APPENDIX B

ON THE BASES OF A CYCLIC UNIQUE REPRESENTATION GROUP

B-1. Unique representation groups.

Consider the residue classes modulo $2^n - 1$ denoted by $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{2^{n-2}}$. Any positive integer $m \leq 2^n - 2$ can be uniquely represented as $2^t_1 + 2^t_2 + \ldots + 2^t_r$, where the $t$'s are all distinct non-negative integers $\leq n - 1$. Hence the residue class

$\overline{m} = 2^t_1 + 2^t_2 + \ldots + 2^t_r$.

Further, $\overline{0} = 2^{n-1} = 1 + \overline{2} + \overline{2^2} + \ldots + \overline{2^{n-1}}$.

Thus if $S$ is the set of the residue classes modulo $2^n - 1$ and $B$ the set

$\{ \overline{2^j} | j = 1, 2, \ldots, n-1 \}$,

then every member of $S$ arises as a simple linear combination on $B$. The total number of simple linear combinations on $B$ is clearly $2^n - 1$, which is the number of members of $S$. Hence every residue class modulo $2^n - 1$ is representable uniquely as a simple linear combination on $B$. The set $S$, we know, is a group with respect to addition modulo $2^n - 1$, '+'. Thus $B$ is
a subset of the group \((S,+)\), not containing the identity element 0, such that every member of S is uniquely representable as a simple linear combination on B. Hence, by definition, S is a u.r. set, with B as its base. Here we have an instance of a u.r. set which is a group in itself.

\((\text{B-1.1})\). **Definition.** Let G be a u.r. set with respect to the operation \('\ast'\). If \((G,\ast)\) is a group, then we say that \((G,\ast)\) is a unique representation group or simply a u.r. group.

\((\text{B-1.2})\) **Theorem.** The identity of the u.r. group \((G,\ast)\) with \(B = \{x_1, x_2, \ldots, x_n\}\) as its base is \(x_1 + x_2 + \ldots + x_n\).

**Proof.** Since \(0 \in G\), 0 is a simple linear combination on B; and if \(x_1 + x_2 + \ldots + x_n \neq 0\), then 0 must be a simple linear combination on some proper subset of B, which is impossible by Lemma 3.3.4. Hence \(x_1 + x_2 + \ldots + x_n = 0\) and the theorem is proved.

\((\text{B-1.3})\) **Theorem.** Let \((G,\ast)\) be a u.r. group of order \(2^n - 1\) with B as a base and \((G',\oplus)\), any group of the same order. If \(f : G \to G'\) is an isomorphism of groups, then \(G'\) is a u.r. group with \(f(B)\) as a base.

**Proof.** Let \(B = \{a_1, \ldots, a_n\}\), so that

\[f(B) = \{f(a_1), \ldots, f(a_n)\}\.]
If $l'$ is any element of $G'$, then there is an element $1$ of $G$ such that $f(l) = l'$. Now $l$ is a simple linear combination on $B$ and is of the form $a_{i_1} + \ldots + a_{i_r}$. Since $f$ is an isomorphism (of groups), $f(l) = l'$ implies,
\[ l' = f(a_{i_1}) \oplus \ldots \oplus f(a_{i_r}); \]
that is, $l'$ is a simple linear combination on $f(B)$. Now suppose that
\[(B-1.4) \quad f(a_{i_1}) \oplus \ldots \oplus f(a_{i_r}) = f(a_{j_1}) \oplus \ldots \oplus f(a_{j_s}).\]
Then \[ f(a_{i_1} + \ldots + a_{i_r}) = f(a_{j_1} + \ldots + a_{j_s}); \]
and since $f$ is one-to-one,
\[ a_{i_1} + \ldots + a_{i_r} = a_{j_1} + \ldots + a_{j_s}. \]
Therefore, every $a_i$ is an $a_j$ and conversely every $a_j$ is an $a_i$.

It then follows from (B-1.4) that every element of $G'$ is expressible uniquely as a simple linear combination on $f(B)$. Hence $G'$ is a u.r. group with $f(B)$ as a base.

(B-1.5) **Theorem.** Every cyclic group of order $2^n - 1$ is a u.r. group.

**Proof.** We know that two cyclic groups of the same order are isomorphic. Also, as we have seen, the set $S$ of the residue classes modulo $2^n - 1$ is a u.r. group of order $2^n - 1$ under addition modulo $2^n - 1$; and the group $(S,+)$ is clearly cyclic.
Therefore, any cyclic group of order \(2^n - 1\) is isomorphic with the u.r. group \((S,+)_n\) of order \(2^n - 1\). Hence, by Theorem B-1.3, any cyclic group of order \(2^n - 1\) is a u.r. group.

We do not know if every u.r. group is cyclic; we have no counter-examples to give. But a necessary and sufficient condition for a u.r. group to be cyclic is given by

(B-1.6) **Theorem.** A u.r. group is cyclic if and only if every element of any base of it is an "integral multiple" of some element of it.

**Note.** If \(n\) is a positive integer and \(a\) an element of the group, then we say \(na = a + a + \ldots + a\) \((n a's)\) is an integral multiple of \(a\). We take the binary composition of \(G\) to be "addition".

**Proof.** If the u.r. group is cyclic, then every element of the group and hence every element of any of its base is an integral multiple of some element (generator) of the group. On the other hand, if every element of any of its base \(B\) is an integral multiple of some element \(a\) of the group, then clearly every simple linear combination on \(B\), that is, every element of the group, must be an integral multiple of \(a\). This proves the theorem.
Bases of cyclic unique representation groups.

The set of residue classes modulo 7 is a u.r. group with two bases \( \{1, 2, 4\} \) and \( \{3, 5, 6\} \). (See (iii) of Examples 3,3,3.) Thus a cyclic u.r. group of order \( 2^n - 1 \), \( n \geq 3 \) can have more than one base. In this section we shall exhibit \( \phi(2^n - 1)/n \) disjoint bases of a cyclic u.r. group of order \( 2^n - 1 \), though we are not in a position to prove that the u.r. group has no more bases.

We reserve \( k \) to denote \( 2^n - 1 \). The cyclic group of residue classes modulo \( k \) is denoted by \( \mathbb{Z}_k \). We know that \( \mathbb{Z}_k \) has \( \phi(k) \) generators (\( \phi \), the Euler function), which form a group under multiplication (\( \cdot \)) modulo \( k \). We denote this group by \( \mathcal{S} \). The order of \( \mathcal{S} \) is \( \phi(k) \) and \( \bar{g} \in \mathcal{S} \) if and only if \( (g,k) = 1 \).

(B-2.1) Lemma. The base
\[
B_1 = \left\{ 2^r \mid r = 0, 1, 2, \ldots, n-1 \right\}
\]
of the u.r. group \( \mathbb{Z}_k \) is a subgroup of \( \mathcal{S} \).

Proof. For every non-negative integer \( r \), \( (2^r, 2^n - 1) = 1 \), so that every member of \( B_1 \) is a generator of \( \mathbb{Z}_k \), that is \( B_1 \subset \mathcal{S} \). To prove that \( B_1 \) is a subgroup of \( \mathcal{S} \) we need only to show that \( B_1 \) is closed under multiplication modulo \( k \).

If \( \bar{a}, \bar{b} \in B_1 \), then \( \bar{a} \cdot \bar{b} = \bar{m} \), where \( m \) is some integer
with $0 \leq m \leq 2n - 2$. If $0 \leq m \leq n - 1$, $\bar{a}_5 \in B_1$. If $m > n$, then $m = n + j$, $0 \leq j \leq n - 2$ and

$$2^m = (2^n - 1)2^j + 2^j = k.2^j + 2^j,$$

that is,

$$2^m \equiv 2^j \pmod{k}.$$

So $\bar{a}_5 = 2^j \in B_1$ and $B_1$ is a subgroup of $S$.

The order of $B_1$ is $n$ and the order of $S$ is $\varphi(k)$, so that $n$ divides $\varphi(k) = \varphi(2^n - 1)$.

Let $B = \{\bar{a}_1, \ldots, \bar{a}_n\}$ be a base for $Z_k$. If $\bar{t} \in Z_k$, we write $\bar{t}B$ to denote the set $\{\bar{t}\bar{a}_1, \ldots, \bar{t}\bar{a}_n\}$.

(B-2.2) Lemma. If $B$ be a base of $Z_k$ and $\bar{t} \in S$ then $\bar{t}B$ also is a base of $Z_k$.

Proof. Let $B = \{\bar{a}_1, \ldots, \bar{a}_n\}$, so that

$$\bar{t}B = \{\bar{t}\bar{a}_1, \ldots, \bar{t}\bar{a}_n\}, \bar{t} \in S.$$

Any simple linear combination on $\bar{t}B$ is of the form

$$\bar{t}a_{i_1} + \bar{t}a_{i_2} + \ldots + \bar{t}a_{i_r},$$

where $\bar{a}_{i_1} + \bar{a}_{i_2} + \ldots + \bar{a}_{i_r}$ is a simple linear combination on $B$.

Let $\bar{t}a_{i_1} + \ldots + \bar{t}a_{i_r}$ and $\bar{t}a_{j_1} + \ldots + \bar{t}a_{j_s}$ be any two simple linear combinations on $\bar{t}B$. If these are equal, we must have

$$t(a_{i_1} + \ldots + a_{i_r}) \equiv t(a_{j_1} + \ldots + a_{j_s}) \pmod{k}.$$

This readily implies

$$a_{i_1} + \ldots + a_{i_r} \equiv a_{j_1} + \ldots + a_{j_s} \pmod{k}.$$
since \( \bar{e} \in \mathcal{S} \), that is, \((t, k) = 1\). Hence

\[
\bar{a}_{i_1} + \ldots + \bar{a}_{i_r} = \bar{a}_{j_1} + \ldots + \bar{a}_{j_s}.
\]

Since either side of this equation is a simple linear combination on \( B \), every \( a_i \) must be an \( a_j \) and vice versa, and \( r = s \).

Therefore every \( \bar{e}a_i \) is a \( \bar{e}a_j \) and conversely; and this shows that the \( k \) simple linear combinations on \( \bar{e}B \) are unique. Hence \( \bar{e}B \) is a base for \( Z_k \) proving the lemma.

By Lemma B-2.1, the base \( B_1 \) is a subgroup of (the abelian group) \( S \); therefore, from Lemma B-2.2 it follows that its (left) cosets \( tB_1 \) in \( S \) are bases of \( Z_k \). In fact, these cosets form the factor group of \( S \) modulo \( B_1 \), \( S/B_1 \), whose order is \( \phi(k)/n \). Thus we have proved

\[
\text{(B-2.3) Theorem. The cyclic group } Z_k \text{ has } \phi(k)/n \text{ mutually disjoint bases, each of which is constituted by its generators.}
\]

The elusive question has been whether these are the only bases of \( Z_k \).

If \( (G, \odot) \) is any cyclic group of order \( k \), then \( Z_k \) and \( G \) are isomorphic and \( G \) is a u.r. group. Let \( f : Z_k \to G \) be an isomorphism (of groups), and \( B \) any base of \( Z_k \). Then, by Theorem B-1.3, \( f(B) \) is a base of \( G \). Since \( f \) is one-to-one,
there must be at least as many bases of $G$ as there are of $\mathbb{Z}_k$; and the converse also is true. So there are as many bases of $G$ as there are of $\mathbb{Z}_k$.

We have thus generalised Theorem B-2.3 into

(B-2.4) **Theorem.** Every cyclic group of order $2^n - 1$ has a set of $\varphi(2^n - 1)/n$ mutually disjoint bases, each of which is constituted by its generators.