International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 6 Issue 8, December 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Full-Rank Factoring of Elementary 2-Groups with Equal Size Factors

Pravin Kumar Singh
(Research Scholar)
P.G. Department of Mathematics L.N.M.U. Darbhanga (Bihar)

Abstract

In order to answer a question motivated by constructing substitution boxes in block ciphers we will exhibit an infinite family of full-rank factorizations of elementary 2-groups into two factors having equal sizes.

Keywords

Factorization of Finite Abelian Groups, Elementary 2-Groups,

Full-Rank Subsets, Full-Rank Factorizations

1. Introduction

We will use multiplicative notation in connection with abelian groups. Let G be a finite abelian group. The product A1 ⋯An of the subsets

$A_1,\dots,A_n$ of G is defined to be the set of the elements

$a_1 \cdots a_n$, $a_1 \in A_1,\dots,a_n \in A_n$.

The product A1 ⋯An is called a direct product if $a_1 \cdots a_n = a'_1 \cdots a'_n, \quad a_1, a'_1 \in A_1, \dots, a_n, a'_n \in A_n$

imply that $a_1 = a'_1, \dots, a_n = a'_n$. Let B be a subset of G. If the product $A_1 \cdots A_n$ is direct and it is equal to B, then we say that B is factored into the subsets $A_1,\dots,A_n$ or equivalently we say that the equation $B = A_1 \cdots A_n$ is a factorization of B. In

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 6 Issue 8, December 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

algebra books the most commonly occurring situation is when an entire abelian group is factored into a direct product of its subgroups.

The span of a subset A of G is the smallest subgroup of G that contains A. The span of A is denoted by ⟨A⟩. A subset A of G is called normalized if the identity element e of G is an element of A. If A is a normalized subset of G for which ⟨A⟩ = G, then we say that A is a full-rank subset of G. A factorization G = A1 ···An is called a full-rank factorization if each factor is a full-rank subset of G.

Full-rank factorizations of finite abelian groups are intimately connected with the theory of error correcting, variable length codes andcryptography. For further details see for instance [1–4], respectively. Let p be a prime. The direct product of n isomorphic copies of a cyclic group of order p is an abelian group and it is called an elementary pgroup of rank n. In a letter Professor Claude Carlet asked me if there were full-rank factorizations of elementary 2-groups into two factors of equal sizes [5]. He could use such a factorization for constructing substitution boxes, or S-boxes, in block ciphers.

The next few words try to explain how the $F : F_2^{2n} \to F_2^{2n}$ by $F((a_1, a_2)) =$ S-box is built from a full-rank factorization. For more detail the reader should consult with [6]. Let G = A_1A_2 be a full-rank factorization of the elementary 2-group G of rank 2n such that $|A_1| = |A_2| = 2^n$. Let F_2 be the finite Galois field with two elements and let $\pi_1 : F_2^n \to A_1$ and $\pi_2 : F_2^n \to A_2$

be bijectivemaps. Using π_1 and π_2 we define $\pi_1(a_1)+\pi_2(a_2)$. The fact that the factorization G = A_1A_2 is a full-rank factorization is a necessary condition that the S-box has a non-zero linearity. The non-linearity of the S-box is the desired property with cryptographic significance. (Problem 3 in Section 3 at the end of the paper is related to this issue.) The group theoretic argument we use to prove Theorem 1 does not give any useful hint how to increase the degree of non-linearity. It seems that more sophisticated techniques like polynomial type reasoning required.In this note we will construct full-rank factorizations G = AB of the elementary 2-group G of rank 6n, where |A| = |B| and n ≥ 3.

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 6 Issue 8, December 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

2. A Construction

The main result of this paper is the following theorem.

Theorem 1. If $n \geq 3$, then the elementary 2-group of rank 6n admits full-rank factorization into two factors of equal sizes.

Proof. Let n be an integer such that $n \geq 3$. Let G be an elementary 2-group of rank 6n with basis elements

$x_{1,1},\ldots,x_{1,6},\ldots,x_{n,1},\ldots,x_{n,6}$.

Let

$$H_i = \langle x_{i,1}, x_{i,2}, x_{i,3} \rangle ,$$
$$K_i = \langle x_{i,4}, x_{i,5}, x_{i,6} \rangle ,$$
$$L_i = \langle x_{i,1}, \ldots, x_{i,6} \rangle ,$$

for each i, $1 \leq i \leq n$. It is clear that $|H_i| = |K_i| = 2^3 = 8$. Further it is clear that the product H_iK_i is direct and it is equal to L_i for each i, $1 \leq i \leq n$.

From the subgroup Hi of G we construct a subset Ai of G by removing and adding certain elements.

Remove :	Add :
$x_{i,1}$	$x_{i,1}x_{i,4}$
$x_{i,2}$	$x_{i,2}x_{i,5}$
$x_{i,3}$	$x_{i,3}x_{i,6}$

In other words we set
$A_i = (H_i \setminus \{x_{i,1},x_{i,2},x_{i,3}\}) \cup \{x_{i,1}x_{i,4},x_{i,2}x_{i,5},x_{i,3}x_{i,6}\}$,

for each i, $1 \leq i \leq n$.
We claim that the product A_iK_i is direct and it is equal to L_i for each i, $1 \leq i \leq n$.
As the product HiKi is direct and it is equal to Li it follows that the sets
h_iK_i, $h_i \in H_i$

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 6 Issue 8, December 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

(1) form a partition of L_i. We have constructed A_i from H_i by removing elements and adding elements. In the partition (1) we replace the set $x_{i,1}K_i$ by the set $x_{i,1}x_{i,4}K_i$. Note that $xi_{,4}K_i = K_i$ as $x_{i,4} \in K_i$. Ingeneral,

$$\begin{aligned} x_{i,1}K_i &= x_{i,1}x_{i,4}K_i, \\ x_{i,2}K_i &= x_{i,2}x_{i,5}K_i, \\ x_{i,3}K_i &= x_{i,3}x_{i,6}K_i, \end{aligned}$$

and so the sets
$a_iK_i,\ \ a_i \in A_i$ (2)
form a partition of Li. The partition (2) is equivalent to that the product A_iK_i is direct and it is equal to L_i, as required. Let

$$A = A_1 \cdots A_n, \qquad K = K_1 \cdots K_n.$$

We claim that the product AK is direct and it is equal to G. Indeed,

$$\begin{aligned} G &= L_1 \cdots L_n \\ &= (A_1K_1)\cdots(A_nK_n) \\ &= (A_1\cdots A_n)(K_1\cdots K_n) \\ &= AK. \end{aligned}$$

Thus the product AK is direct and it is equal to G, as required. In particular the product $A_1 \cdots A_n$ is direct and so $|A| = |A_1|\cdots|A_n|$ =
$(2^3)n = 2^3n$. In the above argument we used the observation that if the product AiKi is direct and is equal to L_i and if the product $L_1 \cdots L_n$ is direct and is equal to G, then the product $A_1K_1 \cdots A_nK_n$ is direct and is equal to G.
Next we claim that $\langle A_i\rangle = L_i$ for each $_i$, $1 \le {}_i \le n$. As $x_{i,2}x_{i,3} \in A_i$ and $x_i{,}1x_{i,2}x_{i,3} \in A_i$, it follows that $x_{i,1} \in \langle A_i\rangle$. As $x_{i,1}x_{i,4} \in A_i$ and $x_{i,1} \in \langle A_i\rangle$, it follows that $x_{i,4} \in \langle A_i\rangle$. A similar reasoning gives that in general

$$\begin{aligned} x_{i,1}, x_{i,4} &\in \langle A_i\rangle, \\ x_{i,2}, x_{i,5} &\in \langle A_i\rangle, \\ x_{i,3}, x_{i,6} &\in \langle A_i\rangle. \end{aligned}$$

Thus $\langle A_i\rangle = L_i$, as we claimed.
Since $e \in A_1,\dots,e \in A_n$, we get that $A_1,\dots,A_n \subset A_{1\dots\dots}$AIt follows that $\langle A\rangle = G$. In other words A is a full-rank subset of .
Let f be the cyclic permutation of the numbers 1,...,n defined by

$$\begin{bmatrix} 1 & 2 & \dots & n-1 & n \\ f(1) & f(2) & \dots & f(n-1) & f(n) \end{bmatrix} = \begin{bmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{bmatrix}$$

From the subgroup K of G we construct a subset B of G. We do this by removing certain subsets from K and adding certain subsets to K.

Remove : Add :

$x_{i,4}K_{f(i)}x_{i,4}x_{f(i),1}K_{f(i)}$

$x_{i,5}K_{f(i)}x_{i,5}x_{f(i),2}K_{f(i)}x_{i,6}K_{f(i)}x_{i,6}x_{f(i),3}K_{f(i)}$

We claim that

$$x_{i,4}K_{f(i)}A = x_{i,4}x_{f(i),1}K_{f(i)}A, \tag{3}$$

$$x_{i,5}K_{f(i)}A = x_{i,5}x_{f(i),2}K_{f(i)}A, \tag{4}$$

$$x_{i,6}K_{f(i)}A = x_{i,6}x_{f(i),3}K_{f(i)}A, \tag{5}$$

for each i, $1 \leq i \leq n$. There are 3n equations to check. But the number of essentially distinct cases can be reduced to 3. For the sake of definiteness we verify the first equation. We compute the left hand side and we compute the right hand side.

$$\begin{aligned} x_{i,4}K_{f(i)}A &= x_{i,4}K_{f(i)}(A_1 \cdots A_n) \\ &= x_{i,4}(K_{f(i)}A_{f(i)})\overline{A}_{f(i)} \\ &= x_{i,4}L_{f(i)}\overline{A}_{f(i)} \end{aligned}$$

Here $A_{f(i)}$ is computed in the following way. We delete $A_{f(i)}$ from the list $A_1,\dots,A_n$ and multiply the remaining sets.

$$\begin{aligned} x_{i,4}x_{f(i),1}K_{f(i)}A &= x_{i,4}x_{f(i),1}K_{f(i)}(A_1 \cdots A_n) \\ &= x_{i,4}x_{f(i),1}(K_{f(i)}A_{f(i)})\overline{A}_{f(i)} \\ &= x_{i,4}x_{f(i),1}L_{f(i)}\overline{A}_{f(i)} \\ &= x_{i,4}L_{f(i)}\overline{A}_{f(i)} \end{aligned}$$

The last step hinges on $\binom{3n}{2}$ the fact that $x_{f(i),1} \in L_{f(i)}$ and so $x_{f(i),1}L_{f(i)} = L_{f(i)}$. The remaining cases can be settled in an analogous way. We claim that the sets

$x_{i,4}K_{f(i)}A$,

$x_{i,5}K_{f(i)}A$,

$x_{i,6}K_{f(i)}A$

are pair-wise disjoint. This claim is of course the same as the claim that the sets

$x_{i,4}x_{f(i),1}K_{f(i)}A$,

$x_{i,5}x_{f(i),2}K_{f(i)}A$,

$x_{i,6}x_{f(i),3}K_{f(i)}A$

are pair-wise disjoint. There are 3n sets and we claim that $\binom{3n}{2}$pairs of sets are disjoint. However, the number of the essentially different cases is not morethan$\binom{8}{2}$=28.

In order to prove the claim let us assume on the contrary that two distinct subsets are not disjoint. Among the many possible cases let us consider the following case first.

$x_{i,4}K_{f(i)}A \cap x_{i,5}K_{f(i)}A \neq \emptyset$

It follows that

$$x_{i,4}(K_{f(i)}A_{f(i)})\overline{A}_{f(i)} \cap x_{i,5}(K_{f(i)}A_{f(i)})\overline{A}_{f(i)} \neq \emptyset$$

$$x_{i,4}L_{f(i)}\overline{A}_{f(i)} \cap x_{i,5}L_{f(i)}\overline{A}_{f(i)} \neq \emptyset.$$

For the sake of definiteness suppose that $f_{(i)} = 1$. Consequently, i = n and

$x_{n,4}L_1A_1 \cap x_{n,5}L_1A_1 \neq \emptyset.$

There are elements $l_1, l_1' \in L_1$ and

$$a_1, a_1' \in A_1, \ldots, a_n, a_n' \in A_n$$

such that

$$l_1 a_2 \cdots a_n x_{n,4} = l_1' a_2' \cdots a_n' x_{n,5}$$

Using the fact that the product L1 ⋯Ln is direct and that

$A_1 \subset L_1, \ldots, A_n \subset L_n$

we get that

$$l_1 = l_1', \; a_2 = a_2', \ldots, a_{n-1} = a_{n-1}', \; a_n x_{n,4} = a_n' x_{n,5}$$

The last equation means that $A_n x_{n,4} \cap A_n x_{n,5} \neq \emptyset$. On the other hand after listing the elements of $A_n x_{n,4}$ and $A_n x_{n,5}$ a routine inspection reveals that $A_n x_{n,4} \cap A_n x_{n,5} = \emptyset$. The details of the inspection are listed in **Table** 1. Let us consider another case among the many possibilities.

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 6 Issue 8, December 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Table 1. The elements of the subsets H_n, A_n, $A_nx_{n,4}$, $A_nx_{n,5}$.

H_n	A_n	$A_nx_{n,4}$	$A_nx_{n,5}$
e	e	$x_{n,4}$	$x_{n,5}$
$x_{n,1}$	$x_{n,1}x_{n,4}$	$x_{n,1}$	$x_{n,1}x_{n,4}x_{n,5}$
$x_{n,2}$	$x_{n,2}x_{n,5}$	$x_{n,2}x_{n,5}x_{n,4}$	$x_{n,2}$
$x_{n,3}$	$x_{n,3}x_{n,6}$	$x_{n,3}x_{n,6}x_{n,4}$	$x_{n,3}x_{n,6}x_{n,5}$
$x_{n,1}x_{n,2}$	$x_{n,1}x_{n,2}$	$x_{n,1}x_{n,2}x_{n,4}$	$x_{n,1}x_{n,2}x_{n,5}$
$x_{n,1}x_{n,3}$	$x_{n,1}x_{n,3}$	$x_{n,1}x_{n,3}x_{n,4}$	$x_{n,1}x_{n,3}x_{n,5}$
$x_{n,2}x_{n,3}$	$x_{n,2}x_{n,3}$	$x_{n,2}x_{n,3}x_{n,4}$	$x_{n,2}x_{n,3}x_{n,5}$
$x_{n,1}x_{n,2}x_{n,3}$	$x_{n,1}x_{n,2}x_{n,3}$	$x_{n,1}x_{n,2}x_{n,3}x_{n,4}$	$x_{n,1}x_{n,2}x_{n,3}x_{n,5}$

$x_{i,4}K_{f(i)}A \cap x_{j,4}K_{f(j)}A \neq \emptyset$

It follows that

$$x_{i,4}L_{f(i)}A_{f(i)} \cap x_{j,4}L_{f(j)}A_{f(j)} \neq \emptyset.$$

In order to avoid unnecessary notational difficulties let us suppose that $f_{(i)} = 1$, $i = n$, $f(j) = 3$, $j = 2$. Now

$$x_{n,4}L_1A_1 \cap x_{2,4}L_3A_3 \neq \emptyset.$$

There are elements and (6) such that

$$l_1a_2 \cdots a_nx_{n,4} = l'_3a'_1a'_2a'_4 \cdots a'_nx_{2,4}$$

It follows that

$$l_1 = a'_1,\ a_2 = a'_2x_{2,4},\ a_3 = l'_3,\ a_4 = a'_4, \ldots, a_{n-1} = a'_{n-1},\ a_nx_{n,4} = a'_n$$

The last equation means that $A_nx_{n,4} \cap A_n \neq \emptyset$. On the other hand after listing the elements of $A_nx_{n,4}$ and A_n a routine inspection reveals that $A_nx_{n,4} \cap A_n = \emptyset$.

A similar argument can be used in connection with all the remaining cases.

We claim that the product AB is direct and it is equal to G. In order to verify the claim note that the sets

$$Ak, \quad k \in K \quad (7)$$

form a partition of G. We have constructed B from K by replacing certain subsets Ak by certain subsets Ab. Using the Equations (3), (4), (5) we can see that the sets

$$Ab, \quad b \in B \quad (8)$$

form a partition of G. Partition (8) simply means that the product AB is direct and it is equal to G, as required.

From the above result it follows that $|B| = |K| = |K_1|\cdots|K_n| = 2^{3n}$. The point we would like to stress is that $|A| = |B|$ holds.

We claim that $\langle B\rangle = G$. Since $x_{i,5}x_{i,6} \in B$ and $x_{i,4}x_{i,5}x_{i,6} \in B$, it follows that $x_{i,4} \in \langle B\rangle$. As $x_{i,4} \in \langle B\rangle$ and $x_{i,4}x_{f(i),1} \in B$, it follows that $x_{f(i),1} \in \langle B\rangle$. In general

$x_{i,4}, x_{f(i),1} \in \langle B\rangle$,

$x_{i,5}, x_{f(i),2} \in \langle B\rangle$,

$x_{i,6}, x_{f(i),3} \in \langle B\rangle$,

for each i, $1 \leq i \leq n$. Thus $\langle B\rangle = G$, as required. In other words B is a full-rank subset of G.

3. Open Problems

We close the paper with a number of open problems. The smallest elementary 2-group G for which the construction of the paper works has 2^{18} elements and so the factors A and B have 2^9 elements. The word length in the commonly used computers is a power of 2. Professor C. Carlet has advanced the following problem.

Problem 1. Is there a full-rank factoring G = AB of the elementary 2-group G of order 2^{16} with $|A| = |B|$?

Here is a more ambitious problem.

Problem 2. Determine the minimum order of all elementary abelian 2-groups that admit full-rank factorizations with equal size factors.

In cryptography not the full-rank property of the factors is the key concept but rather the non-linearity of the factors.

Problem 3. In a factorization G = AB of an elementary 2-group with $|A| = |B|$ try to maximize the deviation of the factors from linearity.

The next questions are motivated by pure group theoretical curiosity.

Problem 4. Can a finite abelian 2-group be factored into more than two full-rank factors of equal size?

Problem 5. Can a finite abelian p-group be factored into full-rank factors of equal size?

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Dinitz, M. (2006) Full Rank Tilings of Finite Abelian Groups.SIAM Journal on Discrete Mathematics, 20, 160-170. https://doi.org/10.1137/S0895480104445794

[2] Etzion, T. and Vardy, A. (1998) On Perfect Codes and Tilings: Problems and Solutions. SIAM Journal on Discrete Mathematics, 11, 205-223. https://doi.org/10.1137/S0895480196309171

[3] Qu, M.H. and Venstone, S.A. (1994) Factorizations in the Elementary Abelian p-Groups and Their Cryptographic Significance. Journal of Cryptography, 7, 201-212. https://doi.org/10.1007/BF00203963

[4] Szab´o, S. (2006) Completing Codes and the R´edei Property of Groups. Theoretical Computer Science, 359, 449-454. https://doi.org/10.1016/j.tcs.2006.02.002

[5] Carlet, C. and Youssef, A. Building S-Boxes from Full-Rank Factorization of an Elementary 2-Group. Private Communication.

[6] Carlet, C. (2010) Vectorial Boolean Functions for Cryptography. In: Crama, Y., Ed., Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, Cambridge, 398-470.

https://doi.org/10.1017/CBO9780511780448.012