May 26, 2014

Abstract

1

The subset U_k mentioned in last lemma, has more specific properties. In the following lemma, we use U_k to build a matrix.

Lemma 1. *For each $k \geq 1$, suppose U_k is the subset of S_k mentioned in the last lemma, and construct a matrix UG_k in the following way:*

- *the element $b_i^{2^k}$ of the set U_k is the ith row of GH_k.*

Then, this matrix has the following properties:

- *The order of GH_k is k to 2^k;*
- *All 2^k columns of GH_k are distinct;*

Proof. For each k, consider the matrix UG_k. Since U_k has k elements which are the rows of UG_k, and since each element of U_k has 2^k components, the order of GH_k is k to 2^k.
Now, suppose UC_k is the set of culomns of UG_k; i.e.,

$$UC_k = \{u_i^{2^k}; u_i^{2^k} \; is \; the \; ith \; column \; of \; UG_k\}$$

We want to prove $u_r^{2^k} = [(u_r^{2^k})_j]$ and $u_s^{2^k} = [(u_s^{2^k})_j]$ are distinct if $r \neq s$, where $1 \leq r \neq s \leq 2^k$, and $1 \leq j \leq k$.
Toward a contradiction, suppose $r \neq s$ but $u_r^{2^k} = u_s^{2^k}$. Since $u_r^{2^k} = u_s^{2^k}$, then $(u_r^{2^k})_j = (u_s^{2^k})_j$ for each $1 \leq j \leq k$.
We have $(u_r^{2^k})_k = (u_s^{2^k})_k$ implies $1 \leq r \,,\; s \leq 2^{k-1}$ or $2^{k-1}+1 \leq r \,,\; s \leq 2^k$. With out loss of generality, suppose $1 \leq r \,,\; s \leq 2^{k-1}$.
Next, we have $(u_r^{2^k})_{k-1} = (u_s^{2^k})_{k-1}$ implies $1 \leq r \,,\; s \leq 2^{k-2}$ or $2^{k-2}+1 \leq r \,,\; s \leq 2^{k-1}$. With out loss of generality, suppose $1 \leq r \,,\; s \leq 2^{k-2}$. If we continue in this way, we have last step as follow:

- Since $(u_r^{2^k})_1 = (u_s^{2^k})_1$, we have $1 \leq r \,,\; s \leq 2^{k-k} = 1$.

This is a contradiction because we suppose $r \neq s$; so, $u_r^{2^k} \neq u_s^{2^k}$. Hence, all columns of GH_k are distinct. □

Now, consider the following lemma which is about the set UC_k mentioned in the last lemma.

Lemma 2. *For each $k \geq 1$, the set UC_k, the set of culomns of UG_k, is an elementary abelian group of order 2^k under componentwise multiplication.*

Proof. For each $k \geq 1$, from lemma 10, the rows of H_{2^k} can be permuted so that the i^{th} row of H'_{2^k} is $b_i^{2^k}$. Then the matrix UG_k is a submatrix of H'_k; i.e., the matrix UG_k form the first k rows of H'_{2^k}. By remark 7, the columns of H_{2^k} form an elementary abelian group under componentwise multiplication. Therefore, the columns of H'_{2^k} also form an elementary abelian group under componentwise multiplication. This implies that UC_k is an elementary group under componentwise multiplication. By previous lemma, the order of this group is 2^k. $\square$

In the following lemma, we prove the existance of an isomorphism between S_k and UC_k.

Lemma 3. *For each $k \geq 1$, there is an isomorphism Φ from S_k to UC_k defined as follow.*

- $\Phi(a_i^{2^k}) = u_i^{2^k}$, *where* $1 \leq i \leq 2^k$.

Proof. For each $k \geq 1$, since the matrix UG_k forms the first k rows of H'_{2^k}, we can map each column of UG_k to each column of H'_{2^k}, in the natrual way. Hence, if

$$S'_k = \{a_i'^{2^k} : a_i'^{2^k} \; is\; the\; ith\; row\; of\; H'_{2^k}\;,\; for\; each\; 1 \leq i \leq 2^k\},$$

then let σ from S'_k to UC_k be the following mapping:

$$\sigma(a_i'^{2^k}) = u_i'^{2^k},\; for\; each\; 1 \leq i \leq 2^k.$$

By considering the componentwise multiplicetion, this is an isomorphism. To complete the proof, we need the isomorphism σ from S_k to S'_k defined as follow:

$$\phi(a_i^{2^k}) = a_i'^{2^k},\; for\; each\; 1 \leq i \leq 2^k.$$

Indeed, σ is an isomorphism. Since H_{2^k} is symmetric, the set S_K can be consider as the set of columns of H_{2^k} as well, and σ can be considered as a permutation of the components of each $a_i^{2^k}$. Since the multiplication is componentwise, σ prevers the operations, and it is an isomorphism. $\square$