NOTE ON THE DESCENDENT THEOREM OF SLEPIAN, MOORE, AND PRANGE

STEPHEN S. SHATZ

In this note we prove the Descendent Theorem **(2)** of Slepian, Moore, and Prange in an abstract form. Our proof shows that the theorem is valid in much more general settings than that of vector spaces over $\mathbf{Z}/2\mathbf{Z}$. Applications of the descendent theorem to coding theory may be found in **(2)**, and a study of Prange's method of proof is carried out by Dade in **(1)**.

1. Descendents and coset leaders. Let A denote an abelian group. A function w on A to the non-negative integers will be called a *weight function* provided that

(1) $w(a) = 0$ if and only if $a = 0$,

(2) $w(a + a') \leqslant w(a) + w(a')$.

Using the notion of weight function, we define the *descendent set* of an element $a \in A$ by

$$d(a) = \{b \in A | w(a - b) = w(a) - w(b) = 1\}.$$

Now assume that the given abelian group A is equipped with a weight function w and that the pair $\langle A, w\rangle$ satisfies the following axiom:

AXIOM 1 (*Descendence Axiom*). *For any* $a \neq 0$, $d(a) \neq \emptyset$.

It is trivial that $d(0) = \emptyset$, and that the set, E, of elements of A of weight one is non-empty under Axiom 1. Moreover, simple arguments establish the following facts

(a) *Under Axiom* 1, $d(a) = \{t \in A \mid w(t) < w(a)$ and $a - t \in E\}$.

(b) *For any* $r \geqslant 1$, *let*

$$d^r(a) = \{t \in A | (\exists b \in d^{r-1}(a))(t \in d(b))\},$$

and let $d^0(a) = \{a\}$. *Then if* $t \in d^r(a)$, *we have* $w(t) + r = w(a)$. *Furthermore* $w(a) = r$ *if and only if* $d^r(a)$ *is non-empty and* $d^{r+1}(a)$ *is empty.*

(c) $a \in E \Leftrightarrow d(a) = \{0\}$.

(d) $w(a) \geqslant r \Leftrightarrow d^r(a) \neq \emptyset$.

(e) *E contains a set of generators for A. More exactly, if $a \in A$ is given and $w(a) = n$, then a is a sum of n elements of E.*

(f) *If* $r \neq s$, *then* $d^r(a) \cap d^s(a) = \emptyset$.

Received April 2, 1965. Work partially supported by M.I.T. Lincoln Laboratory.

Let A' be a subgroup of A and let

$$\bar{w}(\bar{a}) = \min \{w(b) | \ b \in \bar{a}\}.$$

Here $\bar{a}$ is the coset of the element a modulo A'. The usual proof shows that $\bar{w}$ is a weight function for the abelian group A/A'.

DEFINITION **(3).** *An element a of a coset Q which has minimal weight in Q is called a coset leader of Q.*

PROPOSITION 1. *Let $\bar{a}$ be a coset of A' in A, and let α be a coset leader in $\bar{a}$. Then every element of $d(\alpha)$ is a coset leader of the coset to which it belongs.*

Proof. If $\alpha = 0$, the proposition is vacuously true, so we may assume $\alpha \neq 0$. Let $t \in d(\alpha)$; then

$$w(\alpha - t) = w(\alpha) - w(t) = 1.$$

If $e = \alpha - t$ and ξ is any element of $\bar{t}$, then $\xi = t + a'$ for some $a' \in A'$ and

$$\alpha + a' = e + t + a' = e + \xi.$$

Therefore

$$w(\alpha) \leqslant w(a' + \alpha) \leqslant w(e) + w(\xi) = 1 + w(\xi).$$

Hence

$$w(\xi) \geqslant w(\alpha) - 1 = w(t),$$

and the proposition follows.

2. Proof of the descendent theorem. Let $e \in E$; we say that $a \in A$ *has a zero in the* eth *place* if and only if

$$w(a + e) = w(a) + 1.$$

LEMMA. *If $\bar{w}(\overline{a + e}) > \bar{w}(\bar{a})$, then every coset leader of $\bar{a}$ has a zero in the* eth *place. Furthermore, $\alpha + e$ is a coset leader of the coset to which it belongs whenever α is a coset leader of $\bar{a}$.*

Proof. Clearly, $\bar{w}(\overline{a + e}) \leqslant w(\alpha) + 1$. Hence

$$w(\alpha) = \bar{w}(\bar{a}) < \bar{w}(\overline{a + e}) \leqslant w(\alpha) + 1$$

implies $\bar{w}(\overline{a + e}) = w(\alpha) + 1$. On the other hand,

$$(*) \qquad \bar{w}(\overline{a + e}) = \bar{w}(\overline{\alpha + e}) = w(t) \leqslant w(\alpha + e),$$

where t is any coset leader of $\overline{\alpha + e}$. Thus

$$(**) \qquad w(\alpha) + 1 = \bar{w}(\overline{a + e}) \leqslant w(\alpha + e) \leqslant w(\alpha) + 1,$$

which proves

$$w(\alpha + e) = w(\alpha) + 1;$$

that is, α has a zero in the eth place. Now (*) and (**) show that

$$w(t) = w(\alpha + e) = w(\alpha) + 1 = \bar{w}(\overline{\alpha + e})$$

completing the proof.

We require a second and last axiom.

AXIOM 2. (*Ordering Axiom*). *For any subgroup A' of A, there exists a linear ordering $\prec$ on the coset leaders of each coset of A' in A which satisfies*

(3) *Under $\prec$, there is a maximal coset leader in each coset.*

(4) (*Coherence Property*). *If α_1, α_2 are leaders of the coset $\bar{a}$ and if $\alpha_1 \succ \alpha_2$, then $\alpha_1 - e \succ \alpha_2 - e$ for every $e \in E$ such that $\alpha_i - e \in d(\alpha_i)$ $(i = 1, 2)$.*

DEFINITION. *A subset T of A has the descendent property if and only if $d(T) \subseteq T$.*

We call a complete set of coset representatives of a subgroup A' in A a *transversal* for A' in A. If a transversal consists entirely of coset leaders, then it is called a *coset leader transversal.*

THEOREM (*Descendent Theorem*). *Let A be an abelian group together with a weight function w satisfying Axioms* 1 *and* 2. *If A' is a subgroup of A, then there exists a coset leader transversal for A' in A having the descendent property.*

Proof. Let T be the set of all maximal coset leaders in the ordering $\succ$. The set T is clearly a coset leader transversal, and we shall now show that T has the descendent property. If $v \in T$, then every descendent of v has the form $v - e$ for some $e \in E$, and we have

$$w(v - e) = w(v) - 1.$$

Let u be a coset leader of $\overline{v - e}$ such that $u \succ v - e$. (By Proposition 1, $v - e$ is a coset leader of $\overline{v - e}$.) We have to show that $u = v - e$. Now

$$w(u) = w(v - e) = w(v) - 1,$$

hence $w(v) > w(u)$. But $\bar{u} = \overline{v - e}$, hence $\overline{u + e} = \bar{v}$. Therefore

$$w(u + e) \geqslant w(v),$$

so that $w(u + e) > w(u)$. However,

$$w(\overline{u + e}) = w(v), \qquad w(u) = \bar{w}(\bar{u})$$

so that the lemma applies. It follows that $u + e$ is a coset leader of the coset to which it belongs, namely a coset leader of $\bar{v}$. Because $v \in T$, we obtain

$$u + e \prec v.$$

On the other hand, we know that $w(v - e) < w(v)$ and $w(u + e) > w(u)$. Since $u = (u + e) - e$, fact (a) shows that

$$u \in d(u + e).$$

https://doi.org/10.4153/CJM-1966-064-5 Published online by Cambridge University Press

The coherence property of Axiom 2 together with $u + e \prec v$ shows that

$$u \prec v - e.$$

This inequality, together with the fact that $u \succ v - e$, completes the proof.

Remarks. (1) If A is a vector space over $\mathbf{Z}/2\mathbf{Z}$ equipped with the Hamming weight, we deduce the usual form of the descendent theorem.

(2) If A is a finitely generated abelian group, say of rank r, and if A possesses s finite cyclic summands, then there exists a weight function on A. To obtain this, represent each cyclic summand by $\mathbf{Z}$ or $\{0, 1, \ldots, n-1\}$ (in the case of $\mathbf{Z}/n\mathbf{Z}$) and define a weight on each summand via the absolute value. The sum of these weights is a weight on A. By ordering A lexicographically with respect to the above basis, we arrive at an ordering $\prec$ that satisfies Axiom 2. (Axiom 1 is trivially satisfied by the above-defined weight.) This construction yields the Descendent Theorem for an arbitrary finitely generated abelian group (I am indebted to E. Weiss for suggesting the preceding proof).

References

1. E. C. Dade, *Coset leaders*, Group Report 55G-0027; M.I.T. Lincoln Laboratory (Aug. 1960).

2. E. Prange, *Step by step decoding for group codes*, Communication Sciences Laboratory, Electronics Research Directorate, U.S.A.F. Research Division, Bedford, Mass.

3. D. Slepian, *A class of binary signaling alphabets*, Bell System Tech. J., *35* (1956), 203–234.

University of Pennsylvania,
Philadelphia, Pa.