{\lambda})^2 + \dots$ converges and its sum b satisfies

$$\frac{b}{\lambda}(\lambda - a) = (\lambda - a)\frac{b}{\lambda} = 1$$

so that $\lambda - a$ is invertible, a contradiction.

Now consider a^n. By the spectral mapping theorem $\lambda \in \sigma(a)$ implies $\lambda^n \in \sigma(a^n)$. It follows that $|\lambda^n| \le |a^n|$ whence $|\lambda| \le |a^n|^{1/n}$. Since this estimate holds for an arbitrary n, the assertion follows. $\square$

The main question still remains open: is the spectrum of an element always nonvoid? In the preceding proposition we have used completeness to prove the convergence of the series

$$1 + \lambda a + \lambda^2 a^2 + \dots$$

and this, in its turn, to show that the points of $\sigma(a)$ (if they exist) must lie in the closed disk $|\lambda| \le \inf |a^n|^{1/n}$.

The relation between the existence of $(1 - \lambda a)^{-1}$ and the convergence of the series

$$1 + \lambda a + \lambda^2 a^2 + \dots$$

plays also the central role in the main theorem of this section which states that, in a normed algebra, the spectrum of each element is nonvoid.

In spite of the fact that we are dealing with infinite series, completeness is not needed to prove that the spectrum is nonvoid.

Let us try to explain, in the following heuristic discussion, how this fact may be deduced from an examination of the connection between the existence of $(1-\lambda a)^{-1}$ and the convergence of the series $1+\lambda a+\lambda^2 a^2+\ldots$. We begin by the following observation.

2.3 *Let A be a normed algebra, $a \in A$. Suppose that $(1-\lambda a)^{-1}$ exists in some neighbourhood of zero. Then there exists an $\varepsilon > 0$ such that for $|\lambda| < \varepsilon$, $(1-\lambda a)^{-1}$ exists and may be expressed in the form of a convergent power series*

$$(1-\lambda a)^{-1} = 1+\lambda a+\lambda^2 a^2+\ldots$$

Proof. For a positive integer n and a complex number λ, set $s_n(\lambda) = 1+\lambda a+\ldots+\lambda^n a^n$. It is easy to verify that $s_n(\lambda)(1-\lambda a) = 1-\lambda^{n+1}a^{n+1}$. If $(1-\lambda a)^{-1}$ exists then

$$\begin{aligned} s_n(\lambda)-(1-\lambda a)^{-1} &= (1-\lambda^{n+1}a^{n+1})(1-\lambda a)^{-1}-(1-\lambda a)^{-1} = \\ &= -\lambda^{n+1}a^{n+1}(1-\lambda a)^{-1}. \end{aligned}$$

Now suppose that $(1-\lambda a)^{-1}$ exists for all λ in the disk $|\lambda| < \alpha$. If $|\lambda| < \alpha$ and $|\lambda a| < 1$, the preceding identity shows that the series $1+\lambda a+\lambda^2 a^2+\ldots$ converges and its sum equals $(1-\lambda a)^{-1}$. □

The result just proved says:
if $(1-\lambda a)^{-1}$ exists in a neighbourhood of zero then the series $1+\lambda a+\lambda^2 a^2+\ldots$ has a positive radius of convergence. We intend to explain that the main theorem we are aiming at, the existence of the spectrum, is an immediate consequence of an improvement of the proposition just proved: the radius of convergence of the series $1+\lambda a+\lambda^2 a^2+\ldots$ is the largest number β such that $(1-\lambda a)^{-1}$ exists for all $|\lambda| < \beta$. We shall prove this later; now we state it without proof and explain how it can be used to obtain the existence of the spectrum.

2.4 *Let A be a normed algebra, $a \in A$, $\beta > 0$. Suppose that $(1-\lambda a)^{-1}$ exists for all λ in the disk $|\lambda| < \beta$. Then the series*

$$1+\lambda a+(\lambda a)^2+\ldots$$

converges for all $|\lambda| < \beta$.

Once proved, this result makes it possible to show that, in a normed algebra, the spectrum of every element is nonvoid, in fact, that there exists, for each $a \in A$ a $\lambda \in \sigma(a)$ with

$$\limsup |a^n|^{1/n} \le |\lambda|$$

Write, for brevity, $r_0 = \limsup |a^n|^{1/n}$. We shall distinquish two cases: r_0 positive and $r_0 = 0$. Suppose first that $r_0 > 0$. Take a positive ε such that $r_0 > r_0 - \varepsilon > 0$. We intend to show that $1 - \lambda a$ cannot be invertible for all λ in the disk $|\lambda| < \frac{1}{r_0 - \varepsilon}$. Indeed, this would imply, by the proposition just stated, the convergence of the series $1 + \lambda a + \ldots$ in the whole of the disk. Take a λ such that

$$\frac{1}{r_0 - \varepsilon} > |\lambda| > \frac{1}{r_0}.$$

We have then $\limsup |\lambda^n a^n| = |\lambda| r_0 > 1$ so that $|\lambda^n a^n| > 1$ for infinitely many n, a contradiction, since $\sum \lambda^n a^n$ is convergent. It follows that there exists a $|\lambda_0| < \frac{1}{r_0 - \varepsilon}$ for which $1 - \lambda_0 a$ is not invertible.

Clearly $\lambda_0 \neq 0$ and $\frac{1}{\lambda_0} \in \sigma(a)$ and $\frac{1}{|\lambda_0|} > r_0 - \varepsilon$. Since ε was arbitrary, this proves

$$\sup\{|\lambda|; \lambda \in \sigma(a)\} \ge r_0$$

The case $r_0 = 0$ has to be treated separately. If $r_0 = 0$ we intend to show that $0 \in \sigma(a)$, in other words, that a^{-1} does not exist. Indeed, suppose a^{-1} exists; we have then

$$1 = |(a^{-1})^n a^n| \le |a^{-1}|^n |a^n|$$

so that $1 \le |a^{-1}||a^n|^{1/n}$ for every n. Since $\lim |a^n|^{1/n} = \limsup |a^n|^{1/n} = 0$, this is a contradiction.

Summing up, we now know that $\sigma(a)$ is always nonvoid and

$$\sup\{|\lambda|; \lambda \in \sigma(a)\} \ge r_0.$$

If A is complete, we have seen that

$$\sup\{|\lambda|; \lambda \in \sigma(a)\} \le \inf |a^n|^{1/n}$$

Combining these two results (and keeping in mind htat the preceding heuristic discussion is based on the proposition 2.4 still to be proved), we obtain the following

2.5 *Let A be a Banach algebra, $a \in A$. Then $\lim |a^n|^{1/n}$ exists and equals $\inf |a^n|^{1/n}$. Denoting this number by $r(a)$, we have proved*

1^o *the spectrum $\sigma(a)$ is nonvoid*

2^o *the spectrum $\sigma(a)$ is contained in the disk $|\lambda| \le r(a)$ and there exists a $\lambda \in \sigma(a)$ with $|\lambda| = r(a)$.*

The radius of the smallest disk of the form $D(r) = \{\lambda; |\lambda| \le r\}$ such that $\sigma(a) \subset D(r)$ is called the spectral radius of a. The heuristic reasoning sketched above shows that, in a Banach algebra, the spectral radius of a equals

$$r(a) = \lim |a^n|^{1/n} = \inf |a^n|^{1/n}$$

The preceding discussion puts into evidence the importance of the behaviour of the sequence of iterates of a for the convergence of $1 + \lambda a + \lambda^2 a^2 + \ldots$ and for the existence of $(1 - \lambda a)^{-1}$.

We have shown that, in order to prove the existence of at least one point in the spectrum, it suffices to prove 2.4. (In fact, it is not difficult to see that the two assertions are equivalent.)

Now we shall resume the rigorous treatment of the subject. The following proposition examines more closely the radius of convergence of the series.

2.6 *Let B be a Banach algebra, $x \in B$. Denote by M_j the sets of complex numbers λ with the following properties.*

M_1	$\sum \lambda^n x^n$ *is absolutely convergent*
M_2	$\sum \lambda^n x^n$ *is convergent*
M_3	$(\lambda x)^n \to 0$
M_4	$\|(\lambda x)^m < 1\|$ *for some m*
M_5	*the sequence $(\lambda x)^n$ is bounded*

The supremum β of the moduli $|\lambda|$ is the same for all these sets and $\beta > 0$. The limit $|x^n|^{1/n}$ exists and satisfies

$$\lim |x^n|^{1/n} = \inf |x^n|^{1/n} = \frac{1}{\beta};$$

here $\frac{1}{\beta}$ is taken to be 0 if $\beta = \infty$.

Proof. Clearly $M_1 \subset M_2 \subset M_3 \subset M_4 \subset M_5$. It is easy to prove the following implication: if $\lambda_0 \in M_5$ and $|\lambda| < |\lambda_0|$ then $\lambda \in M_1$. Indeed, $|\lambda^n x^n| \leq |\lambda/\lambda_0|^n \; |\lambda_0^n x^n|$ and $|\lambda/\lambda_0| < 1$. This immediately implies that the supremum of $|\lambda|$ is the same for all the sets M_j. If $x = 0$ we have $\beta = \infty$. If $x \neq 0$ then every λ with $|\lambda| < \frac{1}{|x|}$ belongs to M_3. It follows that $\beta > 0$.
Let us prove first that $\frac{1}{\beta} \leq \inf |x^n|^{1/n}$. This is obvious if $\beta = \infty$. Hence assume that $\beta < \infty$ and suppose that

$$\inf |x^n|^{1/n} < \frac{1}{\beta}.$$

There exists a positive λ such that

$$\lambda \inf |x^n|^{1/n} < 1 < \frac{\lambda}{\beta}.$$

It follows that $|(\lambda x)^m < 1|$ for a suitable m so that $\lambda \leq \beta$ and $\frac{\lambda}{\beta} \leq 1$, a contradiction. This proves the inequality

$$\frac{1}{\beta} \leq \inf |x^n|^{1/n}.$$

Now observe that $\lambda \in M_3$ implies the inequality

$$|\lambda| \limsup |x^n|^{1/n} \le 1.$$

Let β' be an arbitrary number $0 < \beta' < \beta$. There exists a $\lambda \in M_3$ such that $|\lambda| > \beta'$. It follows that

$$\beta' \limsup |x^n|^{1/n} \le |\lambda| \limsup |x^n|^{1/n} \le 1$$

whence

$$\limsup |x^n|^{1/n} \le \frac{1}{\beta'}.$$

Since was an arbitrary positive number less than β, the inequality

$$\limsup |x^n|^{1/n} \le \frac{1}{\beta}$$

follows. $\square$

The reader will have observed that condition M_4 differs from the rest of M_j in that it suggests a question of a quantitative character: if $|(\lambda x)^m| < 1$ for some m it is natural to ask what would be the smallest m of this property. Indeed, it is essentially this question that will occupy us in these lectures.

We are now ready to prove the fact that, in a normed algebra, the spectrum of an arbitrary element is nonvoid. The proof is based on an algebraic identity relating the values of $(1-\lambda a)^{-1}$ to the behaviour of the iterates $\lambda^n a^n$ and on the continuity of the inverse.

2.7 *Let A be a Banach algebra with unit, $a_0 \in A$. If a_0 is invertible and $\omega = |a_0^{-1}(a_0 - a)| < 1$ then a is invertible as well and*

$$|a^{-1} - a_0^{-1}| \le |a_0^{-1}| \, \frac{\omega}{1-\omega}$$

Proof. Write a in the form

$$a = a_0 - (a_0 - a) = a_0(1 - a_0^{-1}(a_0 - a))$$

and observe that $(1 - a_0^{-1}(a_0 - a))^{-1}$ exists and its norm does not exceed $\frac{1}{1-\omega}$. Thus $|a^{-1}| \le |a_0^{-1}|\frac{1}{1-\omega}$ and

$$|a^{-1} - a_0^{-1}| = |a_0^{-1}(a_0 - a)a^{-1}| \le \omega|a^{-1}| \le |a_0^{-1}|\frac{\omega}{1-\omega}. \qquad \square$$

In particular, in a Banach algebra, the set $G(A)$ of all invertible elements is open and the mapping $a \to a^{-1}$ is continuous on $G(A)$.

If completeness is not assumed, the set $G(A)$ will not be open in general; nevertheless, continuity of the inverse remains valid.

In the case of a normed algebra we have the following

2.8 *Let A be a normed algebra with unit. Suppose that $a_0 \in A$ and $a \in A$ are both invertible. If $\omega = |a_0^{-1}(a - a_0)| < 1$ then*

$$|a^{-1} - a_0^{-1}| \leq |a_0^{-1}| \frac{\omega}{1-\omega}$$

Proof. Write

$$a^{-1} - a_0^{-1} = a_0^{-1}(a_0 - a)a^{-1} = a_0^{-1}(a_0 - a)(a_0^{-1} - (a_0^{-1} - a^{-1}))$$

Thus $|a^{-1} - a_0^{-1}| \leq \omega(|a_0^{-1}| + |a^{-1} - a_0^{-1}|)$. □

The main theorem of this section is based on an algebraic identity relating the values of the resolvent $(1 - \lambda a)^{-1}$ to the behaviour of the sequence of iterates of a and, in this manner, to the convergence of $1 + \lambda a + \lambda^2 a^2 + \ldots$. It is possible to verify the identity immendiately using known facts about the cyclotomic equation – we prefer to present an intuitive approach using rational functions.

2.9 *Let n be a positive integer, ε a primitive n-th root of 1. Then*

$$(1 - x^n)^{-1} = \frac{1}{n} \sum_1^n (1 - \varepsilon^j x)^{-1}$$

Proof. Denote by Q the polynomial

$$Q(z) = 1 + z + \ldots + z^{n-1}.$$

For every j we have

$$1 - z^n = (1 - \varepsilon^j z) Q(\varepsilon^j z)$$

so that $(1 - z^n)(1 - \varepsilon^j z)^{-1} = Q(\varepsilon^j z)$ and

$$(1 - z^n) \sum (1 - \varepsilon^j z) = \sum Q(\varepsilon^j z).$$

Thus it suffices to prove the identity $\sum Q(\varepsilon^j z) = n$. Differentiating the identity

$$(1 - y^n) = (1 - \varepsilon y)(1 - \varepsilon^2 y) \ldots (1 - \varepsilon^{n-1} y)$$

we obtain

$$n y^{n-1} = \sum \varepsilon^j \frac{1 - y^n}{1 - \varepsilon^j y} = \sum \varepsilon^j Q(\varepsilon^j y)$$

whence

$$n = \sum \frac{1}{(\varepsilon^j y)^{n-1}} Q(\varepsilon^j y) = \sum Q(\frac{1}{\varepsilon^j y}).$$

It follows that $\sum Q(\varepsilon^{-j} x) = n$; since $\sum Q(\varepsilon^j x) = \sum Q(\varepsilon^{-j} x)$, the proof is complete. □

2.10 *Let A be a normed algebra with unit. Let x be an element of A and set $r(x) = \limsup |x^n|^{1/n}$. Then there exists a point $\lambda \in \sigma(x)$ such that*

$$|\lambda| \geq r(x).$$

Proof. We shall distinguish two cases, $r(x) = 0$ and $r(x) > 0$. Suppose $r(x) = 0$ and let us prove that $0 \in \sigma(x)$. Suppose on the contrary that x^{-1} exists. Then $1 = |x^n(x^{-1})^n| \leq |x^n||x^{-1}|^n$ so that $1 \leq |x^n|^{1/n}|x^{-1}|$ for every positive n; this is a contradiction.

Now consider the case $r = r(x) > 0$. Suppose that $(\lambda - x)^{-1}$ exists for all λ with $|\lambda| \geq r$. Consider the function

$$f(\lambda) = (1 - \frac{x}{\lambda})^{-1}$$

defined for all λ with $|\lambda| \geq r$. The algebraic identity (2.9) yields the following fact. If $|\lambda| \geq r$ and if n is an arbitrary positive integer then

$$(1 - (\frac{x}{\lambda})^n)^{-1}$$

exists and may be expressed as a mean of the values of $f(z)$ on the circle $|z| = |\lambda|$.

$$(1 - (\frac{x}{\lambda})^n)^{-1} = \frac{1}{n}\sum f(\omega^j\lambda),$$

where ω is a primitive n-th root of 1.

It follows from lemma (2.8) that f is continuous on the set $|\lambda| \geq r$. In particular it is uniformly continuous on the set

$$M = \{\lambda; r \leq |\lambda| \leq r + 1\}.$$

Accordingly, for every $\varepsilon > 0$ there exists a $\sigma(\varepsilon) > 0$ such that $\lambda_1, \lambda_2 \in M$, $|\lambda_1 - \lambda_2| < \sigma(\varepsilon)$ implies

$$|f(\lambda_1) - f(\lambda_2)| < \varepsilon.$$

Now let $\varepsilon > 0$ be given. Choose a number s such that $r < s < r + \sigma(\varepsilon)$. Then, for every positive integer n the inverses

$$(1 - (\frac{x}{r})^n)^{-1} \text{ and } (1 - (\frac{x}{s})^n)^{-1}$$

both exist and their difference equals

$$\frac{1}{n}\sum(f(\omega^j r) - f(\omega^j s)).$$

Since $|\omega^j r - \omega^j s| < \sigma(\varepsilon)$ it follows that

$$|(1 - (\frac{x}{r})^n)^{-1} - (1 - (\frac{x}{s})^n)^{-1}| < \varepsilon$$

and this holds for all n. Now we shall use twice the previous lemma in the following form: if $b_n \to 1$ and the b_n are invertible then $b_n^{-1} \to 1$. First of all, $s > r$ implies $\limsup |(\frac{x}{s})^n|^{1/n} < 1$ whence $(\frac{x}{s})^n \to 0$; thus

$$|(1 - (\frac{x}{r})^n)^{-1} - 1| < \varepsilon$$

for sufficiently large n. It follows that

$$\lim(1 - (\frac{x}{r})^n)^{-1} = 1$$

so that, by the lemma

$$\lim(1 - (\frac{x}{r})^n) = 1.$$

This is a contradiction since

$$\limsup |(\frac{x}{r})^n| \geq 1. \qquad \square$$

3 The critical exponent of a finite dimensional Banach space

The definition of the critical exponent may be stated in a number of equivalent forms the connections of which we now proceed to expound. In particular the fact that the set

$$\{T \in B(E); |T| \leq 1, r(T) < 1\}$$

is not compact plays an important role in the theory; it shows that the existence a finite critical exponent represents a fairly strong restriction on the geometry of the space.

The equivalence of the following five characterizations of the critical exponent is immediate.

3.1 *Let E be a Banach space. The critical exponent q of E is the smallest positive integer which satisfies one of the following conditions*

1^0 *if $T \in B(E)$ is a contraction and $|T^q| = 1$ then $|T^r| = 1$ for all r*

2^0 *if $T \in B(E)$ is a contraction and $|T^q| = 1$ then $r(T) = 1$*

3^0 *if $T \in B(E)$ is a contraction and $|T^m| < 1$ for some m then $|T^q| < 1$*

4^0 *if $T \in B(E)$ is a contraction and $r(T) < 1$ then $|T^q| < 1$*

5^0 *if $T \in B(E)$ is a contraction then $r(T) < 1$ if and only if $|T^q| < 1$.*

Given a finite-dimensional Banach space E, we denote by $B(E)$ the Banach algebra of all linear operators on E equipped with the operator norm. For each r, $0 \leq r < 1$, let $C(r)$ be the set of all contractions $T \in B(E)$ such that $r(T) \leq r$. For each nonnegative integer q and each nonengative $r < 1$, set

$$\begin{aligned} f(q,r) &= \max\{|A^q|; A \in C(r)\} \\ &= \max\{|A^q|; A \in B(E), |A| \leq 1, r(A) \leq r\} \end{aligned}$$

Clearly, for a fixed q, the function $f(q,\cdot)$ is nondecreasing; together with the obvious estimate $f(q,r) \geq r^q$ this shows that $f(q,r) \uparrow 1$ as $r \to 1$. A moment's reflection shows that $f(q+1,r) \leq f(q,r)$ for every $r < 1$. Indeed, suppose that $f(q+1,r) > f(q,r)$ for some $r < 1$. It follows that there exists a contraction $T \in C(r)$ such that $|T^{q+1}| > f(q,r)$. This implies $f(q,r) \geq |T^q| \geq |T^{q+1}| > f(q,r)$, a contradiction.

Thus far the finite-dimensionality of E has not been used. Compactness plays an essential role in the following nontrivial result.

3.2 *Suppose E is a finite-dimensional Banach space. Then, for each $r < 1$,*

$$f(q,r) \downarrow 0$$

as $q \to \infty$.

The existence of the critical exponent is thus equivalent to the existence of an integer q such that $f(q,r) < 1$ for all $r < 1$.

Proof. For each positive integer m let $U(m)$ be the set

$$U(m) = \{x \in B(E); |x^m| < 1\}$$

The inclusion

$$C(r) \subset \bigcup U(m)$$

together with the fact that $C(r)$ is compact, yields the following observation for each $r < 1$, there exists an $n(r)$ such that

$$C(r) \subset U(n(r))$$

If we take, for $n(r)$, the smallest integer with this property, clearly $0 < r_1 < r_2$ will imply $n(r_1) \leq n(r_2)$. The existence of the critical exponent is equivalent to the statement that the function $n(r)$ remains bounded as r tends to 1, in other words, the existence of a q such that

$$\bigcup_{r<1} C(r) \subset U(q).$$

The set on the lefthand side is not compact – this shows that finite-dimensionality of E alone could hardly be expected to yield the existence of the critical exponent; indeed, it is possible to construct finite-dimensional Banach spaces whose critical exponent is infinite; the existence is thus seen to be a fairly delicate matter depending on the geometry of E.

Since $C(r)$ is compact, the inclusion $C(r) \subset U(q)$ implies the inequality $f(q,r) < 1$. It follows that $f(m,r) \downarrow 0$ as $m \to \infty$ for this particular r. □

It is not easy to obtain an explicit expression for the functions $f(q,r)$. As an example, let us consider the case where E is the twodimensional Hilbert space. The theorems to be discussed in the following chapters show that the critical exponent of E equals 2 so that $f(2,r) < 1$ for each $r < 1$ and permits us to write down an explicit expression $f(2,r)$:

$$f(2,r) = r(1 - r^2 + (1 - r^2 + r^4)^{\frac{1}{2}})$$

4 The critical exponent of Hilbert space

Let $\mathcal{H}$ be a Hilbert space. The Banach algebra of all bounded linear operators on $\mathcal{H}$ will be denoted by $B(\mathcal{H})$. An operator $T \in B(\mathcal{H})$ is said to be a contraction if $|T| \leq 1$. Clearly T is a contraction if and only if $I - T^*T \geq 0$. If T is a contraction we denote by $D(T)$ the positive square root of $I - T^*T$ and by $\mathcal{D}(T)$ the closure of the range of $D(T)$; The operator $D(T)$ is characterized by the fact that $D(T) \geq 0$ and

$$|D(T)x|^2 = |x|^2 - |Tx|^2$$

for all $x \in \mathcal{H}$.

Another useful characterization of contractivity is the following.

The operator T is a contraction if and only if

$$\begin{pmatrix} I & T \\ T^* & I \end{pmatrix} \geq 0.$$

Indeed, it is easy to see that

$$\left(\begin{pmatrix} I & T \\ T^* & I \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right) = |x + Ty|^2 + |y|^2 - |Ty|^2.$$

If T is a contraction, this shows that the matrix is positive. On the other hand setting $x = -Ty$, we see that positivity of the matrix implies $|y|^2 - |Ty|^2 \geq 0$ for all y.

4.1 *Let T be a contraction on a Hilbert space $\mathcal{H}$. For $k = 0, 1, \ldots$ denote by E_k the kernel of $(I - T^{*k}T^k)$. Then*

(1) $E_0 \supset E_1 \supset E_2 \supset \ldots$

(2) *if $E_{k+1} = E_k$ then $TE_k \subset E_k$*

In particular, $E_{k+1} = E_k$ implies $E_j = E_k$ for all $j \geq k$.

Proof. Since

$$I - T^{*k+1}T^{k+1} = I - T^{*k}T^k + T^{*k}(I - T^*T)T^k \geq I \ - T^{*k}T^k$$

the inclusion $x \in E_{k+1}$ implies $x \in E_k$.

To prove the second part, assume that $E_{k+1} = E_k$ and consider an $x \in E_k$. Since $E_k \subset E_{k+1}$ we have

$$|x| \geq |Tx| \geq |T^k(Tx)| = |T^{k+1}x| = |x|$$

so that $|T^k(Tx)| = |Tx|$ and $Tx \in E_k$.

In particular, the second assertion makes it possible to show that the inclusion $E_k \subset E_{k+1}$ implies $E_{k+1} \subset E_{k+2}$. Indeed, suppose $E_k \subset E_{k+1}$ and consider an $x \in E_{k+1}$. Thus $x \in E_k$ by (1) and $y = Tx \in E_k$ by (2). It follows that $y \in E_{k+1}$ so that $|T^{k+1}y| = |y|$. Hence

$$|T^{k+2}x| = |T^{k+1}y| = |y| = |Tx|.$$

Since $E_{k+1} \subset E_1$ we have $|Tx| = |x|$; this proves the inclusion $x \in E_{k+2}$. □

4.2 Lemma. *Suppose $T \in B(E)$ is a contraction, let E_* be a closed subspace of E such that E_* is invariant with respect to T and $T|E_*$ is an isometry. If $TE_* = E_*$ then E_* is reducing for T.*

Proof. For $x \in E_*$ we have $|Tx|^2 = |x|^2$ whence $(T^*Tx, x) = (x, x)$. Since $I - T^*T \geq 0$ it follows that $x \in \ker\,(I - T^*T)$. Thus $E_* \subset \ker\,(I - T^*T)$. Suppose $x \in E_*$. Then $x = Ty$ for a suitable $y \in E_*$ and $T^*x = T^*Ty = y$. Thus $T^*E_* \subset E_*$. □

4.3 Theorem. *Let E be a Hilbert space of dimension n. If T is a contraction on E then the following assertions are equivalent*

(1) $r(T) = 1$

(2) $|T^n| = 1$

(3) *the space E contains a nonzero subspace E_* such that E_* is reducing for T and $T|E_*$ is unitary.*

Proof. Since $r(T) \leq |T^n|^{1/n}$the implication from (1) to (2) is immediate. Thus it remains to prove that $|T^n| = 1$ implies (3). So assume $|T^n| = 1$. Consider the sequence $E_0 \supset E_1 \supset \ldots \supset E_n$. Since E_n has dimension at least one by our assumption there exists a k such that

$$0 \leq k \ < n \quad \text{and} \quad E_k = E_{k+1}.$$

By our lemma E_k is invariant with respect to T, $T|E_k$ is isometric on E_k by definition and $E_k \supset E_n \neq 0$. Since E_k is finite-dimensional and $T|E_k$ isometric, we have $TE_k = E_k$. It follows from the preceding lemma that E_k is reducing for T. □

Recall that a contraction $T \in B(\mathcal{H})$ is called *completely nonunitary* if there exists no nontrivial subspace $\mathcal{H}_0 \subset \mathcal{H}$ reducing for T and such that $T|\mathcal{H}_0$ is unitary.

The theorem may be restated in the following equivalent form

4.4 Theorem. *Let T be a contraction on an n-dimensional Hilbert space E. Then the following assertions are equivalent*

(1) $r(T) < 1$

(2) $|T^n| < 1$

(3) *T is completely nonunitary.*

Expressed in this manner the theorem assumes a form which immediately suggests that a quantitative refinement of the results would be desirable. The rest of our considerations will be devoted to the problem of finding estimates for $|T^n|$ if the spectral radius of T is bounded by a number $r < 1$.

The pigeonhole principle together with the preceding considerations may by used [21] to prove the following analogy of the equivalence of (1) and (2) in the theorem.

4.5 Theorem. *Let $A_1 \ldots A_n$ be pairwise commuting contractions on an n-dimensional Hilbert space. If $r(A_j) < 1$ for all j then*

$$|A_1 \ldots A_n| < 1.$$

Proof. Set $E_0 = E$ and, for $k = 1, 2, \ldots, n$ let

$$E_k = \{x \in E; |A_1 \ldots A_k x| = |x|\}.$$

The A_j being contractions, the E_k are subspaces of E.

1. We prove first the inclusion $E_{k+1} \subset E_k$. Indeed, given $x \in E_{k+1}$, we have

$$|x| = |A_1 \ldots A_k A_{k+1} x| = |A_{k+1} A_1 \ldots A_k x| \leq |A_1 \ldots A_k x| \leq |x|$$

It follows that $|A_1 \ldots A_k x| = |x|$ whence $x \in E_k$.

2. We prove the inclusion $A_{k+1} E_{k+1} \subset E_k$. Indeed, given $x \in E_{k+1}$, we have

$$|x| = |A_1 \ldots A_k A_{k+1} x| \leq |A_{k+1} x| \leq |x|.$$

Consider the sequence

$$E_0 \supset E_1 \supset \ldots \supset E_n.$$

To prove the theorem, we have to show that $E_n = 0$. Suppose, on the contrary, that $E_n \neq 0$. It follows that there exists a $k < n$ such that $E_k = E_{k+1}$. Then $A_{k+1} E_{k+1} \subset E_k = E_{k+1}$ and $A_{k+1} | E_{k+1}$ is an isometry. It follows that $r(A_{k+1}) \geq r(A_{k+1} | E_{k+1})$, a contradiction. $\square$

5 The two maximum problems

The critical exponent of n-dimensional Hilbert space being n, the corresponding quantitative problem is thus the following:

5.1 *for each positive $r < 1$, compute the maximum of $|T^n|$ as T ranges over all operators on n-dimensional Hilbert space such that $|T| \leq 1$ and $r(T) \leq r$.*

It is, in particular, the second constraint that is awkward to handle. Seeking ways to overcome this difficulty, the author observed that the problem becomes more tractable if the second constraint is replaced by a more stringent one; this idea turns out to be the decisive step in the solution. The method adopted in [12] consists in dividing the maximum problem into two stages.

5.1 The first maximum problem

The second constraint $r(T) < r$ is replaced by the equirement that the operator T be annihilated by a polynomial of degree n with all zeros at most r in modulus, in other words, that the spectrum of T be contained in a given subset of $\{|z| \leq r\}$ consisting of no more than n points.

Consider a polynomial p of degree n whose zeros lie in the interior of the unit disk, and consider the class $\mathcal{A}(p)$ of all contractions T on the n-dimensional Hilbert space such that $p(T) = 0$. The spectra of these operators are contained in the spectrum of the polynomial p.

It is possible to construct, for each p, a contraction $S(p)$ annihilated by p and such that the maximum of $|T^n|$ for $T \in \mathcal{A}(p)$ is attained for $T = S(p)$. We shall describe $S(p)$ later. It turns out that $S(p)$ realizes, in fact, the maximum for a more general extremum problem:

5.2 *Consider the set $\mathcal{A}(p)$ of all contractions T on the n-dimensional Hilbert space such that $p(T) = 0$. Given an arbitrary polynomial f, the maximum of $|f(T)|$ as T ranges over $\mathcal{A}(p)$ is assumed at $S(p)$.*

For the moment, let us assume that the first maximum problem is solved.

5.2 The second maximum problem

(Or the problem of the worst polynomial).

Consider a fixed positive $r < 1$ and denote by $\mathcal{Z}_r$ the set of all contractions $T \in B(H^n)$ with $r(T) \leq r$. It follows from the Cayley–Hamilton theorem that every operator with spectral radius at most r is annihilated by a polynomial of degree n with zeros at most r in modulus. Thus

$$\mathcal{Z}_r = \cup \mathcal{A}(p)$$

where p ranges over the class $P(r)$ of all polynomials of degree n whose zeros lie in the disk

$$D(r) = \{z; |z| \leq r\}.$$

Together with the solution of the first maximum problem the identity $\mathcal{Z}_r = \cup\mathcal{A}(p)$ yields the following fact.

Given a polynomial f,

$$\sup\{|f(T)|; T \in \mathcal{Z}_r\} = \sup\{|f(S(p))|; p \in P(r)\}$$

so that our task reduces to finding the polynomial (or polynomials) in $P(r)$ for which the function $p \to |f(S(p))|$ assumes its maximum. In this generality, for arbitrary f, the problem is still open. For the case $f(z) = z^n$ the solution was given in the author's paper [12].

Fairly delicate algebraic considerations enabled the author to show that the maximum of this function is attained for the polynomial $p_{\max}$ defined by

$$p_{\max}(z) = (z - r)^n.$$

This polynomial is the worst polynomial that we are looking for. It maximizes the function

$$p \to |S(p)^n|$$

for $p \in P(r)$. The method of proof does not extend to the case of an arbitrary f as it did in the first maximum problem. The problem of finding the worst polynomial for a general f remains open. In some particular cases it can be shown that $(z-r)^n$ will do. Also there is numerical evidence that $(z-r)^n$ is the worst polynomial for some polynomials f different from z^n.

6 Matrices and operators

The following two chapters are of a technical character. We shall have to represent operators by means of matrices with respect to different bases. We develop a technique of dealing with such matters which considerably simplifies the calculations. We venture to say that — using this approach — the work is much less tedious than the standard treatment.

In the whole chapter n will be a fixed number, H_n will be an abstract n-dimensional Hilbert space, $B(H_n)$ the algebra of all linear operators on H_n. We shall also occasionally consider the concrete n-dimensional Hilbert space C^n whose elements are column vectors indexed by $0, 1, \ldots, n-1$. Thus $x \in C^n$ means

$$x = (x_0, x_1, \ldots, x_{n-1})^T.$$

We shall denote by $e_0, e_1, \ldots, e_{n-1}$ the standard unit vectors

$$e_0 = (1, 0, 0, \ldots, 0)^T.$$

$$e_1 = (0, 1, 0, \ldots, 0)^T.$$

$$\ldots$$

An operator A on C^n will be identified with its matrix

$$a_{ik} = (Ae_k, e_i).$$

An n-tuple of vectors $b_0, \ldots, b_{n-1}$ in H_n will be interpreted in two ways. We shall view it either as a row vector $B = (b_0, \ldots, b_{n-1})$ or as a linear operator B from C^n into H_n defined by the relations

$$Be_k = b_k \qquad k = 0, 1, \ldots n-1.$$

Taken as an operator, B assigns to an $x \in C^n$ the matrix product Bx of the row B and the column x.

In the particular case where $H_n = C^n$, in other words, if the b_j are column vectors, the row vector $(b_0, \ldots, b_{n-1})$ will become a matrix which happens to be the matrix of the operator B just defined.

Similarly, if $T \in B(H_n)$ we shall interpret the product TB either as the row vector $(Tb_0, \ldots, Tb_{n-1})$ or as the operator obtained as the superposition of B and T.

If $A \in B(C^n)$ we define BA as the row obtained by the matrix product.

$$BA = (\sum b_j a_{j,0}, \ldots, \sum b_j a_{j,n-1})$$

or as an operator. Interpreted as an operator BA is the operator from C^n into H_n obtained as the superposition of A and B.

If B is a basis (in other words if the b_j are linearly independent) and T is a linear operator on the linear span $\mathcal{H}_0$ of B, then there exists a unique matrix $\mathcal{M}(T, B)$ such that

$$TB = B\mathcal{M}(T, B).$$

Thus premultiplication by T equals postmultiplication by the matrix $\mathcal{M}(T, B)$. This is why $\mathcal{M}(T, B)$ will be called the matrix of the operator T in the basis B.

It is easy to see that the equation

$$TB = B\mathcal{M}(T, B)$$

is valid in both interpretations of B, either as the equality of two row vectors or of two operators from C^n into H_n. In the particular case where $H_n = C^n$ the operator T as well as B become matrices for which $TB = B\mathcal{M}(T, B)$.

Summing up: if B is a basis, T an operator and $M = \mathcal{M}(T, B)$, then

$$TB = BM;$$

this equality characterizes the matrix of T with respect to the basis B. Indeed, if $M' \in \mathcal{L}(C^n)$ satisfies $TB = BM'$ then $M' = \mathcal{M}(T, B)$.

To illustrate the advantages of the formal multiplication introduced above we intend to describe the relation between the matrices of an operator in two different bases.

If B is a basis and if B' is the basis obtained as $B' = BW$, W being an invertible matrix, then, for each operator T

$$\mathcal{M}(T, B') = W^{-1}\mathcal{M}(T, B)W.$$

It does not require more effort to prove a more general fact.

In a similar manner we define the matrix of T with respect to the pair of the bases: B_1 in the domain space, B_2 in the image space.

The matrix of T with respect to B_1 and B_2, denoted by $\mathcal{M}(T; B_1, B_2)$, is defined by the relation

$$TB_1 = B_2\mathcal{M}(T; B_1, B_2).$$

If the bases B_1 in E_1 and B_2 in E_2 are interpreted as linear operators from C^n into E_1 and E_2 respectively, the relation defining the matrix $\mathcal{M}(T; B_1, B_2)$ is equivalent to the commutativity of the following diagram

$$\begin{tikzcd}
E_1 \arrow[r, "T"] & E_2 \\
C^n \arrow[u, "B_1"] \arrow[r, "\mathcal{M}"'] & C^n \arrow[u, "B_1"']
\end{tikzcd}$$

The technique of formal multiplication introduced above yields considerable simplifications: the proof of the following lemma demonstrates its advantages.

6.1 Lemma. *If the bases B_1 and B_2 are replaced by $B_1' = B_1W_1$ and $B_2' = B_2W_2$ then*

$$\mathcal{M}(T; B_1', B_2') = W_2^{-1}\mathcal{M}(T; B_1, B_2)W_1$$

Proof.

$$\begin{aligned} TB_1' &= TB_1W_1 = B_2\mathcal{M}(T; B_1, B_2)W_1 = \\ &= B_2'W_2^{-1}\mathcal{M}(T; B_1, B_2)W_1. \end{aligned}$$

Let A be a linear operator on H_n with a cyclic vector z; in the other words the vectors

$$z, Az, \ldots, A^{n-1}z$$

form a basis of H_n and the minimal polynomial of A coincides with its characteristic polynomial p. Write p in the form

$$p(z) = -(a_0 + a_1z + \ldots + a_{n-1}z^{n-1}) + z^n$$

and consider the matrix

$$C(p) = \begin{pmatrix} 0 & 0 & & 0 & a_0 \\ 1 & 0 & & 0 & a_1 \\ 0 & 1 & & 0 & a_2 \\ \dots & & & & \\ 0 & 0 & & 1 & a_{n-1} \end{pmatrix}.$$

If B stands for $(z, Az, \dots, A^{n-1}z)$ then $AB = BC(p)$, in the other words, the matrix of A in the basis B is just $C(p)$. Recall the dual interpretation of the relation $AB = BC(p)$.

It represents either the equality of two row vectors if B is considered as a row of vectors or as an identity for operators if B is taken to mean a linear operator from C^n into H_n.

The matrix $C(p)$ will be called the *companion matrix of* p.

7 The geometry of H_n, generalized Gram matrices

In order to deal with the geometric properties of nonorthogonal bases it will be necessary to develop a technique using a generalization of the classical notion of a Gram matrix.

If a and b are two elements of some Hilbert space $\mathcal{H}$ we denote by b^*a the scalar product (a, b) and by ab^* the operator

$$x \to (x, b)a.$$

The mapping which assigns to each $a \in \mathcal{H}$ the operator of premultiplication by a^* is thus a conjugate linear bijection of $\mathcal{H}$ onto its dual. In the particular case $\mathcal{H} = C^n$ this $*$ operator assumes its standard meaning, b^* becomes a row vector and our definition coincides with the multiplication of a row vector and a column vector. This notation has the advantage that the operator ab^* coincides with the matrix ab^* in the case of the space C^n. Also, it behaves nicely with respect to multiplication; indeed

$$A(ab^*)B^* = Aa(Bb)^*$$

for any $A, B \in B(H)$.

If we denote ab^* by T we have the following formulae

$$T^* = ba^*$$

$$T^*T = |a|^2 bb^*$$

$$TT^* = |b|^2 aa^*$$

so that the norm of T equals $|a|\ |b|$.

Observe that these formulae may be obtained directly by formal multiplication. Thus, e.g.

$$T^*T = ba^*ab^* = |a|^2 bb^*.$$

Since $Ta = ab^*a = (b^*a)a$ the vector a is either zero or an eigenvector of T with eigenvalue $b^*a = (a,b)$. The spectrum of T consists thus of at most two numbers; first (a,b) and then zero with multiplicity $n-1$ since the $(n-1)$ dimensional subspace $b^\perp$ is annihilated by T.

We shall denote by $R_n(\mathcal{H})$ the set of all rows of the form $(b_0, \ldots, b_{n-1})$ where $b_j \in \mathcal{H}$.

If U, V are two rows of length n,

$$U, V \ \in R_n(\mathcal{H})$$

we intend to define the Gram matrix $G(U,V)$. First of all, for $B \in R_n(\mathcal{H})$, $B = (b_0, \ldots, b_{n-1})$ we take B^* to be the column vector of functionals

$$B^* = \begin{pmatrix} b_0^* \\ \vdots \\ b_{n-1}^* \end{pmatrix}.$$

If B is interpreted as a linear operator from C^n into $\mathcal{H}$ then B^* has also a meaning as a linear operator from $\mathcal{H}$ into C^n; its action can also be described as the formal multiplication of the n by 1 matrix $(b_0^*, \ldots, b_{n-1}^*)^T$ on 1 by 1 matrices – elements of $\mathcal{H}$.

Given $x, y \in C^n$, consider the two vectors $u = Ux$, $v = Vy$ so that $u, v \in \mathcal{H}$. For the scalar product (u,v) we obtain

$$\begin{gathered} (u,v) = v^*u = y^*V^*U\ x = \\ \sum_{j,k} y_j^* v_j^* u_k x_k = \sum_{j,k} y_j^* G_{jk} x_k \end{gathered}$$

where we have denoted by G_{jk} the scalar products

$$G_{jk} = v_j^* u_k = (u_k, v_j).$$

The matrix $G(U,V) = V^*U$ will be called the Gram matrix of the rows U and V. Its elements are

$$G(U,V)_{jk} = (u_k, v_j)$$
$$G(U,V) = V^*U.$$

Thus $G(U,V)$ is an n by n matrix or an operator in C^n.

The scalar product of u and v may thus be written in the form

$$(u,v) = y^*Gx = (Gx, y).$$

Again, if R and S are interpreted as linear operators from C^n into $\mathcal{H}$ then S^*R is a linear operator in C^n and its matrix is just $G(R,S)$. Thus, in the particular case of vectors in C^n the row vector R may be identified with the n by n matrix $(f_0, \ldots, f_{n-1})$ and it is not difficult to verify that the above formula remains true even in this interpretation of S^*R.

If the rows U and V are transformed by matrices A and B

$$U' = UA \qquad V' = VB$$

then $G(U', V') = V'^* U' = B^* V^* U A$ so that

$$G(U', V') = B^* G(U, V) A.$$

If the rows U and V are transformed by operators, we obtain another formula for $G(U', V')$. Let T, W be two operators in $\mathcal{H}$; then

$$G(TU, WV) = \mathcal{M}(W, V)^* G(U, V) \mathcal{M}(T, U).$$

Indeed, since

$$TU = U \ \mathcal{M}(T, U)$$

$$WV = V \ \mathcal{M}(W, V),$$

$$\begin{aligned} G(TU, WV) &= (WV)^*(TU) = (V(M(W, V))^*(UM(T, U)) = \\ &= M(W, V)V^* U M(T, U). \end{aligned}$$

If an operator T is represented by a matrix with respect to a not necessarily orthonormal basis then, to obtain the matrix of T^* in the same basis, the adjoint of the matrix of T has to be modified using the Gram matrix of the basis.

7.1 *Let $T \in B(\mathcal{H})$, let X be a basis for $\mathcal{H}$, $X = (x_0, \ldots, x_{n-1})$. Then*

$$\mathcal{M}(T^*, X) = G^{-1} \mathcal{M}(T, X)^* G$$

where $G = X^* X$ is the Gram matrix of the basis X.

Proof. The proof is based on the equality

$$X^*(T^* X) = (TX)^* X.$$

It follows that

$$\begin{aligned} X^* \cdot X \mathcal{M}(T^*, X) &= X^* \cdot (T^* X) = (TX)^* X = (X \mathcal{M}(T, X))^* X = \\ &= \mathcal{M}(T, X)^* X^* \cdot X \end{aligned}$$

so that

$$G \mathcal{M}(T^*, X) = \mathcal{M}(T, X)^* G. \qquad \square$$

7.2 *If S intertwines T_1 and T_2*

$$ST_1 = T_2 S$$

then T_2 has the same matrix in the basis SX as T_1 has in the basis X

$$\mathcal{M}(T_1, X) = \mathcal{M}(T_2, SX).$$

Proof. We have

$$T_2(SX) = ST_1X = S(X\mathcal{M}(T_1, X)) = (SX)\mathcal{M}(T_1, X). \qquad \square$$

Two operators T_1, T_2 are said to be unitarily equivalent if there exists a unitary operator U such that $UT_1 = T_2 U$.

7.3 Proposition. *The operators $T_1, T_2 \in B(\mathcal{H})$ are unitarily equivalent if and only if there exist two bases B_1, B_2 such that*

$$\mathcal{M}(T_1, B_1) = \mathcal{M}(T_2, B_2)$$
$$G(B_1) = G(B_2).$$

Proof. If $UT_1 = T_2 U$ for some unitary U, choose a basis B and set $B' = UB$. Then

$$\mathcal{M}(T_1, B) = \mathcal{M}(T_2, B')$$

by the observation above. Furthermore

$$G(B') = (UB)^* UB = B^* B = G(B).$$

On the other hand, suppose we have two bases B_1, B_2 with the same Gram matrix such that $\mathcal{M}(T_1, B_1) = \mathcal{M}(T_2, B_2)$. Denoting this matrix by $\mathcal{M}$ we have the equations

$$T_1 B_1 = B_1 \mathcal{M}$$
$$T_2 B_2 = B_2 \mathcal{M}$$

The equality $G(B_1) = G(B_2)$ implies $|B_1 x| = |B_2 x|$ for every $x \in \mathcal{H}$ so that there exists a unitary operator U for which $B_2 = UB_1$. Now

$$T_2 U B_1 = T_2 B_2 = B_2 \mathcal{M} = UB_1 \mathcal{M} = UT_1 B_1$$

whence $T_2 U = UT_1$. $\square$

Given a basis B, the norm of a vector x is expressed in the form $|x|^2 = (Gu, u)$ where u is the vector of coordinates of x in the basis B. The corresponding expression for $|Tx|^2$ reads as follows

7.4 *Let T be a linear operator on H_n and let B be a basis of the space. Then, for an arbitrary vector $x \in H_n$*

$$|Tx|^2 = (M^* G M u, u)$$

where u is the vector of the coordinates of x in the basis B, $M = \mathcal{M}(T, B)$ and G is the Gram matrix of B.

Proof. The vector u is determined by the equality $x = Bu$. Thus

$$\begin{aligned} |Tx|^2 &= |TBu|^2 = |BMu|^2 = (BMu, BMu) = \\ &= (M^* B^* B M u, u) = (M^* G M u, u) \end{aligned}$$

□

Let us describe a simple method of constructing the inverse of a Gram matrix. Suppose we have n-tuples

$$R = (f_0, \ldots, f_{n-1}) \qquad S = (g_0, \ldots, g_{n-1})$$

such that $G(R, S)$ is invertible. (The invertibility of $S^* R$ implies the invertibility of both S and R so that the vectors f as well as the vectors g will be linearly independent.) Suppose we find two operators A and B such that $(Af_i, Bg_k) = \delta_{ik}$; let us show that

$$G^{-1} = \mathcal{M}(A, R)\mathcal{M}(B, S)^*.$$

Indeed, it follows from the above formula that

$$1 = \mathcal{M}(B, S)^* G \mathcal{M}(A, R)$$

whence

$$\begin{aligned} &\mathcal{M}(B, S)^*(G\mathcal{M}(A, R)\mathcal{M}(B, S)^* - 1) = \\ = \; &(\mathcal{M}(B, S)^* G \mathcal{M}(A, R))\mathcal{M}(B, S)^* - \mathcal{M}(B, S)^* = 0. \end{aligned}$$

The following lemma shows how the square root of $G(A)$ may be used to orthonormalize the basis A.

7.5 *Suppose the vectors $a_1, \ldots, a_n$ are linearly independent. Suppose W is a matrix such that*

$$W^* W = G(a_1, \ldots, a_n)^{-1}$$

Then the system $(a_1, \ldots, a_n)W^*$ is orthonormal.

Proof. Since $G(a_1, \ldots, a_n) = A^* A$, we have

$$W^* W = (A^* A)^{-1} = A^{-1}(A^*)^{-1}$$

whence $AW^* \cdot WA^* = 1$ so that $WA^*AW^* = 1$. It follows that

$$G(AW^*) = WA^* \cdot AW^* = 1 \qquad \square$$

As an illustration of the techniques using Gram matrices let us mention the Nevanlinna – Pick problem.

We shall work in the Hardy space H^2 on the open unit disk $D = \{z, |z| < 1\}$. For each $w \in D$ we denote by $e(w)$ the corresponding evaluation functional

$$e(w)(z) = \frac{1}{1 - w^* z};$$

in this manner $(f, e(w)) = f(w)$ for every $f \in H^2$.

7.6 *Given n distinct points $z_1, \ldots, z_n \in D$ and n complex numbers $w_1, \ldots, w_n$, the following conditions are equivalent:*

1^0 *there exists a function h holomorphic in D such that $|h(z)| \leq 1$ for $z \in D$ and $h(z_j) = w_j$.*

2^0 *the matrix*

$$\frac{1 - w_i^* w_j}{1 - z_i^* z_j}$$

is nonnegative definite.

Assume 1^0 and consider the multiplication operator $M(h)$ on H^2. Since $h(z_j) = w_j$ it follows that $(f, M(h)^* e(z_j)) = (M(h)f, e(z_j)) = w_j f(z_j) = (f, w_j^* e(z_j))$ for every $f \in H^2$ whence

$$M(h)^* e(z_j) = w_j^* e(z_j).$$

Consequently, the matrix of $M(h)^*$ taken in the basis $e(z_1), \ldots, e(z_n)$ is the diagonal matrix W^* with $w_1^*, \ldots, w_n^*$ on the diagonal. Since $|h(z)| \leq 1$ for $z \in D$, the norm of $M(h)$ and, consequently of $M(h)^*$, cannot exceed 1.

Thus the existence of an h with the required properties implies
the operator transforming $e(z_j)$ into $w_j^* e(z_j)$ is a contraction.

In terms of Gram matrices

$$G(w_1^* e(z_1), \ldots, w_n^* e(z_n)) \leq G(e(z_1), \ldots, e(z_n))$$

or

$$W^* G W \leq G.$$

The nontrivial implication, the sufficiency of 2^0, will be proved in the lecture devoted to the work of D. Sarason.

8 The geometry of $B(H_n)$

The original solution of the maximum problem [12] was based on a simple result which permits to study the operator norm in $B(H_n)$ using the geometry of $B(H_n)$ in the Frobenius norm, in other words, treating $B(H_n)$ as a Hilbert space. This approach leads in a natural manner to infinite-dimensional considerations and to what is known today as dilation theory.

If $\mathcal{H}$ is a finite-dimensional Hilbert space then $B(\mathcal{H})$ is a Hilbert space under the scalar product

$$(A, B) = tr\ B^*A = tr\ AB^*.$$

Let us list here, for further reference, some of the properties of this scalar product; the following relations hold

$$(XA, B) = (A, X^*B)$$
$$(AX, B) = (A, BX^*).$$

It follows that the adjoint of the operator $\mathcal{M} \in B(B(H_n))$

$$\mathcal{M} : X \to RXS$$

is the operator $\mathcal{M}^*$

$$\mathcal{M}^*(X) = R^*XS^*.$$

Consider now the tensors ab^*. Since clearly $tr\ ab^* = b^*a = (a, b)$ we have the following formulae

$$(ab^*, M) = (a, Mb)$$
$$(M, ab^*) = (Mb, a).$$

Indeed,

$$(ab^*, M) = tr\ ab^*M^* = tr\ a(Mb)^* = (Mb)^*a = (a, Mb).$$

In the particular case that $M = R^*R$ we have the useful formula

$$(xy^*, R^*R) = (Rx, Ry).$$

The scalar product (x, y) may be represented as

$$(x, y) = (xy^*, 1) = (1, yx^*).$$

The following lemma gives an expression for the operator norm in terms of the scalar product in $B(\mathcal{H})$. Using this lemma we intend to show, in the next section, how the relation established in this manner between the two matrices on $B(H_n)$ leads in a natural manner to the consideration of dilations.

8.1 *If R is a linear operator on H_n then*

$$|R|^2 = \sup\{(B, R^*R); B \geq 0, (B,1) = 1\}.$$

The supremum is attained on the subset of all one-dimensional operators:

$$|R|^2 = \sup\{(vv^*, R^*R); (vv^*, 1) = 1\}.$$

Proof. Every $B \geq 0$ may be written as the sum of n operators of the form $b_j b_j^*$. The condition $(B,1) = 1$ reduces then to $\sum |b_j|^2 = 1$. Our maximum problem is thus transformed into

$$\sup\{\sum_1^n |Rb_j|^2; \sum_1^n |b_j|^2 = 1\}.$$

Since $\sum |Rb_j|^2 \leq |R|^2 \sum |b_j|^2 \leq |R|^2$ this supremum cannot exceed $|R|^2$; on the other hand, the value $|R|^2$ is attainable by operators B of the form bb^* with $|b| = 1$. $\square$

9 The first maximum problem

In the present section we intend to solve the first maximum problem. To restate the problem, it will be convenient to introduce some notation. We are given a fixed polynomial p of degree n with all zeros in the open unit disk and denote by $\mathcal{A}(p)$ the set of all contractions $A \in B(H_n)$ such that $p(A) = 0$. The set $\mathcal{A}(p)$ is thus given by the two constraints:

$$|A| \leq 1 \qquad \text{and} \qquad p(A) = 0.$$

For any polynomial f the problem is to maximize $|f(A)|$ as A ranges over the set $\mathcal{A}(p)$. It turns out that there is an element $A_p \in \mathcal{A}(p)$, independent of f, which maximizes $|f(A)|$ over the set given by the two constraints above.
In this section we shall give a description of this extremal operator.

Let $\mathcal{H}$ be the n-dimensional Hilbert space. Let p be a polynomial of degree n with all zeros in the open unit disk D.

We denote by $\mathcal{A}(p)$ the set of all contractions $A \in B(\mathcal{H})$ such that $p(A) = 0$.

We shall also associate with p a set of matrices $\mathcal{Z}(p)$ defined as follows. We denote by $\mathcal{C}$ the congruence operator on M_n

$$X \to C(p)^* X C(p)$$

and by E_0 the matrix $e_0 e_0^*$. Then

$$\mathcal{Z}(p) = \{Z \in M_n; (1 - \mathcal{C})Z \ \geq 0, (Z, E_0) = 1\}.$$

We shall establish a relation between $\mathcal{A}(p)$ and $\mathcal{Z}(p)$ which makes it possible to linearize the maximum problem. Given a vector $z \in \mathcal{H}$ of norm 1, consider the mapping $g : B(\mathcal{H}) \to M_n$ defined by

$$g(Y) = G(z, Yz, \dots, Y^{n-1}z).$$

Our further investigations are based on the following result:

$$g(\mathcal{A}(p)) = \mathcal{Z}(p).$$

Consider an $A \in \mathcal{A}(p)$. Denote by B the row vector consisting of the vectors $(z, Az, \dots, A^{n-1}z)$ and consider the matrix $G(B)$. Since $|z| = 1$ we have $(G(B), E_0) = |z|^2 = 1$. The equality $p(A) = 0$ implies $AB = BC(p)$. Thus

$$\begin{aligned}(G(B)x, x) &- (C^*G(B)Cx, x) = \\ &= |Bx|^2 - |BCx|^2 = |Bx|^2 - |ABx|^2 \geq 0\end{aligned}$$

the operator A being a contraction. It follows that

$$(1 - \mathcal{C})G(B) \geq 0$$

so that $G(B) \in \mathcal{Z}$.

On the other hand, let $Z \in M_n$ and $Z - C^*ZC \geq 0$. Since all zeros of p are less than one in modulus we have $C(p)^m \to 0$. Since

$$Z - C^{*m}ZC^m = \sum_0^{m-1} C^{*k}(Z - C^*ZC)C^k \geq 0$$

this implies that $Z \geq 0$. It follows that there exist vectors $z_0, \dots, z_{n-1}$ such that $Z = G(z_0, \dots, z_{n-1})$ and $z_0 = z$. Denote by B the row

$$B = (z_0, \dots, z_{n-1})$$

and set $W = BC$. Then

$$G(B) - G(W) = G(B) - C^*G(B)C \geq 0.$$

It follows that, for every $x \in C^n$,

$$|Wx|^2 = (G(W)x, x) \leq (G(B)x, x) = |Bx|^2.$$

Now consider the linear span $\mathcal{H}_0$ of the vectors $z_0, \dots, z_{n-1}$. The inequality $|Wx| \leq |Bx|$ just proved shows that it is possible to define, on $\mathcal{H}_0$, a linear contraction A_0 by setting $A_0 z_j = w_j$ for $j = 0, 1, \dots, n-1$. It follows that $A_0 B = W = BC$ whence $p(A_0)B = Bp(C) = 0$ so that $p(A_0) = 0$. Let α be an arbitrary zero of the polynomial p and set

$$A = A_0 P(\mathcal{H}_0) + \alpha(1 - P(\mathcal{H}_0)).$$

Since $A^k x = A_0^k P(\mathcal{H}_0)x + \alpha^k(1 - P(\mathcal{H}_0))x$ for $k \geq 1$ is follows that $p(A) = 0$. It is not difficult to see that A is a contraction. Furthermore, $A^j z_0 = z_j$ for $0 \leq j \leq n-1$ and this implies $g(A) = G(z_0, \dots, z_{n-1}) = Z$.

This lemma makes it possible to transform the maximum problem

$$\max\{|f(A)|^2; \quad |A| \leq 1, \quad p(A) = 0\}$$

formulated in the geometry of $B(\mathcal{H})$ with the operator norm into a problem in the geometry of $B(\mathcal{H})$ as Hilbert space.

Let $A \in B(H_n), z \in H_n$. Denote by B the row

$$B = (z, Az, \ldots, A^{n-1}z).$$

If A is annihilated by p then

$$AB = BC.$$

Let f be an arbitrary polynomial, set $F = f(C)$. We start by expressing the operator norm in terms of the geometry of $B(\mathcal{H})$ as Hilbert space. We show first that

$$|f(A)z|^2 = (F^*G(B)F, E_0).$$

Indeed,

$$\begin{aligned} &|f(A)z|^2 = G(f(A)B)_{00} = (G(f(A)B), E_0) = \\ &= (G(Bf(C)), E_0) = (F^*G(B)F, E_0). \end{aligned}$$

We intend to compute

$$\begin{aligned} & \max\{|f(A)|^2; |A| \leq 1, p(A) = 0\} = \\ = \; & \max\{|f(A)z|^2; |A| \leq 1, p(A) = 0, |z| = 1\} = \\ = \; & \max\{(F^*G(B)F, E_0); G(B) = G(z, Az, \ldots) \\ & |A| \leq 1, p(A) = 0, |z| = 1\}. \end{aligned}$$

The value we are looking for equals

$$\max(F^*G(B)F, E_0)$$

where $G(B)$ ranges over all matrices of the form

$$G(z, Az, \ldots, A^{n-1}z)$$

with $|A| \leq 1$, $p(A) = 0$ and $|z| = 1$. This is exactly the set which we have denoted by $g(\mathcal{A}(p))$ in the preceding lemma. Using the result of the lemma, we obtain

$$\begin{aligned} & \max\{|f(A)|^2; |A| \leq 1, p(A) = 0\} = \\ = \; & \max\{(F^*ZF, E_0); (1 - \mathcal{C})Z \geq 0, (Z, E_0) = 1\}. \end{aligned}$$

Denote by $\mathcal{F}$ the congruence

$$\mathcal{F} : X \to F^*XF$$

and observe that $\mathcal{F}$ commutes with $\mathcal{C}$. Writing M for $(1-\mathcal{C})Z$, the last maximum may be rewritten in the form

$$\begin{aligned}
& \max\{(\mathcal{F}(1-\mathcal{C})^{-1}M, E_0);\ M \geq 0,\ ((1-\mathcal{C})^{-1}M, E_0) = 1\} = \\
= \ & \max\{(M, (1-\mathcal{C}^*)^{-1}\mathcal{F}^*E_0);\ M \geq 0,\ (M, (1-\mathcal{C}^*)^{-1}E_0) = 1\} = \\
= \ & \max\{(M, \mathcal{F}^*(1-\mathcal{C}^*)^{-1}E_0);\ M \geq 0,\ (M, (1-\mathcal{C}^*)^{-1}E_0) = 1\}.
\end{aligned}$$

Transformed into this form, the maximum problem immediately suggests, in a natural manner, an interpretation as a problem for operators acting on infinite-dimensional spaces of sequences. This led the author to the consideration of what is known today as dilation theory.

Since we intend to explain the connections with dilation theory in more detail later, we postpone the discussion to the next lecture, and present at this moment another somewhat less elegant proof which has the advantage of giving the solution directly in the form of a concrete matrix.

Write K for $(1-\mathcal{C}^*)^{-1}E_0$ and observe that K is positive definite. Indeed,

$$\begin{aligned}
& K \ \geq (1 + \mathcal{C}^* + \ldots + \mathcal{C}^{*n-1})E_0 = \\
= \ & E_0 + CE_0C^* + \ldots + C^{n-1}E_0C^{*n-1} = 1.
\end{aligned}$$

Denote by $\mathcal{K}$ the congruence

$$\mathcal{K}X = K^{1/2}XK^{1/2}$$

and observe that $\mathcal{K}^* = \mathcal{K}$ and $K = \mathcal{K}1$. The supremum to be computed is thus

$$\begin{aligned}
& \max\{(M, \mathcal{F}^*K);\quad M \geq 0,\quad (M, K) = 1\} = \\
= \ & \max\{(\mathcal{K}M, \mathcal{K}^{-1}\mathcal{F}^*K);\quad M \geq 0,\quad (\mathcal{K}M, 1) = 1\}.
\end{aligned}$$

Since $\mathcal{K}$ is a linear automorphism of the set $\mathcal{P}$ of all positive semidefinite matrices the maximum to be computed is thus

$$\max\{(B, \mathcal{K}^{-1}\mathcal{F}^*K); B \geq 0, (B, 1) = 1\}.$$

Observe that $\mathcal{K}^{-1}\mathcal{F}^*K = K^{-1/2}FKF^*K^{-1/2} = RR^*$ where $R = K^{-1/2}FK^{1/2} = K^{-1/2}f(C)K^{1/2} = f(K^{-1/2}CK^{1/2})$. Our maximum is thus

$$\max\{(B, RR^*); B \geq 0, (B, 1) = 1\} = |R^*|^2.$$

Since $K = (1-\mathcal{C}^*)^{-1}E_0$, we have

$$K - CKC^* = E_0.$$

Denote by A_p the matrix $K^{-1/2}CK^{1/2}$. We have

$$\begin{aligned}
& 1 - A_pA_p^* = 1 - K^{-1/2}CK\ C^*K^{-1/2} = \\
= \ & K^{-1/2}(K\ - CK\ C^*)K^{-1/2} = K^{-1/2}E_0K^{-1/2} \geq 0
\end{aligned}$$

so that $|A_p| = |A_p^*| \leq 1$.

Furthermore

$$p(A_p) = K^{-1/2} p(C) K^{1/2} = 0.$$

The operator A_p is thus similar to C and, consequently, nonderogatory.

The result may thus be formulated as follows.

9.1 *Let f be any polynomial. Then the maximum*

$$\{|f(A)|^2; \quad |A| \leq 1, \quad p(A) = 0\}$$

is attained at A_p.

Proof. The maximum equals

$$|R^*|^2 = |R|^2 = |f(A_p)|^2. \qquad \square$$

Having satisfied the matrix theorist by writing down the solution in the form of a concrete matrix we now proceed to explain the connection with the theory of complex functions. It seems that the best way of doing this is to follow the original reasoning as presented by the author in [12]; this leads, in a natural manner, to the consideration of sequence spaces and will also help establish connections with dilation theory.

Consider a vector $v \in \mathcal{H}_n$, the operator vv^* and the scalar product

$$((1 - \mathcal{C}^*)^{-1} vv^*, E_0)$$

we intend to prove that this expression equals

$$|\psi(v)|^2$$

where $\psi(v)$ is the infinite column vector $C^\infty(p)^* v$.

Indeed,

$$\begin{aligned} ((1 - \mathcal{C})^{-1} vv^*, E_0) &= \sum (C^{*k} v \; (C^{*k} v)^*, E_0) = \\ &= \sum |(C^{*k} v)_0|^2 \end{aligned}$$

where $(C^{*k} v)_0$ is the 0-th coordinate of the vector $C^{*k} v$ but this is nothing more than the k-th coordinate of $(C^\infty(p))^* v$. $\square$

Now let us return to the point where we expressed the maximum in the form

$$\max\{((1 - \mathcal{C})^{-1} \mathcal{F} M, E_0); M \geq 0, ((1 - \mathcal{C})^{-1} M, E_0) = 1\}.$$

If we allow M to range only over matrices of the form vv^*, we obtain the following proposition.

$$\begin{aligned} & \max\{|f(A)|; |A| \leq 1, p(A) = 0\} = \\ = \; & |f(S)^*| \text{ Ker } p(S)^*| = \\ = \; & |f(S^*)| \text{ Ker } p(S^*)| \end{aligned}$$

Proof. Write F for $f(C(p))$. For each vector $v \in C^n$ let $\psi(v)$ be the infinite column vector

$$\psi(v) = C^\infty(p)^* v.$$

If M is of the form vv^*, we have

$$((1-\mathcal{C})^{-1}\mathcal{F}M, E_0) = ((1-\mathcal{C})^{-1}F^*vv^*F, E_0) = |\psi(F^*v)|^2.$$

For $\psi(F^*v)$ we obtain

$$\begin{aligned} & \psi(F^*v) = C^\infty(p)^* f(C(p))^* v \;\; = \\ = \;\; & (f(C(p))C^\infty(p))^* v = (C^\infty(p) f(S))^* v \;\; = \\ = \;\; & f(S)^* C^\infty(p)^* v \;\; = f(S)^* \psi v. \end{aligned}$$

Thus
$\sup\{((1-\mathcal{C})^{-1}\mathcal{F}vv^*, E_0); ((1-\mathcal{C})^{-1}vv^*, E_0) = 1\} = \sup\{|f(S)^*\psi v|^2; |\psi v|^2 = 1\}$.
The vectors of the form ψv, $v \in C^n$ fill the whole space Ker $p(S)^*$. □

The considerations described above have led us, in a natural manner, to the extremal operator $S^*|$ Ker $p(S^*)$. It turns out that this operator is unitarily equivalent to another operator which plays the central role in a parallel theory developed at the same time by D. Sarason; this operator became known later as the model operator.

Since the connection is not immediately obvious, let us discuss it in detail.

Let us denote by J the mapping which assigns to each $f \in L^2$ the element g defined by

$$g(z) = \bar{z}\; f(\bar{z}).$$

Clearly J is an isometry.
The relation $J^2 = 1$ is immediate; thus J is onto, hence unitary so that

$$J = J^* = J^{-1}.$$

Thus J is a selfadjoint involution which maps H^2 onto H^2_-.

We denote by V the shift operator on L^2

$$Vf = g \;\text{ means }\; g(z) = zf(z).$$

The unitary operators V and J are related by the relation

$$JV^* = VJ.$$

Let φ be an inner function so that $\varphi(V)$ is a unitary operator on L^2. Denote by W the product

$$W = \varphi(V)J = J\varphi(V^*)$$

and let us prove that W maps Ker $\varphi(S^*) = H(\tilde{\varphi})$ onto $H(\varphi)$.

Suppose $u \in H^2$. We then have the following series of equivalent statements

$$u \in \text{ Ker } \varphi(S^*)$$
$$\varphi(V^*)u \in H^2_-$$
$$Wu = J\varphi(V^*)u \in H^2.$$

At the same time $Wu = \varphi(V)Ju \perp \varphi(V)H^2$ since $Ju \perp H^2$. This proves that W Ker $\varphi(S^*) \subset H^2 \ominus \varphi H^2$. Since $H^2 \ominus \varphi H^2 = \text{Ker } \varphi(S)^* = \text{Ker } \tilde{\varphi}(S^*)$ we have $\tilde{W}$ Ker $\tilde{\varphi}(S^*) \subset H^2 \ominus \tilde{\varphi} H^2 = \text{Ker } \varphi(S^*)$ if $\tilde{W}$ stands for $\tilde{\varphi}(V)J$. Since $W\tilde{W} = 1$ we have W Ker $\varphi(S^*) = H^2 \ominus \varphi H^2$.

10 Bounded analytic functions

The main theorem of the last section may be extended to a larger class of operators by replacing polynomials by bounded analytic functions. This was done by Sz. Nagy in [21]. In order to state the result in this generality, it will be necessary to use some facts about the extension of the analytic functional calculus to bounded analytic functions.

Let $\mathcal{H}$ be a Hilbert space. A linear operator $T \in B(\mathcal{H})$ is said to be completely nonunitary if there is no subspace $\mathcal{H}_0 \subset \mathcal{H}$ reducing for T such that $T|\mathcal{H}_0$ is unitary. For completely nonunitary operators T it is possible to extend the algebraic homomorphism

$$p \to p(T)$$

from the algebra of polynomials to the algebra H^∞ of all bounded functions holomorphism in the open unit disk D.

This may be done as follows. Given $u \in H^\infty$, define, for $0 < r < 1$, the function u_r by setting $u_r(z) = u(rz)$. Thus u_r is holomorphic on a neighbourhood of the closed unit disk. If T is a completely nonunitary contraction it is possible to show that $\lim u_r(T)$ exists in the strong operator topology as $r \to 1$. This limit defines $u(T)$.

We shall use the following important fact.

10.1 *Let T be a completely nonunitary contraction and let $u \in H^\infty$, $u \neq 0$ be given. If h is an element of $\mathcal{H}$ which satisfies $u(T)h = 0$ then $T^n h \to 0$.*

This is all we shall need in order to extend the maximum problem of the last section to bounded analytic functions.

For the reader who is familiar with the elements of dilation theory we intend to include, at the end of this chapter some comments on the functional calculus on H^∞ and the result just quoted.

Now consider two functions $\varphi, \psi \in H^\infty$. We intend to show that the result of the preceding section remains valid in this more general situation.

10.2 *The operator $T(\varphi) = S^*|Ker\ \varphi(S^*)$ realizes the maximum of $|\psi(T)|$ as T ranges over the family of all completely nonunitary contractions T satisfying $\varphi(T) = 0$.*

We now proceed to give the precise formulation of the results. It consists of two statements.

(1) the operator $T(\varphi)$ is completely nonunitary and $\varphi(T(\varphi)) = 0$.

(2) given a Hilbert space $\mathcal{H}$ and a completely nonunitary contraction $T \in B(\mathcal{H})$ such that $\varphi(T) = 0$ then

$$|\psi(T)| \leq |\psi(T(\varphi))|.$$

First of all, S^* is a contraction, Ker $\varphi(S^*)$ is a closed subspace invariant with respect to S^* and $\varphi(S^*|\text{Ker } \varphi(S^*)) = 0$. Since $S^{*n} \to 0$ both S^* and $T(\varphi)$ are completely nonunitary. This proves (1).

To prove the nontrivial part, consider a Hilbert space $\mathcal{H}$ and denote by $\mathcal{A}(\varphi)$ the family of all completely nonunitary contractions $T \in B(\mathcal{H})$ such that $\varphi(T) = 0$.
For every $x \in \mathcal{H}$

$$\begin{aligned} x = (1 - T^*T)x \quad &+ \quad T^*(1 - T^*T)Tx + T^{*2}(1 - T^*T)T^2x + \\ \ldots \quad &+ \quad T^{*n-1}(1 - T^*T)T^{n-1}x + T^{*n}T^nx; \end{aligned}$$

thus

$$|x|^2 = |Dx|^2 + |DTx|^2 + \ldots + |DT^{n-1}x|^2 + |T^nx|^2.$$

It follows from the proposition quoted above that $T^nx \to 0$ for every x so that the mapping $v : \mathcal{H} \to l^2(\mathcal{D})$ defined by

$$vx = (Dx, DTx, DT^2x, \ldots)$$

is an isometry. Furthermore

$$vT = Bv$$

where B is the backward shift on $l^2(\mathcal{D})$

$$B(y_0, y_1, \ldots) = (y_1, y_2, \ldots).$$

Since $B^n \to 0$ strongly, B is a completely nonunitary contraction so we may form $\varphi(B)$ and Ker $\varphi(B)$. For brevity, we write $B(\varphi)$ for $B|\text{Ker } \varphi(B)$. We prove first that $|\psi(T)| \leq |\psi(B(\varphi))|$.

To see that, we observe first that $\varphi(B)vh = v\ \varphi(T)h = 0$ for every $h \in \mathcal{H}$ so that v maps $\mathcal{H}$ into Ker $\varphi(B)$. It follows that, for each $h \in \mathcal{H}$,

$$\begin{aligned} |\psi(T)h| &= |v\psi(T)h| = |\psi(B)vh| \leq \\ &\leq |(\psi(B)|\text{Ker } \varphi(B))vh| = \\ &= |\psi(B|\text{Ker } \varphi(B))vh| \leq |\psi(B(\varphi))|\ |vh| \leq \\ &\leq |\psi(B(\varphi))\ |h|. \end{aligned}$$

Now consider a complete orthonormal set e_i in $\mathcal{D}$. For each i let R_i be the mapping $R_i : l^2(\mathcal{D}) \to l^2$ defined by

$$R_i(x_0, x_1, \ldots) = ((x_0, e_i), (x_1, e_i), \ldots).$$

It is easy to verify that

$$R_i B = S^* R_i$$

$$|y|^2 = \sum_i |R_i y|^2 \quad \text{for all} \quad y \in l^2(\mathcal{D}).$$

It follows from the intertwining relation that

$$R_i \text{ Ker } \varphi(B) \subset \text{ Ker } \varphi(S^*).$$

Suppose $x \in$ Ker $\varphi(B)$; then

$$\begin{aligned}
|\psi(B)x|^2 &= \sum_i |R_i \psi(B)x|^2 = \sum_i |\psi(S^*) R_i x|^2 = \\
&= \sum_i |(\psi(S^*)|\text{Ker } \varphi(S^*)) R_i x|^2 \leq \\
&\leq |\psi(S^*)|\text{Ker } \varphi(S^*)| \sum_i |R_i x|^2
\end{aligned}$$

it follows that $|\psi(B)|\text{Ker}|\ \varphi(B) \leq |\psi(S^*)|\text{Ker } \varphi(S^*)|$.

To complete the proof, it suffices to observe that $S^*|\text{Ker } \varphi(S^*) \in \mathcal{A}(\varphi)$.

11 Möbius functions of the shift and extremal operators

The extremal operator $T(p)$ corresponding to a polynomial p of degree n with all zeros in the open unit disk is defined as follows.

If S is the shift operator

$$(x_0, x_1, ...) \rightarrow (0.x_0, x_1, ...)$$

on the Hilbert space of all square summable sequences, the kernel of $p(S^*)$ is an n-dimensional S^*-invariant subspace and $T(p)$ is defined as the restriction of S^* to Ker$p(S^*)$. We have shown [12] that $T(p)$ enjoys the following extremum property:

Given any linear contraction T on an n-dimensional Hilbert space such that $p(T) = 0$ then

$$| T^m | \leq | T(p)^m |$$

for all nonnegative m.

The motivation of this result is in the theory of iteration processes: the critical exponent of the n-dimensional Hilbert space being n [11] the norm of the n-th power of an n-dimensional contraction yields important information about the convergence of the corresponding iteration process. In a manner of speaking, the result says that, in the class $A(p)$ of all n-dimensonal contractions T annihilated by p, the convergence of the process $y_{s+1} = Ay_s + b$ cannot be slower than that for the process corresponding to $T(p)$: within the class $A(p)$ the norm of each T^m assumes its maximum at $T(p)$. This extremal property of $T(p)$ can be extended even further: the m-th powers are not the only functions of T maximized at $T(p)$. It is possible to show [21] that the inequality remains valid for any holomorphic function: if h is holomorphic in the unit disk then $| h(T) | \leq | h(T(p)) |$ for any $T \varepsilon A(p)$. It is interesting to note that a simple technical modification of the proof given originally by the author in [12] also yields this extended result [14].

Since $T(p)$ turns out to be nonderogatory, its algebraic structure is easily described. In order to examine its geometric structure, the author has computed, in [12], the matrix of $T(p)$ with respect to a natural orthonormal basis. See also [16]. This matrix asssumes an especially simple form in the important particular case of the polynomial $p(z) = (z - \alpha)^n$; it turns out to be the Toeplitz matrix corresponding to a symbol, a Möbius function.

The method used in [14, 16] was based on identifying the Hilbert space of sequences with the Hardy space H^2 of functions holomorphic in the unit disk and using suitable Blaschke products to construct the basis required. This method involves some computation with H^2 functions but has the advantage of providing insight into the geometric structure of the backward shift when restricted to Ker $p(S^*)$.

In the present note we intend to point out that the results may be obtained in a considerably simpler manner as consequwences of some natural identities involving Möbius functions of the shift operator. The advantage of this approach lies in the fact that it reduces the amount of computations and illuminates different features of the matter; the operator identities are not without interest in their own right. In what follows we intend to prove these identities and to indicate how they can be used to obtain matrix representations of $T(p)$.

The operator identities to be discussed describe relations between Möbius functions of the shift operator on H^2. Although the Hardy space H^2 is our main concern the reader will observe that the identities are valid for an isometry in an arbitrary Hilbert space. The open unit disk will be denoted by D.

For each $\lambda \in D$ we define the evaluation functional $e(\lambda) \in H^2$ by the requirement that $f(\lambda) = (f, e(\lambda))$ for each $f \in H^2$. Thus

$$e(\lambda)(z) = \frac{1}{1 - \lambda^* z}.$$

The shift operator on H^2 will be denoted by S; thus $(Sf)(z) = zf(z)$ for every z in the open unit disk and every $f \in H^2$.

The following two basic identities will be used throughout the present note. They are valid for any isometry S in an arbitrary Hilbert space

$$(S^* - \beta)(S - \alpha^*) = (1 - \alpha^* S^*)(1 - \beta S)$$

$$(1 - \alpha S)(1 - \alpha^* S^*) - (S - \alpha^*)(S^* - \alpha) = (1 - |\alpha|^2)(1 - SS^*).$$

We now proceed to list several elementary formulae which will be used in the sequel. The verification of these formulae is immediate; it will be convenient, however, to explicitly state them since they will be repeatedly used in our considerations.

Notation. For every $\alpha \in D$ we set

$$E(\alpha) = (1 - \alpha S)^{-1}$$

$$M(\alpha) = (S - \alpha^*)(1 - \alpha S)^{-1}$$

11.1 *For every $\alpha \in D$*

$$S^*E(\alpha) = S^* + \alpha E(\alpha)$$

$$S^*e(\alpha) = \alpha^* e(\alpha)$$

Proof. The first formula follows from

$$S^*((1-\alpha S)^{-1} - 1) = S^*\alpha S(1-\alpha S)^{-1}$$

the second relation is a consequence of the identity $e(\alpha) = E(\alpha^*)e(0)$. $\square$

11.2 *For every $\alpha \in D$ the operator $M(\alpha)$ is an isometry, the kernel of $M(\alpha)^*$ is the one-dimensional subspace spanned by $e(\alpha^*)$.*

Proof. For every $\beta = \alpha$ the basic identity yields

$$(S^* - \alpha)(S - \alpha^*) = (1 - \alpha^* S^*)(1 - \alpha S)$$

whence $M(\alpha)^* M(\alpha) = 1$. The second assertion is a consequence of the second basic identity. Indeed, the kernel of $M(\alpha)^*$ equals the range of $1 - M(\alpha)M(\alpha^*)$ and

$$\begin{aligned} 1 - M(\alpha)M(\alpha^*) &= (1-\alpha S)^{-1}((1-\alpha S)(1-\alpha^* S^*) - \\ &- (S-\alpha^*)(S^*-\alpha))(1-\alpha^* S^*)^{-1} = \\ &= (1-\alpha S)^{-1}(1-|\alpha|^2)(1-SS^*)(1-\alpha^* S^*)^{-1}. \end{aligned}$$

Since $(1 - \alpha^* S^*)$ is invertible the range of $1 - M(\alpha)^* M(\alpha)$ is identical with the range of $(1-\alpha S)^{-1}(1 - SS^*)$ and this, in its turn, is the set of all elements of the form $\frac{\vartheta}{1-\alpha z}$.
$\square$

11.3

$$(S^* - \alpha)M(\alpha) = 1 - \alpha^* S^*$$

Proof. A consequence of

$$(S^* - \alpha)(S - \alpha^*) = (1 - \alpha^* S^*)(1 - \alpha S) \qquad \square$$

In this section we intend to establish some simple identities involving operator Blaschke products: Applied to suitable elements of H^2 these operator identities make it possible to construct natural orthonormal bases of $\ker p(S^*)$ with respect to which the matrix of the restriction of S^* assumes a fairly simple triangular form.

We shall need the explicit form of the inverse of a band matrix.

11.4 *Proposition. Given a matrix of the form*

$$B = \begin{pmatrix} 1 & 0 & 0 & & 0 & 0 \\ -\beta_1 & 1 & 0 & & 0 & 0 \\ 0 & -\beta_2 & 1 & & 0 & 0 \\ & & & & & \\ 0 & 0 & 0 & & -\beta_{n-1} & 1 \end{pmatrix}$$

the inverse B^{-1} is

$$B^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ \beta_1 & 1 & 0 & 0 & \dots \\ \beta_{12} & \beta_2 & 1 & 0 & \dots \\ \beta_{13} & \beta_{23} & \beta_3 & 1 & \dots \\ \dots & & & & \end{pmatrix}$$

More precisely $(B^{-1})_{i,k} = \beta_{k+i,i}$ for $k \leq i$ where $\beta_{qq} = 1$, $\beta_{pq} = 0$ for $p > q+1$ and $\beta_{pq} = \beta_p \beta_{p+1} \dots \beta_q$ for $p \leq q$.

Let p be the polynomial

$$p(z) = (z - \alpha_1) \dots (z - \alpha_n)$$

with all zeros $\alpha_j \in D$.
For $k = 1, 2, \dots$ define U_k as follows

$$U_1 = E(\alpha_1)$$

$$\text{if} \quad k > 1, \quad U_k = M(\alpha_1) \dots M(\alpha_{k-1}) E(\alpha_k)$$

The action of S^* on the sequence U_k may be described as follows.
For $k = 1$, we have

$$(S^* - \alpha_1) U_1 = (S^* - \alpha_1) E(\alpha_1) = S^*.$$

Writing, for brevity, $W_k = (S^* - \alpha_k) U_k$, we obtain, for $k > 1$,

$$\begin{aligned} W_k &= (S^* - \alpha_k) E_k M_1 \dots M_{k-1} = S^* M_1 \dots M_{k-1} = \\ &= S^*(S - \alpha_{k-1}^*) E(\alpha_{k-1}) M_1 \dots M_{k-2} = \\ &= (1 - \alpha_{k-1}^* S^*) E(\alpha_{k-1}) M_1 \dots M_{k-2} = \\ &= U_{k-1} - \alpha_{k-1}^* (W_{k-1} + \alpha_{k-1} U_{k-1}) = \sigma_{k-1} U_{k-1} - \alpha_{k-1}^* W_{k-1} \end{aligned}$$

where we have set $\sigma_m = 1 - |\alpha_m|^2$. Summing up, we have the following sequence of equations

$$W_1 = S^*$$

$$W_2 + \alpha_1^* W_1 = \sigma_1 U_1$$

$$W_3 + \alpha_2^* W_2 = \sigma_2 U_2.$$

$$\dots$$

This sequence of equations may be restated in the form of a matrix equation

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ \alpha_1^* & 1 & 0 & \dots & 0 & 0 \\ 0 & \alpha_2^* & 1 & \dots & 0 & 0 \\ & & & & \vdots & \\ 0 & 0 & 0 & \dots & \alpha_{n-1}^* & 1 \end{pmatrix} \begin{pmatrix} W_1 \\ W_2 \\ \\ W_n \end{pmatrix} = \begin{pmatrix} S^* \\ \sigma_1 U_1 \\ \\ \sigma_{n-1} U_{n-1} \end{pmatrix}.$$

Replacing, for simplicity, α_i^* by $-\beta_i$, we obtain

$$\begin{pmatrix} W_1 \\ \\ W_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & & \\ -\beta_1 & 1 & 0 & & \\ 0 & -\beta_2 & 1 & & \\ & & & \ddots & \\ & & & -\beta_{n-1} & 1 \end{pmatrix}^{-1} \begin{pmatrix} S^* \\ \sigma_1 U_1 \\ \\ \sigma_{n-1} U_{n-1} \end{pmatrix}. \qquad (11.1)$$

Thus W_i equals the scalar product of the row of index $i-1$ with the column $(S^*, \sigma_1 U_1, \dots \sigma_{n-1} U_{n-1})^T$. Thus $W_1 = S^*$ and, for $i > 1$,

$$\begin{aligned} W_i &= \beta_1 \dots \beta_{i-1} S^* + \beta_2 \dots \beta_{i-1} \sigma_1 U_1 + \beta_3 \dots \beta_{i-1} \sigma_2 U_2 + \dots \\ &+ \qquad \beta_{i-1} \sigma_{i-2} U_{i-2} + \sigma_{i-1} U_{i-1} \end{aligned}$$

Proposition. The action of S^* is described by the relations

$$S^* U_1 = S^* + \alpha_1 U_1$$

for $i > 1$

$$\begin{aligned} S^* U_i &= \beta_1 \dots \beta_{i-1} S^* + \beta_2 \dots \beta_{i-1} \sigma_1 U_1 + \beta_3 \dots \beta_{i-1} \sigma_2 U_2 + \\ &+ \dots + \beta_{i-1} \sigma_{i-2} U_{i-2} + \sigma_{i-1} U_{i-1} + \alpha_i U_i \end{aligned}$$

Proposition. The vectors $e_i = \sigma_i^{1/2} U_i e_0$, $i = 1, 2, \dots, n$ form an orthonormal system. The matrix of S^* with respect to this basis is given by

$$\begin{aligned} (S^* - \alpha_i) e_i &= \sigma_1^{1/2} \beta_2 \dots \beta_{i-1} \sigma_i^{1/2} e_1 + \sigma_2^{1/2} \beta_3 \dots \beta_{i-1} \sigma_i^{1/2} e_2 + \\ &+ \sigma_{i-2}^{1/2} \beta_{i-1} \sigma_i^{1/2} e_{i-2} + \sigma_{i-1}^{1/2} \sigma_i^{1/2} e_{i-1} \end{aligned}$$

Proof. Set $u_j = U_j e(0) = M_1 \dots M_{j-1} e(\alpha_j^*)$ and let us show that the set $u_1, \dots, u_n$ is orthogonal. Indeed, if $j < k$ we have

$$\begin{aligned} (u_j, u_k) &= (e(\alpha_j^*), M_j \dots M_{k-1} e(\alpha_k^*)) = \\ &= (M(\alpha_j)^* e(\alpha_j^*), M_{j+1} \dots M_{k-1} e(\alpha_k^*)) = 0. \end{aligned}$$

To prove that $u_j \in \ker p(S^*)$ it suffices to show that $(S^*-\alpha_1)\dots(S^*-\alpha_j)U_j$ may be represented in the form $g(S^*)S^*$ for a suitable polynomial g. Indeed, $(S^*-\alpha_1)U_1 = S^*$. For $j>1$ we obtain, using the identity $(S^*-\alpha) = (1-\alpha^* S^*)M(\alpha)^*$,

$$\begin{aligned}(S^*-\alpha_1)\dots(S^*-\alpha_j)U_j &= (1-\alpha_1^* S^*)\dots(1-\alpha_{j-1}^* S^*)(S^*-\alpha_j)\\ & \quad M_1^*\dots M_{j-1}^* M_1\dots M_{j-1}E(\alpha_j) =\\ &= (1-\alpha_1^* S^*)\dots(1-\alpha_{j-1}^* S^*)S^*.\end{aligned}$$

□

The results admit a reformulation in terms of (operatorvalued) Möbius functions

Proposition. Denote by A the diagonal matrix with $\alpha_1,\dots,\alpha_n$ on the diagonal and by $\mathcal{M}$ the Möbius operator function

$$\mathcal{M}(X) = (X+A)(1+A^*X)^{-1}.$$

Then

$$(S^*U_1,\dots,S^*U_n) = (\beta_{10},\beta_{11},\dots,\beta_{1,n-1})S^* + (U_1,\dots,U_n)\mathcal{M}(S_n^T).$$

Proof. Equation (**??**) may be rewritten in the form

$$\begin{pmatrix} S^*U_1\\ \vdots\\ S^*U_n\end{pmatrix} - A\begin{pmatrix} U_1\\ \vdots\\ U_n\end{pmatrix} = (1+S_nA^*)^{-1}\left(\begin{pmatrix} S^*\\ 0\\ \vdots\\ 0\end{pmatrix} + S_n(1-AA^*)\begin{pmatrix} U_1\\ \vdots\\ U_n\end{pmatrix}\right).$$

Taking transposes

$$\begin{aligned}(S^*U_1,\dots S^*U_n) &= (S^*,0,\dots 0)(1+A^*S_n^T)^{-1} + (U_1,\dots,U_n)\\ &\quad (A+(1-AA^*)S_n^T(1+A^*S_n^T)^{-1}) =\\ &= (\beta_{10},\dots,\beta_{1,n-1})S^* + (U_1,\dots,U_n)(S_n^T+A)(1+A^*S_n^T)^{-1}\end{aligned}$$

In the case of the polynomial $p(z) = (z-\alpha)^n$ the matrix of S^* assumes the particularly simple form of a Toeplitz matrix. We shall see that, in this case, it suffices to work with scalar Möbius functions. We intend to prove the following

11.5 Proposition. *Let $\alpha \in D$, $p(z) = (z-\alpha)^n$, $g(\lambda) = \frac{\lambda+\alpha}{1+\alpha^*\lambda}$, $M = M(\alpha)$, $f(\lambda) = (1-\lambda M)^{-1}$. Then*

$$S^* f(\lambda) = (S^*-\alpha)(1+\alpha^*\lambda)^{-1} + g(\lambda)f(\lambda).$$

The vectors $u_0,\dots,u_{n-1}$, where $u_j = M^j e(\alpha^*)$, form an orthogonal system with respect to which the matrix of S^* equals $g(S_n^*)$.

Proof. Let $\alpha \in D$ and set $M = M(\alpha)$. Consider the operatorvalued analytic function f defined for $\lambda \in D$ as

$$f(\lambda) = (1 - \lambda M)^{-1}.$$

Using $M^* M = 1$, it is easy to prove the relation

$$M^* f(\lambda) = M^* + \lambda f(\lambda).$$

It follows that

$$\begin{aligned} (S^* - \alpha) f(\lambda) &= (1 - \alpha^* S^*) M^* f(\lambda) = \\ &= (1 - \alpha^* S^*)(M^* + \lambda f(\lambda)) = \\ &= S^* - \alpha + \lambda f(\lambda) - \alpha^* \lambda S^* f(\lambda) \end{aligned}$$

whence

$$(1 + \alpha^* \lambda) S^* f(\lambda) = S^* - \alpha + (\lambda + \alpha) f(\lambda).$$

For $S^* f(\lambda)$ we obtain thus

$$S^* f(\lambda) = \frac{S^* - \alpha}{1 + \alpha^* \lambda} + \frac{\lambda + \alpha}{1 + \alpha^* \lambda} f(\lambda).$$

In particular

$$S^* f(\lambda) e(\alpha^*) = \frac{\lambda + \alpha}{1 + \alpha^* \lambda} f(\lambda) e(\alpha^*). \qquad \Box$$

The vectors $u_j = M^j e(\alpha^*)$, $j = 0, 1, \ldots, n-1$ form an orthogonal basis of Ker $p(S^*)$ for $p(z) = (z - \alpha)^n$. If g is the Möbius function $g(\lambda) = \frac{\lambda + \alpha}{1 + \alpha^* \lambda}$ we intend to show that the matrix of S^* with respect to the basis $u_0, \ldots, u_{n-1}$ equals $g(S_n^*)$. This is a consequence of the following identities

$$\begin{aligned} &(S^* u_0, \ldots, S^* u_{n-1})(1, \lambda, \ldots, \lambda^{n-1})^T = \sum_{j=0}^{n-1} S^* u_j \lambda^j = \\ &= S^* f(\lambda) e(\alpha^*) \bmod \lambda^n = g(\lambda) f(\lambda) e(\alpha^*) \bmod \lambda^n = \\ &= g(\lambda) \sum_0^{n-1} u_j \lambda^j \bmod \lambda^n = (u_0 \ldots u_{n-1}) g(S_n^*)(1, \ldots, \lambda^{n-1})^T \end{aligned}$$

12 Complex functions

For the first maximum problem, we have reproduced the original solution given by the author. The later development of dilation theory made it possible to relate the result to powerful theorems that are avaiable today. In this section we intend to explain the connections in order to present the first maximum problem in the context of general dilation theory. We shall use a beautiful inequality due to J. von Neumann and an important theorem of D. Sarason.

12.1 Theorem. *Suppose A is a completely nonunitary contraction on a Hilbert space $\mathcal{H}$ and let $f \in H^\infty$. Then $f(A)$ in meaningful and*

$$|f(A)| \le |f|_\infty.$$

We begin by proving the inequality in the particular case of a Möbius function.

12.2 *Let T be a contraction, α a complex number, $|\alpha| < 1$. Then*

$$|(T-\alpha)(1-\alpha^* T)^{-1}| \le 1.$$

Proof. Given $x \in \mathcal{H}$, set $(1-\alpha^* T)^{-1}x = y$. Thus $|(T-\alpha)(1-\alpha^* T)^{-1}x|^2 - |x|^2 = |(T-\alpha)y|^2 - |(1-\alpha^* T)y|^2 = |Ty|^2 + |\alpha|^2|y|^2 - 2Re(Ty, \alpha y) - |y|^2 - |\alpha|^2|Ty|^2 + 2Re(y, \alpha^* Ty) = (1-|\alpha|^2)(|Ty|^2 - |y|^2) \le 0$.

As an immediate consequence, the inequality $|f(A)| \le |f|_\infty$ may be extended to Blaschke products. The general case is then obtained by a limit process.

To explain the ideas of D. Sarason, we begin by stating a result which says, in a somewhat loose formulation, that the algebra of all bounded linear operators on H^2 commuting with the shift operator may be identified with H^∞, the algebra of all bounded holomorphic functions on the unit disk. More precisely, given a bounded linear operator T on H^2 such that T commutes with S, then

$$T = f(S)$$

for a suitable $f \in H^\infty$. In other words, T is the operator of multiplication by f. The norm of the multiplication operator $M(f)$ equals the norm of f,

$$|M(f)| = |f|_\infty = \sup\{|f(z)|; z \in D\}.$$

We begin by considering the finite-dimensional prototype of this fact.

12.3 *Suppose $T \in B(C^n)$ commutes with S_n. Then $T = a(S_n)$ for a suitable polynomial a.*

Proof. Denote by $(a_0, \ldots, a_{n-1})^T$ the vector Te_0; and by a the polynomial $a_0 + a_1 z + \ldots + a_{n-1}z^{n-1}$. We intend to prove that $T = a(S_n)$.

It suffices to show that $Te_k = a(S_n)e_k$ for $k = 0, 1, \ldots n-1$. Given a k with $0 \le k \le n-1$ we have

$$\begin{aligned} Te_k &= TS_n^k e_0 = S_n^k T e_0 = S_n^k a(S_n) e_0 = \\ &= a(S_n) S_n^k e_0 = a(S_n) e_k. \end{aligned}$$

12.4 *Suppose $T \in B(H^2)$ commutes with S. Then there exists an $a \in H^\infty$ such that $T = a(S)$.*

More precisely, $T = M(a)$, the operator of multiplication by a and $|T| = |a|_\infty$.

Proof. The same argument may be used except that, in this case, we have to show that the function $a = Te_0$ is bounded.

We shall use the fact that $S^*e(w) = w^*e(w)$ for every $w \in D$; thus $p(S)^*e(w) = p(w)^*e(w)$ for every polynomial p.

Consider an arbitrary polynomial p. Then $(Tp, e(w)) = (Tp(S)e_0, e(w)) = (p(S)Te_0, e(w)) = (Te_0, p(S)^*e(w)) = (a, p(w)^*e(w)) = (p(w)a, e(w)) = p(w)a(w)$
$= a(w)p(w)$. Thus T acts, on polynomials, as multiplication by the function a.

To prove that a is bounded, we rewrite the identity just proved in the form

$$(p, T^*e(w)) = (p, a(w)^*e(w)).$$

Since polynomials are dense in H^2, this implies

$$T^*e(w) = a(w)^*e(w)$$

for every $w \in D$ whence $|a(w)^*| \leq |T^*|$. It follows that $a \in H^\infty$ and $|a|_\infty \leq |T|$. Given $f \in H^2$, we have

$$\begin{aligned}(Tf, e(w)) &= (f, T^*e(w)) = (f, a(w)^*e(w)) = \\ &\quad a(w)(f, e(w)) = a(w)f(w).\end{aligned}$$

Thus $T = M(a)$ whence $|T| = |a|_\infty$.

To each (nonconstant) inner function φ we assign a closed subspace $H(\varphi)$ as follows:

$H(\varphi)$ is defined as the orthogonal complement of the set φH^2.

Observe that the multiplication operator $M(\varphi)$ is an isometry so that φH^2 is a closed subspace of H^2; the space H^2 is thus decomposed into the orthogonal sum of two closed subspaces

$$H^2 = H(\varphi) + \varphi H^2.$$

The orthogonal operator $P(H(\varphi))$ will be denoted by $P(\varphi)$.

It is not difficult to give an explicit expression for the projection operator $P(\varphi)$. Indeed

$$P(\varphi)f = M(\varphi)P\_M(\bar{\varphi})$$

for $f \in H^2$.

To see that, consider an $f \in H^2$ and set $g = P(\varphi)f$. It follows that $f = g + \varphi h$ for a suitable $h \in H^2$ and $(g, \varphi H^2) = 0$. Thus $(\bar{\varphi}g, H^2) = 0$ whence

$$\bar{\varphi}g = P\_\bar{\varphi}g = P\_(\bar{\varphi}g + h) = P\_\bar{\varphi}f$$

so that

$$g = \varphi P\_\bar{\varphi}f.$$

We denote by $S(\varphi)$ the compression to $H(\varphi)$ of the operator S

$$S(\varphi) = P(\varphi)S|H(\varphi);$$

since φH^2 is invariant with respect to S the space $H(\varphi)$ is S^* invariant whence

$$P(\varphi)S = P(\varphi)SP(\varphi)$$

and

$$P(\varphi)S = S(\varphi)P(\varphi).$$

This relation implies

$$f(S(\varphi)) = P(\varphi)f(S)|H(\varphi)$$

for every polynomial f.

Denote by k the mapping which assigns to each $f \in H^\infty$ the compression to $H(\varphi)$ of the multiplication operator $M(f)$ on H^2

$$k(f) = P(\varphi)f(S)|H(\varphi) = f(S(\varphi)).$$

Now we may state result of D. Sarason. It represents a complete analogon for $S(\varphi)$ of the result on operators commuting with S. We have seen that every bounded linear operator on H^2 which commutes with S is a function of S (an operator of multiplication by a function $h \in H^\infty$). The theorem of Sarason says that every bounded linear operator on $H(\varphi)$ which commutes with $S(\varphi)$ is a function of $S(\varphi)$. The complete statement is as follows.

12.5 *Denote by $H^\infty(\varphi)$ the algebra of all operators on $H(\varphi)$ which commute with $S(\varphi)$. The mapping k is a homomorphism of H^∞ onto $H^\infty(\varphi)$ the kernel of which is φH^∞. The corresponding isomorphism of $H^\infty/\varphi H^\infty$ onto $H^\infty(\varphi)$ is isometric.*

This is all we shall need. The theorem of Sarason actually says more about this isomorphism: the quotient $H^\infty/\varphi H^\infty$, taken as a Banach space, turns out to be the dual of another Banach space. If we equip $H^\infty/\varphi H^\infty$ with the corresponding weak star topology and if $H^\infty(\varphi)$ is taken in the weak operator topology then the natural isomorphism is homeomorphic.

We now proceed to show how the theorem may be used to obtain a solution of the first maximum problem; the rest of the chapter will be devoted to the proof.

12.6 Theorem *Consider a nonconstant inner function φ. Then*

1^0 *the operator $S(\varphi)$ is a completely nonunitary contraction and $\varphi(S(\varphi)) = 0$*

2^0 *if f is an arbitrary H^∞ function then*

$$|f(A)| \leq |f(S(\varphi))|$$

for any completely nonunitary contraction A on a Hilbert space such that $\varphi(A) = 0$.

Proof. Given any g in the residue class of f,

$$f - g \in \varphi H^\infty,$$

we have $f(A) = g(A)$ and, by the von Neumann inequality,

$$|f(A)| = |g(A)| \leq |g|_\infty$$

whence $|f(A)| \leq |f + \varphi H^\infty|_\infty$. By the theorem of Sarason the quantity on the right hand side equals $|f(S(\varphi))|$; this proves the theorem.

Now let us return to Sarason's theorem.

Consider a $T \in B(H(\varphi))$ such that

$$TS(\varphi) = S(\varphi)T$$

and let us show that, to obtain the result, it suffices to find a lifting of T to an operator $Y \in B(H^2)$ which commutes with S. Indeed, suppose there exists a $Y \in B(H^2)$ such that

$$YS = SY \qquad \text{and} \qquad P(\varphi)Y = TP(\varphi).$$

Since Y commutes with S, there exists an $f \in H^\infty$ such that $Y = M(f) = f(S)$.

In this manner the proof reduces to the construction of a lifting Y with the two properties above.

The existence of such a Y is guaranteed by a powerful theorem due to Sz-Nagy and Foias, the so called commutant lifting theorem. We shall not pursue this method of proof further; instead, we present another less abstract proof, closer to the original idea of D. Sarason. It has the further advantage of establishing a connection with Hankel operators and the Nehari theorem.

We denote by L^2 the L^2space on the unit circle, taken with the normalized Lebesue meaque. For every integer k we define e_k by the formula $e_k(z) = z^k$. Thus H^2 is the set of those $h \in L^2$ for which $(h, e_k) = 0$ for $k < 0$, the orthogonal complement of H^2 in L^2 will be denoted by H^2_- and the corresponding orthogonal projection by P_-.

We denote by U the shift operator on L^2

$$(Uf)(z) = zf(z)$$

and by S its restriction to H^2. If L^∞ stands for the corresponding space of bounded measurable functions, every $f \in L^\infty$ generates the corresponding multiplication operator $M(f)$ and the corresponding Hankel operator $H(f)$ from H^2 into H^2_- defined by the formula

$$H(f) = P_- M(f)|H^2.$$

Now we state the Nehari theorem

12.7 *Suppose A is a bounded linear operator from H^2 into H^2_-. Then the following conditions are equivalent*

$\mathbf{1}^0$ *the matrix of A taken in the natural bases has the Hankel property: there exists a sequence $a_1, a_2, \ldots$ such that*

$$(Ae_i, e_k) = a_{i+k}$$

for all $i \geq 0$, $k > 0$,

$\mathbf{2}^0$ *the operator A intertwines the forward shift on H^2 with the backward shift on H^2_-*

$$P_-UA = AS$$

$\mathbf{3}^0$ *there exists an $f \in L^\infty$ such that*

$$A = H(f).$$

Proof. We prove first the implication $3^0 \to 2^0$. If $A = H(f)$ then,

$$\begin{aligned} & AS = P_-M(f)S = P_-UM(f)|H^2 = \\ = \; & P_-U(P_- + P_+)M(f)|H^2 = P_-UP_-M(f)|H^2 \\ = \; & P_-UA. \end{aligned}$$

The conditions 1^0 and 2^0 are trivially equivalent. This follows from the identity valid for $k \geq 0$ and $j > 0$

$$\begin{aligned} & (Ae_k, e_{-j}) = (AS^k e_0, e_{-j}) = \\ = \; & (AS^k e_0, U^{*j-1} e_{-1}) = (P_-U^{j-1} AS^k e_0, e_{-1}) \end{aligned}$$

if $P_-UA = AS$, the last expression equals $(AS^{j+k} e_0, e_{-1})$
if condition 1^0 is satisfied, we have, for each $k \geq 0$ and $j > 0$

$$\begin{aligned} & (P_-UAe_k, e_{-j}) = (UAe_k, e_{-j}) = (Ae_k, U^* e_{-j}) = \\ & = a_{k+(j+1)} = a_{(k+1)+j} = (ASe_k, e_{-j}) \end{aligned}$$

Since $k \geq 0$ and $j > 0$ were arbitrary, the identity $P_-UA = AS$ follows.

Obviously, the difficult part is the implication from 1^0 or 2^0 to 3^0. This would lead us far from our main topic, so we now proceed to explain the connection with Sarason.

Denote by M the operator of multiplication by φ on L^2, $M = M(\varphi)$. Observe that M is a unitary operator on L^2, $M^* = M(\bar{\varphi})$ and recall that $P(\varphi) = MP_-M^*|H^2$. Furthermore, $M^*H(\varphi) \subset H^2_-$ since $H(\varphi) \perp MH^2$.

12.8 Lemma *Let $A \in B(H(\varphi))$ and consider the operator $B : H^2 \to H(\varphi)$ defined by*

$$B = AP(\varphi).$$

Then the following assertions are equivalent

1^0 *A commutes with $S(\varphi)$*

2^0 *$BS = S(\varphi)B$*

3^0 *M^*B is a Hankel operator*

Proof. If A commutes with $S(\varphi)$ then

$$S(\varphi)B = S(\varphi)AP(\varphi) = AS(\varphi)P(\varphi) = AP(\varphi)S = BS.$$

If $BS = S(\varphi)B$ then

$$AS(\varphi)P(\varphi) = AP(\varphi)S = BS = S(\varphi)B = S(\varphi)AP(\varphi)$$

whence $AS(\varphi) = S(\varphi)A$. Conditions 1^0 and 2^0 are thus equivalent.

If $BS = S(\varphi)B$ then $M^*BS = M^*S(\varphi)B = M^*MP\_M^*SB = P\_UM^*B$ and M^*B is Hankel. If M^*B is Hankel then $BS = MM^*BS = MP\_UM^*B = MP\_M^*SB = S(\varphi)B$.

Now we are able to complete the proof of (9.5).

Proof. Suppose $T \in B(H(\varphi))$ commutes with $S(\varphi)$. It follows that $M^*TP(\varphi) = H(f)$ for some $f \in L^\infty$. Furtermore $H(f)MH^2 = M^*TP(\varphi)MH^2 = 0$ so that $fMH^2 \subset H^2$, in particular $f\varphi \in H^2$. Thus $g = f\varphi \in H^\infty$. If $h \in H(\varphi)$ we have $Th = MH(f)h = MP\_fh = MP\_M^*gh = P(\varphi)gh$. The norm $|T| = |MH(f)| = |H(f)| = \inf |f - H^\infty| = \inf |g - \varphi H^\infty|$. □

13 Nevalinna – Pick revisited

13.1 *Suppose $z_1, \dots, z_n$ and $w_1, \dots, w_n$ are complex numbers such that $z_j \in D$ and the matrix*

$$\frac{1 - w_i^* w_j}{1 - z_i^* z_j}$$

is positive semidefinite. Then there exists a function holomorphic in D, $|f|_\infty \leq 1$ with $f(z_j) = w_j$.

Denote by φ the Blaschke product

$$\varphi(z) = B(z_1) \dots B(z_n)$$

where $B(z_j)$ is the Möbius function

$$B(z_j)(z) = \frac{z - z_j}{1 - z_j^* z}$$

and consider the Hilbert space $H(\varphi)$. We prove first that $H(\varphi)$ coincides with the linear span of $e(z_1), \dots, e(z_n)$.

Indeed, for each $f \in H^2$,

$$(\varphi f, e(z_j)) = \varphi(z_j) f(z_j) = 0$$

so that $e(z_j) \perp \varphi H^2$. On the other hand, if $h \in H^2$ is perpendicular to $e(z_1) \ldots$, $e(z_n)$, we see that k vanishes at the points $z_1, \ldots, z_n$ and is, consequently, divisible by φ.

Now let $A \in B(H(\varphi))$ be defined by the requirement that $A^* e(z_j) = w_j^* e(z_j)$ for $j = 1, 2, \ldots, n$. Since $S(\varphi)^* e(z_j) = S^* e(z_j) = z_j^* e(z_j)$, the operator A^* commutes with $S(\varphi)^*$ whence $AS(\varphi) = S(\varphi)A$.

By our assumption $|A^*| \leq 1$, hence $|A| \leq 1$ and, by the theorem of Sarason, there exists an $f \in H^\infty$, $|f|_\infty \leq 1$ such that $A = P(\varphi)M(f)|H(\varphi)$. Let us show that $f(z_j) = w_j$. Consider an arbitrary $h \in H^2$.

$$\begin{aligned} w_j h(z_j) &= (h, w_j^* e(z_j)) = (h, A^* e(z_j)) = \\ &= (Ah, e(z_j)) = (P(\varphi)M(f)h, e(z_j)) = \\ &= (M(f)h, e(z_j)) = f(z_j)h(z_j). \end{aligned}$$

Since h was an arbitrary element of H^2, the assertion follows.

Bibliography

[1] Z. Dostál: Uniqueness of the operator attaining $C(H_{n,r,n})$. Časopis Pêst. Mat. 103 (1978), 236-243.

[2] Z. Dostál: Polynomials of the eigenvalues and powers of matrices. Comment. Math. Univ. Carolin. 19, 3 (1978), 459-469.

[3] Z. Dostál: Norms of iterates and the spectral radius of matrices. Comment. Math. Univ. Carolin. 105 (1980), 256-260.

[4] H. Flanders: On the norm and spectral radius. Linear and Multilinear Algebra 2 (1974), 239-240.

[5] Y. Kato: Pták type theorem for C^*-algebras. Arch. Math 50 (1988), 550-552.

[6] V. Kiržner, M.I. Tabačnikov: On critical exponents of norms in n-dimensional spaces. Siberian Math. J. 12 (1971), 672-675.

[7] U.I. Ljubi č, M.I. Tabačnikov: On a theorem of Mařík and Pták. Siberian Math. J. 10 (1969), 470-473.

[8] J. Mařík, V. Pták: Norms, spectra and combinatorial properties of matrices. Czech. Math. J. 85 (1960), 181-196.

[9] M. Perles: Critical exponents of convex bodies. Ph. D. Thesis (Hebrew with English Summary), Hebrew University, Jerusalem, 1964.

[10] M. Perles: Critical exponents of convex sets. Proc. Colloq. Convexity, Copenhagen 1965 (Københavns Univ. Mat. Inst.), 1967, 221-228.

[11] V. Pták: Norms and the spectral radius of matrices. Czech Math. J. 87 (1962), 553-557.

[12] V. Pták: Spectral radius, norms of iterates and the critical exponent. Lin. Alg. Appl. 1 (1968), 245-260.

[13] V. Pták: An infinite companion matrix. Comm. Math. Univ. Carol. 19 (1978), 447-458.

[14] V. Pták: A maximum problem for matrices. Lin. Alg. Appl. 28 (1979), 193-204.

[15] V. Pták: A lower bound for the spectral radius. Proc. Amer. Math. Soc. 80 (1980), 435-440.

[16] V. Pták, N.J. Young: Functions of operators and the spectral radius. Lin. Alg. Appl. 29 (1980), 357-392.

[17] V. Pták: A maximum problem for operators. Časopis Pêst Mat. 109 (1984), 168-193.

[18] V. Pták: Extremal operators and oblique projections. Časopis Pêst Mat. 110 (1985), 343-350.

[19] V. Pták: An extremal problem for operators. Lin. Alg. Appl. 84 (1986), 213-226.

[20] D. Sarason: Generalized interpolation in H^∞. Trans. Amer. Matth. Soc. 127 1967, 179-203.

[21] B. Sz-Nagy: Sur la norme des functions de certains opérateurs. Acta Math. Ac. Sci. Hung. 20 (1969), 331-334

[22] H. Wimmer: Spektralradius und Spektralnorm. Czech Math. J. 99 (1974), 501-502.

[23] N.J. Young: Norms of matrix powers. Comment. Math. Univ. Carolin. 19 (1978), 415-430.

[24] N.J. Young: Norms of powers of matrices with constrained spectrum. Lin. Alg. Appl. 23 (1979), 227-244.

[25] N.J. Young: Matrices which maximise and analytic function. Acta Math. Acad. Sci. Hungar 34 (1979), 239-243.