# On reducing subspaces of composition operators 

JAMES GUYKER

If $\varphi$ is an analytic function mapping the unit disk into itself, Ryff [10] has shown that $\varphi$ induces a bounded linear operator $C_{\varphi}$ on Hardy space $H^{2}$ defined by $C_{\varphi} f=f \circ \varphi$. Many of the basic properties of $C_{\varphi}$ depend on the fixed points of $\varphi$ in the closure of the disk (see [4], [9] for references). If $\varphi$ is not a rotation about a fixed point, then by the Denjoy-Wolff theorem ([6], [13]) $\varphi$ has a unique fixed point $\alpha$ such that $\left|\varphi^{\prime}(\alpha)\right| \leqq 1$. In this paper, the reducing subspaces of classes of $C_{\varphi}$ are characterized when $|\alpha|<1$ and either $\varphi$ is univalent or some positive integral power of $C_{\varphi}$ is compact. The complementary case when $\alpha=0$ and $\varphi$ is inner follows from results of Nordgren [8] and Brown [2].

Notion. We will assume henceforth that $\varphi$ is neither a constant nor a Möbius transformation of the disk onto itself, that $\alpha$ is the Denjoy-Wolff fixed point of $\varphi$, and that $|\alpha|<1$. Then $\left|\varphi^{\prime}(\alpha)\right|<1$, and there is a natural basis of $H^{2}$ with respect to which $C_{\varphi}$ is lower triangular with diagonal $\left[1, \varphi^{\prime}(\alpha), \varphi^{\prime}(\alpha)^{2}, \ldots\right]$. Indeed, let

$$
b_{n}(\alpha, z)=\frac{\left(1-\left.|\alpha|\right|^{2}\right)^{1 / 2}}{1-z \bar{\alpha}}\left[\frac{z-\alpha}{1-z \bar{\alpha}}\right]^{n} \quad(n=0,1, \ldots),
$$

then for $i \leqq j$,

$$
\left\langle C_{\varphi} b_{j}, b_{i}\right\rangle=\left\langle\frac{1-|\alpha|^{2}}{1-\varphi(z) \bar{\alpha}}\left[\frac{\varphi(z)-\varphi(\alpha)}{z-\alpha}\right]^{j}\left[\frac{1-z \bar{\alpha}}{1-\varphi(z) \bar{\alpha}}\right]^{j}\left[\frac{z-\alpha}{1-z \bar{\alpha}}\right]^{j-i}, \frac{1}{1-2 \bar{\alpha}}\right\rangle,
$$

which is $\varphi^{\prime}(\alpha)^{\prime}$ whenever $i=j$, and is 0 when $i<j$.
Moreover, if $f$ is in $H^{2}$, then $f=\Sigma\left\langle f, b_{n}\right\rangle b_{n}$ where

$$
\left\langle f, b_{n}\right\rangle=\sum_{k=0}^{n}\binom{n}{k} \frac{f^{(k)}(\alpha)}{k!}(-\bar{\alpha})^{-n-k}\left(1-|\alpha|^{2}\right)^{k+(1 / 2)} .
$$

This follows directly by writing $f$ in terms of its Taylor series, expanding

$$
\left[\frac{z-\alpha}{1-z \bar{\alpha} \bar{\alpha}}\right]^{n}=\left[-\alpha+\left(1-|\alpha|^{2}\right) \frac{z}{1-z \bar{\alpha}}\right]^{n}
$$

Received July 29, 1986.
by the binomial theorem, and by observing that $\left\langle(z-\alpha)^{k}, z^{n} /(1-z \bar{\alpha})^{n+1}\right\rangle$ is 0 whenever $n \neq k$, and is 1 when $n=k$, since the adjoint of multiplication by $z /(1-z \bar{\alpha})$ on $H^{2}$ maps $h(z)$ into $(h(z)-h(\alpha)) /(z-\alpha)$.

We recall that a subspace $\mathscr{M}$ reduces an operator $T$ on a Hilbert space $\mathscr{H}$ if both $\mathscr{M}$ and $\mathscr{H} \ominus \mathscr{M}$ are invariant under $T$, or equivalently, if the orthogonal projection onto $\mathscr{M}$ commutes with $T$. If the only subspaces that reduce $T$ are $\{0\}$ and $\mathscr{H}$ itself, then $T$ is said to be irreducible (otherwise $T$ is reducible).

Theorem 1. If $\varphi$ is univalent and $\alpha \neq 0$, then $C_{\varphi}$ is irreducible.
When $\alpha=0$, the constants reduce $C_{\varphi}$. In fact, by [4, Theorem 4.1], the kernel of $1-C_{\varphi}$ contains only the constant functions, so it follows in this case that $\mathscr{M}$ reduces $C_{\varphi}$ if and only if $\mathscr{M}=\mathscr{M}_{0} \oplus \mathscr{M}_{1}$, where $\mathscr{M}_{0}$ is either $\{0\}$ or the space of constants, and $\mathscr{M}_{1}$ reduces the restriction of $C_{\varphi}$ to $z H^{2}$. A complete description (Theorem 2) of the subspaces $\mathscr{M}_{1}$ may be obtained under a compactness condition, with univalence weakened to $\varphi^{\prime}(\alpha) \neq 0$. The study of compact composition operators was initiated by Schwartz in [11], and continued by several authors ([3], [5], [12]). In particular, Caughran and Schwartz [3, Theorem 2] have shown that when some positive integral power of $C_{\varphi}$ is compact, the Denjoy-Wolff point always lies inside the disk. Note that $C_{\varphi}^{N}=C_{\varphi_{N}}$ where $\varphi_{N}$ is defined inductively by $\varphi_{1}=\varphi$ and $\varphi_{n+1}=\varphi \circ \varphi_{n}$.

Theorem 2. Suppose that $C_{\varphi}^{N}$ is compact for some positive integer $N$, and that $\varphi^{\prime}(\alpha) \neq 0$. Then $C_{\varphi}$ is reducible if and only if $\alpha=0$. Moreover, if $\alpha=0$, then the restriction of $C_{\varphi}$ to $\mathrm{zH}^{2}$ is reducible if and only if there exists an $H^{\infty}$ function $\Psi$ which is bounded by one, and a nonnegative integer $p \neq 1$, such that $\varphi(z)=z \Psi\left(z^{p}\right)$; in this -case, a subspace $\mathscr{M}$ reduces $C_{\phi}$ restricted to $z H^{2}$ if and only if $\mathscr{M}=\vee\left\{b_{i p+j}: i \geqq 0\right.$, $j \in \Gamma\}$ where $\Gamma$ is an arbitrary subset of $\{1, \ldots, p\}(\{1,2, \ldots\}$ if $p=0)$.

The reducing subspaces of more general composition operators are formed from cyclic subsets of basis vectors as follows. Let $j \geqq 1, p \geqq 0$, and $r \geqq 1$ be integers such that if $p>0$, then $j \leqq p$ and $p$ is relatively prime to $r$. Let $j_{0}=j$ and $j_{n+1}=$ $=r j_{n}-i_{n} p(n=0,1, \ldots)$ where $i_{n}$ is the unique integer which is 0 if $p=0$, and satisfies $i_{n} p<r j_{n} \leqq\left(i_{n}+1\right) p$ if $p>0$. The set $\left\{j_{n}: n \geqq 0\right\}$ will be called the $(r, p)$-cycle generated by $j$. Let $p>0$. Then since $1 \leqq j_{n} \leqq p$ for all $n$, the terms of the sequence $j_{n}$ repeat. It follows easily that if $j_{m+1}=j_{n+1}(m>n)$, then $j_{m}=j_{n}$; and hence $j_{m-n}=j$. Therefore, $j$ is the first term to reappear. Moreover, the set $\{1, \ldots, p\}$ $(\{1,2, \ldots\}$ if $p=0)$ may be written as a disjoint union of $(r, p)$-cycles. With no additional conditions on $\varphi$, we have

Theorem 3. If $\alpha \neq 0$, then no nontrivial closed span of basis vectors $b_{n}(n \geqq 0)$ reduces $C_{\varphi}$. If $\alpha=0$, and is of order $r$, then a nontrivial closed span $\mathscr{A}$ of vectors $b_{n}$
( $n \geqq 1$ ) reduces the restriction of $C_{\varphi}$ to $z H^{2}$ if and only if there exists a nonnegative integer $p \neq 1$, which is relatively prime to $r$ whenever $p \neq 0$, such that $\varphi(z)=z^{r} \Psi\left(z^{p}\right)$ for some $H^{\infty}$ function $\Psi$ which is bounded by one, and $\mathscr{M}=\vee\left\{b_{i p+j}: i \geqq 0, j \in \Gamma\right\}$ where $\Gamma$ is a union of $(r, p)$-cycles.

In view of the above results, a natural question is: when either $\varphi$ is univalent or $C_{\varphi}^{N}$ is compact, are all the reducing subspaces of $C_{\varphi}$ closed spans of basis vectors? The related step in the proof of Theorem 2 follows by expressing the span of the first $n$ basis vectors ( $n=0,1, \ldots$ ) in terms of the kernel of some element of the von Neumann algebra generated by $1, C_{\varphi}$ and $C_{\varphi}^{*}$. A similar argument may be used in the following example.

Example 1. Let $\varphi=\lambda \theta$ where $\lambda$ is a constant $(0<|\lambda|<1)$ and $\theta$ is an inner function such that $\theta(0)=0$. By ([1, Theorem 20], [8, Theorem 1], or [10, Theorem 3]), $C_{\theta}$ is an isometry, so that $C_{\varphi}^{*} C_{\varphi}$ is a diagonal operator with diagonal $\left(1,|\lambda|,|\lambda|^{2}, \ldots\right)$. Therefore, $\bigvee_{0}^{n} b_{i}=\operatorname{ker} \prod_{0}^{n}\left(C_{\varphi}^{*} C_{\varphi}-|\lambda|^{i}\right)(n=0,1, \ldots)$, and it follows that the reducing subspaces are closed spans of $b_{n}$ 's and are thus described by Theorem 3.

Further evidence is provided by the following result which implies that reducing subspaces are (at least) closed spans of finite linear combinations of basis vectors.

Theorem 4. Suppose that $\|\varphi\|_{\infty}<1$ and $\varphi^{\prime}(\alpha)=0$. If $X$ commutes with $C_{\varphi}$ and $\left(\lambda_{i j}\right)$ is the matrix of $X$ with respect to $\left\{b_{n}\right\}$, then $\lambda_{0 j}=0(j=1,2, \ldots)$ and there exists an integer $M$ such that $\lambda_{i j}=0(i=1,2, \ldots)$ for every $j \geqq M i$.

Theorem 4 suggests an alternative approach to answering the above question in the affirmative, as illustrated by

Example 2. Let $\alpha=0$ be of order $r>1$, and suppose that $\varphi$ is a polynomial of degree $r^{M}$ such that $\left\|\varphi_{N}\right\|_{\infty}<1$ for some positive integers $M$ and $N$. Then the reducing subspaces of $C_{\varphi}$ are given by Theorem 3: Let $P$ be the projection onto a reducing subspace. Since $P$ commutes with $C_{\Phi_{N}}^{*}$, it follows from Theorem 4 that $P b_{n}$ is a polynomial for every $n$; thus, it suffices to show that the degree of $P b_{n}$ does not exceed $n$ for every $n$. Suppose that $n<\operatorname{deg} P b_{n}$ for some $n$, and let $i$ be the least such integer. Setting $j=\operatorname{deg} P b_{i}$, we have that

$$
\left\langle P C_{\varphi_{N}}^{*^{M}} C_{\varphi_{N}} b_{i}, b_{j}\right\rangle=\left\langle C_{\varphi_{N}}^{*_{N}^{M}} C_{\varphi_{N}} P b_{i}, b_{j}\right\rangle
$$

and hence by straightforward calculations, $\mu^{i}=\mu^{j}$ where

$$
\mu=\left[\left\langle b_{r}, \varphi\right\rangle^{1 /(r-1)}\left\langle\varphi, b_{r M}\right\rangle^{1 /\left(r^{M}-1\right)}\right]^{r^{M N-1}}
$$

(so that $0<|\mu|<1$ ). Therefore $i=j$, a contradiction.

The verification of Theorem 3 depends upon a reformulation of the usual multinomial theorem, which subsequently determines how often powers of $\varphi$ have nonzero coefficients.

Lemma. Let

$$
f(z)=a_{10}+\sum_{i=1}^{\infty} \sum_{j=0}^{p-1} a_{1, i_{p+j}} z^{i p+j}
$$

be a formal power series where $a_{10}$ is nonzero, and for $j=0,1, \ldots$, define

$$
\hat{a}_{1 j}=a_{1, p+j} \quad \text { and } \quad \hat{a}_{m J}=\sum_{k=0}^{j} a_{1, p+k} \hat{a}_{m-1, j-k} \quad(m>1) .
$$

Then for every positive integer $n$,

$$
f(z)^{n}=a_{10}^{n}+\sum_{i=1}^{\infty} \sum_{j=0}^{p-1} a_{n, i p+j} z^{i p+j}
$$

where

$$
a_{n, i p+j}=\sum_{m=1}^{i}\binom{n}{m} a_{10}^{n-m} \hat{a}_{m,(i-m) p+j}
$$

In particular, for fixed $i$ and $j$, either $a_{n, i p+j}=0$ for all $n \geqq 1$, or $a_{n, i p+j}=0$ for at most $i-1$ values of $n \geqq 1$. If $a_{1 p} \neq 0$, then $a_{n, i p}=0$ for at most $i-1$ values of $n \geqq 1$.

The following estimate in $H^{\infty}$ is essential to the proof of Theorem 4, and may be of independent interest.

Proposition. If $\varphi^{(i)}(\alpha)=0$ for every $i=1, \ldots, r-1$, then

$$
\left\|C_{\varphi}^{n} b_{m}\right\|_{\infty} \leqq\left\|\frac{\varphi-\alpha}{1-\varphi \bar{\alpha}}\right\|_{\infty}^{m\left(r^{n}-1\right)(r-1)}
$$

for all nonnegative integers $m$ and $n$.
Acknowledgments. I am grateful to Professor M. A. Kanshoek for his support and encouragement during my sabbatical at the Free University, at which time this work was completed. Also, I am indebted to Professors L. de Branges and C. C. COWEN for their lectures and conversations concerning composition operators.

Proof of Theorem 1. Let $\mathscr{M}$ reduce $C_{\varphi}$. By [4, Theorem 4.1], the kernel of $1-C_{\varphi}$ consists of just the constant functions. Thus we may assume that constants belong to $\mathscr{M}$, and hence so does $C_{\varphi}^{*^{n}} 1=\left[1-z \overline{\varphi_{n}(0)}\right]^{-1}(n=1,2, \ldots)$.

Let $f$ be orthogonal to $\mathscr{M}$. Then $f$ vanishes on the set $\Omega=\left\{\varphi_{n}(0): n \geqq 1\right\}$. If $\varphi_{m}(0)=\varphi_{n+m}(0)$ for some positive integers $m$ and $n$, then $\varphi_{m}(0)$ is a fixed point of $\varphi_{n}$. But $\alpha$ is also a fixed point of $\varphi_{n}$, and $\varphi_{n}$ is not a rotation about a fixed point
since otherwise $\varphi$ would be inner and hence by [7; Theorem 3.17] $\varphi$ would be a Möbius transformation. Thus it follows that $\varphi_{m}(0)=\alpha=\varphi_{m}(\alpha)$, and since $\varphi_{m}$ is univalent, we have that $\alpha=0$, a contradiction. Hence, the set $\Omega$ consists of distinct points which must cluster in the closure of the disk. However, by Schwarz's lemma,

$$
\left|\frac{\varphi_{n}(z)-\alpha}{1-\varphi_{n}(z) \bar{\alpha}}\right| \leqq\left|\frac{z-\alpha}{1-z \bar{\alpha}}\right|
$$

for every $z$ in the disk. Setting $z=0$, we conclude that $\Omega$ must cluster inside the disk. Therefore, $f$ is identically zero.

Proof of the lemma. The formula is obvious for $n=1$, so by induction, we assume it is valid for some $n$. Multiplying $f(z)^{n+1}=f(z) \cdot f(z)^{n}$, we have that

$$
\begin{gathered}
a_{n+1, i p+j}=a_{10} a_{n, i p+j}+\left[\sum_{k=0}^{(i-2) p+j} a_{1, p+k} a_{n,(i-1) p+j-k}\right]+a_{1, i p+j} a_{10}^{n}= \\
=\left[\sum_{m=1}^{i}\binom{n}{m} a_{10}^{n-m+1} \hat{a}_{m,(i-m) p+j}\right]+\left[\sum_{m=2}^{i}\binom{n}{m-1} a_{10}^{n-m+1} \hat{a}_{m,(i-m) p+j}\right]+a_{10}^{n} a_{1, i p+j}= \\
=\sum_{m=1}^{i}\left[\binom{n}{m}+\binom{n}{m-1}\right] a_{10}^{n-m+1} \hat{a}_{m,(i-m) p+j}=\sum_{m=1}^{i}\binom{n+1}{m} a_{10}^{(n+1)-m} \hat{a}_{m,(i-m) p+j} .
\end{gathered}
$$

Thus, the form of $f(z)^{n}$ follows for every $n$.
Fix $i$ and $j$, and let $n \geqq i$. Then $\left(n a_{10}^{n}\right)^{-1} a_{n, i p+j}$ is a polynomial in $n$ of degree at most $i-1$. Suppose that $a_{k, i_{p+j}}=0$ for some $k$ such that $1 \leqq k \leqq i-1$. It follows that the sum of the first $k$ terms of $\left(n a_{10}^{n}\right)^{-1} a_{n, i p+j}$ is equal to

$$
\sum_{m=1}^{k} \frac{1}{m!}\left[\frac{(n-1)!}{(n-m)!}-\frac{(k-1)!}{(k-m)!}\right] a_{10}^{-m} \hat{a}_{m,(i-m) p+j}
$$

which is divisible by $n-k$. Since each of the last $i-k$ terms contains a factor of $n-k$, we have that $n-k$ divides $\left(n a_{10}^{n}\right)^{-1} a_{n, i p+j}$. Therefore, either all of the. coefficients of ( $\left.n a_{10}^{n}\right)^{-1} a_{n, i p+j}(n \geqq i)$ are zero, or $a_{n, i p+j}=0$ for at most $i-1$ values. of $n \geqq 1$.

Finally, suppose that $a_{1 p} \neq 0$. Then the leading coefficient of $\left(n a_{10}^{n}\right)^{-1} a_{n, i p}$ ( $n \geqq i$ ) is $\left(i!a_{10}^{i}\right)^{-1} \hat{a}_{i 0}=\left(i!a_{10}^{i}\right)^{-1} a_{1 p}^{i} \neq 0$. Hence, $a_{n, i p}=0$ for at most $i-1$ values of $n \geqq 1$.

Proof of Theorem 3. Let $\alpha \neq 0$, and suppose that $\mathscr{M}$ is a nontrivial closed span of $b_{n}$ 's $(n \geqq 0)$ which reduces $C_{\varphi}$. Since $\mathscr{M}^{\perp}$ is of the same form, we may assume that $b_{0}$ is in $\mathscr{M}$. Let $n$ be the greatest integer such that $b_{m}$ belongs to $\mathscr{M}$ for every $m=0, \ldots, n$. Since $\mathscr{M}$ is invariant under $C_{\varphi}$, we have that $f=C_{\varphi} \cdot \sum_{0}^{n}(-\bar{\alpha})^{m} \times$
$\times\left(1-|\alpha|^{2}\right)^{-1 / 2} b_{m}$ is in $\mathscr{M}$ and $\left\langle f, b_{n+1}\right\rangle=0$. However, by induction,

$$
f^{\prime}(z)=-(n+1)(-\bar{\alpha})^{n+1} \cdot \varphi^{\prime}(z)[1-\varphi(z) \bar{\alpha}]^{-n-2}[\varphi(z)-\alpha]^{n}
$$

and

$$
f^{(n+1)}(\alpha)=-(n+1)!(-\bar{\alpha})^{n+1}\left(1-|\alpha|^{2}\right)^{-n-2} \varphi^{\prime}(\alpha)^{n+1} .
$$

Therefore,

$$
\left\langle f, b_{n+1}\right\rangle=(-\bar{\alpha})^{n+1}\left(1-|\alpha|^{2}\right)^{-1 / 2}\left[1-\varphi^{\prime}(\alpha)^{n+1}\right] \neq 0,
$$

a contradiction. Thus, $\mathscr{M}$ must be trivial.
Next, let $\alpha=0$ be a zero of $\varphi$ of order $r$, and let $\mathscr{M}$ be a nontrivial closed span of vectors $b_{n}=z^{n}(n \geqq 1)$ which reduces the restriction of $C_{\varphi}$ to $z H^{2}$. Let us write $\varphi(z)=z^{\prime} \Psi(z)$ for some $H^{\infty}$ function $\Psi$. If $\Psi$ is a constant function, then the proposed forms of $\varphi$ and $\mathscr{M}$ clearly follow with $p=0$. Henceforth, using the notation of the lemma, we assume that $\Psi(z)=\sum\left\langle\Psi, b_{n}\right\rangle b_{n}=a_{10}+a_{1 q} z^{q}+a_{1, q+1} z^{q+1}+\ldots$ where $a_{10}$ and $a_{1 q}$ are nonzero. Observe that if $\mathscr{M}$ contains $z^{n}$, and $a_{n, r q} \neq 0$, then $\mathscr{M}$ also contains $z^{n+q}$. Indeed, $\varphi(z)^{n}=z^{n n} \Psi(z)^{n}$ is in $\mathscr{M}$, and $\left\langle\varphi(z)^{n}, z^{r(n+q)}\right\rangle \neq 0$; therefore, by the given form of $\mathscr{M}, z^{(n+q)}$ belongs to $\mathscr{M}$. Since $z^{m}$ is orthogonal to $\mathscr{M}$ whenever $z^{m}$ is, we have that $\mathscr{M}$ contains $z^{n+q}$.

Let $z^{n}$ be in $\mathscr{M}$. By the lemma, there exists an integer $K$ such that $a_{k, r_{q}} \neq 0$ for every $k \geqq r^{K} n$. Now, $z^{\kappa_{n}}$ is in $\mathscr{M}$. And, if $z^{\kappa_{n}+m q}$ is in $\mathscr{M}$ for some $m \geqq 0$, then
 duction, $z^{K_{n+m}}$ is in $\mathscr{M}$ for every $m=0,1, \ldots$, and hence, in particular, $z^{r^{K(n+q)}}$ is in $\mathscr{M}$. Consequently, $\mathscr{M}$ contains $z^{n+q}$ whenever it contains $z^{n}$.

For integers $i$ and $j$, let $i \wedge j$ denote the greatest common divisor of $i$ and $j$. Let $q(1)=q$, and for $t=2,3, \ldots$, define $q(t)=[r \wedge q(t-1)]^{-1} q(t-1)$. Since $\{q(t)\}$ is a monotonically decreasing sequence of positive integers, there exists a least integer $T$ such that $q(T+1)=q(T)$, i.e., $r \wedge q(T)=1$. Note that $q(T)=r^{-T} \varrho q$ where $\varrho=\prod_{1}^{T}[r \wedge q(t)]^{-1} r$. If $z^{n}$ belongs to $\mathscr{M}$, it follows that $z^{n+q(T)}=z^{r^{-T}\left(r^{T_{n}} n q q\right)}$ belongs to $\mathscr{M}$. Similarly, the orthogonal complement of $\mathscr{M}$ in $z H^{2}$ is invariant under multiplication by $2^{q(T)}$. Therefore, there exists a subset $\Gamma_{1}$ of $\{1, \ldots, q(T)\}$ such that $\mathscr{M}$ is the closed span of vectors of the form $z^{i q(T)+j}\left(i \geqq 0 ; j \in \Gamma_{1}\right)$. Furthermore, if $j$ is in $\Gamma_{1}$, then $i q(T)<r j \leqq(i+1) q(T)$ for some integer $i$, and $r j-i q(T)$ is in $\Gamma_{1}$. Hence, $\Gamma_{1}$ is a union of $[r, q(T)]$-cycles.

If $\Psi=\Psi\left(z^{q(T)}\right)$, let $p=q(T)$ and $\Gamma=\Gamma_{1}$; otherwise, let $p(1)=q(T)$. Suppose that for some integer $s \geqq 1$, a positive integer $p(s)$, relatively prime to $r$, is defined such that $\mathscr{M}=\vee\left\{z^{i p(s)+j}: i \geqq 0, j \in \Gamma_{s}\right\}$ for some union $\Gamma_{s}$ of $[r, p(s)]$-cycles, and $\Psi \neq \Psi\left(z^{p(s)}\right)$. Let $I=\min \left\{i: a_{1, i p(s)+j} \neq 0\right.$ for some $j$ such that $\left.0<j<p(s)\right\}$, and let $J=\min \left\{j>0: a_{1, I p(s)+j} \neq 0\right\}$. By the lemma, $a_{n, I p(s)+J}=n a_{10}^{n-1} a_{1, I p(s)+J} \neq 0$. for every $n=1,2, \ldots$. As above, $z^{n+I p(s)+J}$, and hence $z^{n+J}$, belong to $\mathscr{M}$ whenever $z^{n}$ belongs to $\mathscr{M}$.

Let $z^{n}$ be in $\mathscr{M}$. Then $n=i p(s)+j$ where $j$ is in $\Gamma_{s}$ and $i \geqq 0$. Since $\Gamma_{s}$ is a union of cycles, there exists an element $j^{\prime}$ in $\Gamma_{s}$ and an integer $i^{\prime}$ such that $j=r j^{\prime}-i^{\prime} p(s)$. Thus, $n+J=\left(i-i^{\prime}\right) p(s)+\left(r j^{\prime}+J\right)$, so that $z^{n+J}$ is in $\mathscr{M}$. Similarly, $z H^{2} \ominus \mathscr{M}$ is invariant under multiplication by $z^{J}$.

Let $p(s+1)=p(s) \wedge J$. Then $p(s+1)$ is relatively prime to $r$, and there exist integers $u$ and $v$ such that $p(s+1)=u p(s)+v J$. It follows that $\mathscr{M}$ and the orthogonal complement of $\mathscr{M}$ in $z H^{2}$ are invariant under multiplication by $z^{p(s+1)}$, and hence, as above, there exists a union $\Gamma_{s+1}$ of $[r, p(s+1)]$-cycles such that $\mathscr{M}=\vee\left\{z^{i p(s+1)+j}\right.$ : $\left.i \geqq 0, j \in \Gamma_{s+1}\right\}$. Therefore, $p(s+1)(s=1,2, \ldots)$ may be defined recursively provided $\Psi \neq \Psi\left(z^{p(s)}\right)$ for every $s$. But this is impossible since $\{p(s)\}$ is a strictly decreasing sequence of positive integers. Consequently, there exists an integer $S$ such that $\Psi=\Psi\left(z^{p(S)}\right)$, and the forms of $\varphi$ and $\mathscr{M}$ follow by setting $p=p(S)$ and $\Gamma=\Gamma_{S}$. Note that $p \neq 1$ since $\mathscr{M}$ is nontrivial.

Conversely, suppose that $\varphi(z)=z^{r} \Psi\left(z^{p}\right)$ where $r \wedge p=1$ if $p \neq 0$, and that $\mathscr{M}=\vee\left\{z^{i p+j}: i \geqq 0, j \in \Gamma\right\}$ for some union $\Gamma$ of $(r, p)$-cycles. If $p=0$, then clearly. $\mathscr{M}$ is invariant under $C_{\varphi}$; so we assume that $p>1$. If $z^{n}$ belongs to $\mathscr{M}$, then so does $z^{r q+m p}$ for every $m \geqq 0$. Indeed $n=i p+j$ where $j$ is in $\Gamma$ and $i \geqq 0$ and there exists an integer $i^{\prime}$ such that $i^{\prime} p<r j \leqq\left(i^{\prime}+1\right) p$. Hence, $r j=i^{\prime} p+j^{\prime}$, where $j^{\prime}$ is in $\Gamma$ by the definition of $(r, p)$-cycle. Therefore, $z^{r n+m p}=z^{\left(r i+i^{\prime}+m\right) p} z^{j^{\prime}}$ is in $\mathscr{M}$, and thus, so is $\varphi(z)^{n}=z^{r n} \Psi\left(z^{p}\right)^{n}$. It follows that $\mathscr{M}$ is invariant under $C_{\varphi}$.

Finally, $\mathscr{A}^{\perp}$ is invariant under $C_{\varphi}$ since it is the closed span of vectors of the form $z^{i p+j}\left(i \geqq 0 ; j \in \Gamma^{\prime}\right)$, where $\Gamma^{\prime}$ is the complement in $\{1, \ldots, p\}(\{1,2, \ldots\}$, if $p=0$ ) of $\Gamma$ and is hence the union of $(r, p)$-cycles.

Proof of Theorem 2. Since $C_{\varphi}^{*^{N}}=C_{\varphi_{N}}^{*}$ is compact with nonzero eigenvalues $\overline{\varphi^{\prime}(\alpha)}{ }^{m N}(m=0,1, \ldots)$, it follows from [4, Theorem 4.1] that $\overline{\varphi^{\prime}(\alpha)^{m}}$ is an eigenvalue of $C_{\varphi}^{*}$ of multiplicity one for every $m$. Thus, by the matrix of $C_{\varphi}^{*}$ with respect to $\left\{b_{n}\right\}$, we have that $\bigvee_{0}^{n} b_{m}=\operatorname{ker} \prod_{0}^{n}\left[C_{\varphi}^{*}-\bar{\varphi}^{\prime}(\alpha)^{m}\right]$ for every $n=0,1, \ldots$. Therefore, by induction, either $b_{n}$ belongs to $\mathscr{M}$ or is orthogonal to $\mathscr{M}$ for each $n$, and hence the form of $\mathscr{M}$ is given by Theorem 3.

Proof of the proposition. Using induction on $n$ with $m$ fixed, the case $n=0$ is obvious, so we assume that the inequality holds for some $n$. Since $\varphi(\alpha)=\alpha$ and $\varphi^{(i)}(\alpha)=0(i=1, \ldots, r-1)$, we have that $\varphi_{n}^{(i)}(\alpha)=0$ for every $i=1, \ldots, r^{n}-1$. Hence, $C_{\varphi}^{n+1} b_{m}=C_{\varphi} f$ where $f=b_{m}\left(\alpha, \varphi_{n}\right)=[(z-\alpha) /(1-z \bar{\alpha})]^{m r^{n}} g$ for some $H^{\infty}$ function $g$. Therefore, $\left\|C_{\varphi}^{n+1} b_{m}\right\|_{\infty}=\|(\varphi-\alpha) /(1-\varphi \bar{\alpha})\|_{\infty}^{m r^{n}}\|g(\varphi)\|_{\infty} \quad$ where $\|g(\varphi)\|_{\infty} \leqq$ $\leqq\|g\|_{\infty}=\|f\|_{\infty} \leqq\|(\varphi-\alpha) /(1-\varphi \bar{\alpha})\|_{\infty}^{m\left(r^{n}-1\right) /(r-1)}$ by the induction hypothesis. The case $n+1$ now follows by combining the above inequalities.

Proof of Theorem 4. Since $\|\varphi\|_{\infty}<1, C_{\varphi}$ is compact by [11, Theorem 5.2].

Therefore, by [4, Theorem 4.1], the kernel of $1-C_{\varphi}^{*}$ is one-dimensional, and since it is invariant under $X^{*}$, we have that $\lambda_{0 j}=0(j \geqq 1)$.

Suppose that $\varphi^{(m)}(\alpha)=0(m=1, \ldots, r-1)$ and $\varphi^{(r)}(\alpha) \neq 0$. By direct computations, there exist constants $\mu_{i^{\prime}}=\mu_{i^{\prime}}(n)$ such that for every $i \geqq 0$,

$$
b_{i}=\bar{\mu}^{-i\left(r^{n}-1\right) /(r-1)} C_{\varphi}^{*^{n}} b_{i r^{n}}+\sum_{i^{\prime}<i} \mu_{i^{\prime}} b_{i^{\prime}}
$$

where $\mu=\left(1-|\alpha|^{2}\right)^{r-1} \varphi^{(r)}(\alpha)(r!)^{-1}$. Moreover, since $\|\varphi\|_{\infty}<1$, it follows that $\|(\varphi-\alpha) /(1-\varphi \bar{\alpha})\|_{\infty}<1$, and hence there exists an integer $M \geqq 1$ such that $\|(\varphi-\alpha) /(1-\varphi \bar{\alpha})\|_{\infty}^{M}<|\mu|$. Thus,

$$
\lambda_{i j}=\left\langle X b_{j}, b_{i}\right\rangle_{2}=\mu^{-i\left(r^{n}-1\right) /(r-1)}\left\langle X C_{\varphi}^{n} b_{j}, b_{i r n}\right\rangle_{2}+\sum_{i^{\prime}<i} \bar{\mu}_{i^{\prime}} \lambda_{i^{\prime} j}
$$

and consequently by the proposition, for $j \geqq M i$ we have that

$$
\left|\lambda_{i j}-\sum_{i^{\prime}<i} \bar{\mu}_{i^{\prime}} \lambda_{i^{\prime} j}\right| \leqq\|X\|_{2}\left(\left\|\frac{\varphi-\alpha}{1-\varphi \bar{\alpha}}\right\|_{\infty}^{M}|\mu|^{-1}\right)^{i\left(r^{n}-1\right) /(r-1)} .
$$

Therefore, the theorem follows by induction on $i \geqq 1$, and the separate case $i=0$, since the right hand side converges to zero as $n$ tends to infinity.

## References

[1] L. de Branges and J. Rovnyak, Square Summable Power Series, Holt, Rinehart, and Winston (New York, 1966).
[2] A. Brown, On a class of operators, Proc. Amer. Math. Soc., 4 (1953), 723-728.
[3] J. G. Caughran and H. J. Schwartz, Spectra of compact composition operators, Proc. Amer. Math. Soc., 51 (1975), 127-130.
[4] C. C. Cowen, Composition operators on $H^{\text {², }}$ J. Operator Theory, 9 (1983), 77-106.
[5] J. A. Deddens, Analytic Toeplitz and composition operators, Canad. J. Math., 24 (1972), 859-865.
[6] A. Denjoy, Sur l'itération des fonctions analytiques, C. R. Acad. Sci. Paris Sér. A., 182 (1926), 255-257.
[7] P. L. Duren, Theory of $H^{p}$ Spaces, Academic Press (New York, 1970).
[8] E. A. Nordgren, Composition operators, Canad. J. Math., 20 (1968), 442-449.
[9] E. A. Nordgren, Composition operators on Hilbert spaces, in: Hilbert Space Operators, Lecture Notes in Math., 693, Springer-Verlag (Berlin, 1978), pp. 37-63.
[10] J. V. Ryff, Subordinate $H^{\text {p }}$ functions, Duke Math. J., 33 (1966), 347-354.
[11] H. J. Schwartz, Composition Operators on $H^{p}$, Thesis, (University of Toledo, 1969).
[12] J. H. Shapiro and P. D. Taylor, Compact, nuclear, and Hilbert-Schmidt composition operators on $H^{2}$, Indiana Univ. Math. J., 23 (1973), 471-496.
[13] J. Wolff, Sur l'itération des fonctions, C. R. Acad. Sci. Paris Sér. A., 182 (1926), 42-43, 200-201.

SUNY COLLEGE AT BUFFALO
BUFFALO, NEW YORK 14222
U.S. A.

