LOGARITHMS OF MATRICES

BURRELL W. HELTON

1. **Introduction.** This paper contains proofs of several theorems concerning logarithms of matrices such as $\log A$ exists if A^{-1} exists, the set of logarithms of I is uncountable, each commutative subset of the logarithms of a matrix A is countable, and each commutative subset of the logarithms of I is a finite-dimensional vector space over the set of integers. Most of these proofs also hold for Banach algebras with suitable norms.

2. **Definitions.** $\boldsymbol{M}$ denotes the algebra of $n\times n$ matrices of complex numbers and $|\cdot|$ denotes a norm with respect to which $\boldsymbol{M}$ is complete, $|I|=1$, and $|A|=0$ if and only if $A=0$. Capital letters will be used to represent elements of $\boldsymbol{M}$, bold-faced letters for sets, and lower case letters for real numbers. Reduced fraction means a rational number expressed as a reduced fraction. The following definitions will be used.

DEFINITION 1. $\operatorname{Exp} A=E(A)=\sum_{n=0}^{\infty}(1/n!)A^n$ and A is a logarithm of B if and only if $B=E(A)$.

DEFINITION 2. $\operatorname{Log} A$ denotes the subset of $\boldsymbol{M}$ such that $B\in\operatorname{Log} A$ if and only if B is a logarithm of A.

DEFINITION 3. A is nonsingular means A^{-1} exists.

DEFINITION 4. A is a reduced logarithm of I means $A\in\operatorname{Log} I$ and if $0<|p|<1$, then $pA\notin\operatorname{Log} I$.

DEFINITION 5. B is a preferred logarithm of A means $B\in\operatorname{Log} A$ and if A commutes with C, then B commutes with C.

3. **Theorems.** A proof of Theorem 1 can be found in [1, p. 167].

THEOREM 1. *If* $M=E(A)$, $N=E(B)$ *and* $AB=BA$, *then*

$$E(A)E(B) = E(A+B)$$

and

$$A+B\in\operatorname{Log} MN.$$

THEOREM 2. *If B is a continuous function of bounded variation from $[0, 1]$ into $\boldsymbol{M}$ such that B^{-1} exists, all values of B commute and $B(0)=1$, then $\int_0^x B^{-1}dB$ is a preferred logarithm of $B(x)$ for $0\leq x\leq 1$.*

OUTLINE OF PROOF.

Received by the editors February 7, 1967.

$$B(x) = 1 + \int_0^x BB^{-1}dB = 1 + \int_0^x B^{-1}(t)dB(t)$$
$$+ \int_0^x \left[\int_0^t B^{-1}(p)dB(p)\right]B^{-1}(t)dB(t) + \cdots$$
$$= \sum_{n=0}^{\infty} (1/n!)\left(\int_0^x B^{-1}dB\right)^n.$$

The following theorem, due to M. Nagumo [**4**, p. 67], follows as a corollary to the preceding theorem.

THEOREM 3. *If A^{-1} exists, then A has a preferred logarithm.*

PROOF. Since there are only a finite set of values z for which $[I+z(A-I)]^{-1}$ does not exist and since A^{-1} exists, there is a continuous function g of bounded variation from $[0, 1]$ to the complex numbers such that $g(0)=0$, $g(1)=1$ and, if $B(x)=[I+g(x)(A-I)]$, then B satisfies the hypothesis of Theorem 2. Since $B(1)=A$, then $\int_0^1 B^{-1}dB \in \text{Log } B(1) = \text{Log } A$. The referee has pointed out that the argument used in Theorems 2 and 3 yields the more general Theorem 9.5.1 in Hille and Phillips [**3**, p. 285].

THEOREM 4. *If $A \in \text{Log } I$ and $|A| < 1$, then $A=0$.*

PROOF. $0=E(A)-I=(I+\sum_{k=1}^{\infty} A^k/k!)-I=A(I+B)$, where $B=A/2!+A^2/3!+\cdots$. Since $|B|<1$, then $(I+B)^{-1}$ exists and $A=0$.

THEOREM 5. *Log I is an uncountable set.*

PROOF. There exists uncountably many pairs a, b of positive numbers such that $a^2+b^2=1$ and such that

$$\begin{pmatrix} a & b & & & \\ b & -a & & 0 & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 1 \end{pmatrix} = A$$

is a nonsingular square root of I. Hence, there exist uncountably many matrices of the form $\log A$ such that $I=E(2 \log A)$.

THEOREM 6. *If S is a commutative subset of* Log A, *then S is countable.*

PROOF. If S is an uncountable subset of Log A, then S has an uncountable bounded subset which has an accumulation point. Hence, there exist matrices B, $C\in S$ such that $0<|B-C|<1$ and $E(B)=A=E(C)$. Therefore, $E(B-C)=I$ and by Theorem 4 $B-C=0$ which contradicts $0<|B-C|$.

THEOREM 7. *If $0\neq A\in \text{Log } I$, then there is a unique positive number n such that if k is a real number, then $k/nA\in \text{Log } I$ if and only if k is an integer. Furthermore, n is an integer.*

PROOF. Suppose $0\neq A\in \text{Log } I$ and S is the set of positive numbers such that $h\in S$ if and only if $hA\in \text{Log } I$. The set S has a greatest lower bound m; furthermore, $m\in S$. If $m\notin S$, there are numbers p, $q\in S$ such that $0<|(p-q)|<1$ and by Theorem 4 $(p-q)A=0$; this last equation contradicts the preceding inequality.

If k is an integer, then $kmA\in \text{Log } I$ because $mA\in \text{Log } I$. If k is a real number such that $kmA\in \text{Log } I$, then k is an integer; if this is false, then there is an integer h such that $1>h-k>0$, $(h-k)mA \in \text{Log } I$, and $m>(h-k)m\in S$. Since $(1/m)mA=A\in \text{Log } I$, then $1/m$ is a positive integer n such that $mA=(1/n)A$. Furthermore, n is unique, because if p is a number satisfying these conditions, then

$$((p+n)/p)((1/n)A) = ((p+n)/n)((1/p)A) = (1/n+1/p)A \in \text{Log } I,$$

$(p+n)/p$ and $(p+n)/n$ are integers, n divides p and p divides n, and $n=p$.

THEOREM 8. *If A and B commute and are reduced logarithms of I and a/p and b/q are reduced fractions such that $(a/p)A+(b/q)B\in \text{Log } I$, then $p=q$.*

PROOF. $(a/p)A+(b/q)B\in \text{Log } I\rightarrow aA+(bp/q)B\in \text{Log } I\rightarrow (bp/q)B \in \text{Log } I\rightarrow q$ divides $bp\rightarrow q$ divides p. Similarly, p divides q; hence, $p=q$.

THEOREM 9. *If B is a preferred logarithm of A and $A^{1/m}$ is an mth root of A such that $(A^{1/m})^{-1}$ exists, then there is an mth root $I^{1/m}$ of I such that $A^{1/m}=E(B/m)I^{1/m}$.*

PROOF. Since $(A^{1/m})^{-1}$ exists, $A^{1/m}$ has a preferred logarithm C. Furthermore, B and C commute because A and $A^{1/m}$ commute. Since $E(mC)=A=E(B)$, then $E(mC-B)=I$ and there is an mth root $I^{1/m}$ of I such that $E(C-B/m)=I^{1/m}$. Hence,

$$E(B/m)I^{1/m} = E(B/m)E(C-B/m) = E(C) = A^{1/m}.$$

LEMMA 1. *If b is an irrational number and $a>0$, there are integers p*

and q and an irrational number r such that $pb=q+r$ and $|r|<a$ (Corollary to [2, *Theorem* 36, *p.* 30]).

THEOREM 10. *If $\{A_i\}_{i=0}^m$ is a commutative sequence of linearly independent logarithms of I and $\{a_i\}_{i=0}^m$ is a sequence of real numbers such that $\sum_{i=0}^m a_iA_i \in \operatorname{Log} I$, then a_0 is a rational number.*

PROOF. Suppose $\{A_i\}_{i=0}^m$ and $\{a_i\}_{i=0}^m$ satisfy the hypothesis and that a_0 is an irrational number. From the lemma, if $1>c>0$, there exist integers p and q and an irrational number b_0 such that $pa_0 = q+b_0$ and $|b_0|<c$. Furthermore, $\sum_{i=0}^m pa_iA_i \in \operatorname{Log} I$. Let $\{b_i\}_{i=1}^m$ be the sequence of numbers such that for $i=1, \cdots, m$, $b_i=pa_i-n_i$ where n_i is the largest integer such that $pa_i \geqq n_i$; then $\sum_{i=0}^m b_iA_i \in \operatorname{Log} I$, $|b_i|<1$ for $i=0, 1, \cdots, m$, and $|\sum_{i=0}^m b_iA_i| \leqq \sum_{i=0}^m |A_i|$. Therefore, for each positive integer k, there is a matrix B_k and a sequence $\{b_{ki}\}_{i=0}^m$ of numbers such that $B_k=\sum_{i=0}^m b_{ki}A_i$ is a logarithm of I, $|B_k| \leqq \sum_{i=0}^m |A_i|$, b_{k0} is an irrational number and $|b_{k+1,0}| < |b_{k0}|$.

Since $\{B_k\}_{k=1}^\infty$ is a bounded sequence, it has a convergent subsequence and there exist two integers r and t such that $|B_r-B_t|<1$. From Theorem 4, it follows that $B_r-B_t=0$. However, $B_r-B_t = \sum_{i=0}^m (b_{ri}-b_{ti})A_i \neq 0$ because $A_0, A_1, \cdots, A_m$ are linearly independent and $b_{r0}\neq b_{t0}$.

LEMMA 2. *If m and a are positive integers such that a does not divide m, then there are integers p and q and a reduced fraction c/b such that $p/m+q/a=c/b$ and $b>m$ (Corollary to* [2, *Theorem* 25, *p.* 21]).

LEMMA 3. *If S is a commutative subset of* Log *I which is closed with respect to addition and subtraction, a/b is a reduced fraction, $A\in S$, $(a/b)A+B\in S$ and p is an integer, then there is an integer q such that $(p/b)A+qB\in S$.*

THEOREM 11. *Suppose S is a commutative subset of* Log *I which is closed with respect to addition and subtraction. Conclusion. There exist an integer $m\leqq 2n^2$ and linearly independent elements $B_1, B_2, \cdots, B_m$ of S such that if $B\in S$ then there exist integers $b_1, b_2, \cdots, b_m$ such that $B=\sum_{i=1}^m b_iB_i$.*

PROOF. Since S is a subset of the linear vector space of $n\times n$ matrices with complex elements, then there exist, over the field of real numbers, m linearly independent elements $A_1, A_2, \cdots, A_m$ of S which span S and $m\leqq 2n^2$. By Theorem 15 if $\{p_i\}_{i=1}^k$ is a sequence of real numbers such that $\sum_{i=1}^k p_iA_i\in S$, then each of $p_1, p_2, \cdots, p_k$ is a rational number.

For each integer $t=1, 2, \cdots, m$, let $\boldsymbol{K}_t$ denote the set of positive integers such that $k\in\boldsymbol{K}_t$ if and only if there is a sequence $\{a_i/b_i\}_{i=t}^m$ of reduced fractions such that $\sum_{i=t}^m (a_i/b_i)A_i\in\boldsymbol{S}$, $|a_i/b_i|<1$ for $i=t, t+1, \cdots, m$ and $k=b_t>0$. $\boldsymbol{K}_t$ is not an infinite set. If this is false, there exists a set $\{M_j\}_{j=1}^\infty\subset\boldsymbol{S}$ such that $|M_j|<\sum_{i=1}^m |A_i|$ for $j=1, 2, 3, \cdots$, and $M_k\neq M_j$ if $k\neq j$; therefore, there exist two positive integers p and q such that $M_p\neq M_q$, $|M_p-M_q|<1$ and from Theorem 9 $M_p=M_q$. Hence, if $\boldsymbol{K}_t$ is nonempty, it is a finite set and has a largest positive integer m_t.

If $1\leqq t\leqq m$ and $\sum_{i=t}^m (a_i/b_i)A_i\in\boldsymbol{S}$ and a_t/b_t is a reduced fraction, then b_t divides m_t. Suppose false; then, if $b_t>0$, by Lemma 2, there exist integers p and q and a reduced fraction k/b such that $b>m_t$ and $p/m_t+q/b_t=k/b$. By Lemma 3, there are matrices C and D of the form $\sum_{i=t+1}^m (a_i/b_i)A_i$ such that $(p/m_t)A_t+C\in\boldsymbol{S}$ and $(q/b_t)A_t+D\in\boldsymbol{S}$; therefore,

$$(k/b)A_t + C + D = ((p/m_t)A_t + C) + ((q/b_t)A_t + D) \in \boldsymbol{S};$$

hence, $b\in\boldsymbol{K}_t$ and $b\leqq m_t$, which contradicts $b>m_t$. Similarly, if $b_t<0$, then $a_t/b_t=-a_t/-b_t$ and $-b_t$ divides m_t.

If $0\leqq t\leqq m$, $\boldsymbol{K}_t$ is nonempty and m_t is the largest integer in $\boldsymbol{K}_t$, then by Lemma 3 there is a matrix B_t and a sequence $\{c_{ti}\}_{i=t+1}^m$ of reduced fractions such that $B_t=(1/m_t)A_t+\sum_{i=t+1}^m c_{ti}A_i$ and $B_t\in\boldsymbol{S}$. These matrices $B_1, B_2, \cdots, B_m$ are linearly independent and will satisfy the conclusion of the theorem. If $B\in\boldsymbol{S}$, there are reduced fractions $a_1/b_1, k_{12}, k_{13}, \cdots, k_{1m}$ such that $B=(a_1/b_1)A_1+\sum_{i=2}^m k_{1i}A_i$ belongs to $\boldsymbol{S}$; also, there exists an integer x_1 such that $m_1=x_1b_1$. Since $B_1=1/m_1A_1+\sum_{i=2}^m c_{1i}A_i$, then

$$\begin{aligned} B &= B - a_1x_1(B_1 - B_1) \\ &= (a_1/b_1)A_1 + \sum_{i=2}^m k_{1i}A_i - a_1x_1\left((1/m_1)A_1 + \sum_{i=2}^m c_{1i}A_i\right) + a_1x_1B_1 \\ &= a_1(1/b_1 - x_1/m_1)A_1 + \sum_{i=2}^m (k_{1i} - a_1x_1c_{1i})A_i + a_1x_1B_1 \\ &= 0 + \sum_{i=2}^m k_{2i}A_i + a_1x_1B_1, \quad \text{where } k_{2i} = k_{1i} - a_1x_1c_{1i}. \end{aligned}$$

Similarly, there are integers a_2 and x_2 and a sequence $\{k_{3i}\}_{i=3}^m$ of rational numbers such that

$$\sum_{i=2}^m k_{2i}A_i = a_2x_2B_2 + \sum_{i=3}^m k_{3i}A_i.$$

By continuing this procedure with $B_3, \cdots, B_m$, we define sequences $\{a_i\}_{i=1}^m$ and $\{x_i\}_{i=1}^m$ of integers such that $B = \sum_{i=1}^m a_i x_i B_i$.

THEOREM 12. *If* S *is a commutative subset of* Log A, *then there exist an integer* $m \leqq 2n^2$ *and a sequence* $\{C_i\}_{i=1}^m$ *of linearly independent commutative elements of* Log I *such that if* P *and* Q *belong to* S, *then there exists a sequence* $\{a_i\}_{i=1}^m$ *of integers such that* $P = Q + \sum_{i=1}^m a_i C_i$. *Furthermore, for* $i = 1, 2, \cdots, m$, C_i *commutes with each element of* S.

PROOF. If P and Q belong to S, then $P - Q \in \text{Log } I$. Let R be the subset of Log I such that $B \in R$ if and only if there exist sequences $\{A_i\}_{i=1}^k$ and $\{B_i\}_{i=1}^k$ of elements of S and a sequence $\{a_i\}_{i=1}^k$ of integers such that $B = \sum_{i=1}^k a_i(A_i - B_i)$. Theorem 11 holds and assures the existence of a sequence $\{C_i\}_{i=1}^m$ of linearly independent elements of R such that if P and Q belong to S, then $P - Q$ belongs to R and there exists a sequence $\{a_i\}_{i=1}^m$ of integers such that $P - Q = \sum_{i=1}^m a_i C_i$. Furthermore, all the elements of R and S commute.

BIBLIOGRAPHY

1. Richard Bellman, *Introduction to matrix analysis*, McGraw-Hill, New York, 1960.

2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford Univ. Press, London, 1965.

3. Einar Hille and Ralph S. Phillips, *Functional analysis and semi-groups*, rev. ed., Amer. Math. Soc. Colloq. Publ., Vol. 31, Amer. Math. Soc., Providence, R. I., 1957.

4. Von Mitio Nagumo, *Einige analytische Untersuchungen in linearen metrischen Ringen*, Japan. J. Math. **13** (1936), 61–80.

SOUTHWEST TEXAS STATE COLLEGE