Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 5, 14–19

The four roots lemma

Kristijan Tabak

Rochester Institute of Technology, Zagreb Campus
D. T. Gavrana 15, 10000 Zagreb, Croatia
e-mail: kxtcad@rit.edu

Abstract: Using pairwise abbreviation and simple characterization of zero-sums over $\mathbb{Z}[\varepsilon]$, where ε is root of unity of order 2^n, we menage to prove that a norm of a sum of any four mutually different roots has to be different that 2.
Keywords: Norm invariance, Group ring, Pairwise abbreviation.
AMS Classification: 11S05, 11T06.

1 Introduction

In various combinatorial structures sums of roots rise up. Especially those of a constant norm. Therefore, there is always a present need to offer some nice characterization of such sums. One good example where such sums occur is in difference set theory. More about difference sets can be found in [1, 2, 3]. Various methods used in difference set theory, as well in estimating values of sums of roots are presented in [4, 5, 6]. Applications of difference sets on coding theory can be found in [7, 8]. Further algebraic approach has been initialized mainly in [9, 10].

Using really simple algebraic argument we find out more about the nature of zero-sums of roots of unity. To be more precise we have following:

Theorem 1. *Let $\varepsilon = e^{\frac{2\pi i}{2^k}}$, $k \geq 1$ and suppose that $\varepsilon^{\alpha_1} + \varepsilon^{\alpha_2} + \cdots + \varepsilon^{\alpha_l} = 0$. Then l is even and there is a partition of the set $\{\alpha_1, \alpha_2, \dots, \alpha_l\}$ in 2-element subsets $\{\alpha_i, \alpha_j\}$ such that*

$$\varepsilon^{\alpha_i} + \varepsilon^{\alpha_j} = 0.$$

Proof: Let $f(x) = x^{\alpha_1} + x^{\alpha_2} + \cdots + x^{\alpha_l}$ and let ε be a root of unity of order 2^k. Then $g(x) = x^{2^{k-1}} + 1$ is the minimal polynomial for the algebraic number ε. We have assumed that ε is a root of $f(x)$, therefore $g(x)$ divides $f(x)$. Thus $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$, thus we have proved our assertion. $\square$

2 Main result

It is known that for vectors $a_1, a_2, \ldots, a_m$ in $\mathbb{C}^n$ following holds $|\sum_{i=1}^{m} a_i| = \sum_{i=1}^{m} |a_i|$ if and only if a_i's are collinear. Otherwise, $|\sum_{i=1}^{m} a_i| \leq \sum_{i=1}^{m} |a_i|$. Now, we are presenting our main result.

Lemma 1. *Let η be a root of unity of order 2^n, where $n \geq 1$. If $\eta^{x_1}, \eta^{x_2}, \eta^{x_3}, \eta^{x_4}$ are mutually different, then $|\eta^{x_1} + \eta^{x_2} + \eta^{x_3} + \eta^{x_4}| \neq 2$.*

Proof: Let us assume that claim in not true. Hence, suppose that there are four mutually different roots $\eta^{x_1}, \eta^{x_2}, \eta^{x_3}, \eta^{x_4}$ such that

$$|\eta^{x_1} + \eta^{x_2} + \eta^{x_3} + \eta^{x_4}| = 2. \tag{1}$$

Let us show that we may assume $\eta^{x_i} + \eta^{x_j} \neq 0$. If there are two roots which are additive inverses, then for two roots which remained we would have $|\eta^{x_k} + \eta^{x_s}| = 2$. Then we get $|\eta^{x_k} + \eta^{x_s}| = |\eta^{x_k}| + |\eta^{x_s}|$. Then it is straightforward that $\eta^{x_k},\ \eta^{x_s}$ should be linearly dependent, hence $\eta^{x_k} = \eta^{x_s}$ which is a contradiction.

We may write $|\eta^{x_1} + \eta^{x_2} + \eta^{x_3} + \eta^{x_4}| = |1 + \eta^{x_1 - x_4} + \eta^{x_2 - x_4} + \eta^{x_3 - x_4}|$. Without losing generality we introduce notation: $x_i \leftrightarrow x_i - x_4$ for $i = 1, 2, 3$. This gives us a motivation to reformulate original problem (1) in a way that we have a premise:

$$|1 + \eta^{x_1} + \eta^{x_2} + \eta^{x_3}| = 2, \tag{2}$$

where $\eta^{x_i} \neq 1$ are mutually different. Hence

$$\sum_{i=1}^{3} (\eta^{x_i} + \eta^{-x_i}) + \sum_{1 \leq i < j \leq 3}^{3} (\eta^{x_i - x_j} + \eta^{x_j - x_i}) = 0. \tag{3}$$

Let us introduce: $P = \sum_{i=1}^{3} (\eta^{x_i} + \eta^{-x_i}),\ T = \sum_{1 \leq i < j \leq 3}^{3} (\eta^{x_i - x_j} + \eta^{x_j - x_i})$. Hence (3) becomes $P + T = 0$. For the sake of simplicity we will write

$$\begin{aligned} i \leftrightarrow j &\quad \text{if} \quad \eta^{x_i} + \eta^{x_j} = 0, \\ i \leftrightarrow js &\quad \text{if} \quad \eta^{x_i} + \eta^{x_j - x_s} = 0, \\ -i \leftrightarrow j &\quad \text{if} \quad \eta^{-x_i} + \eta^{x_j} = 0. \end{aligned}$$

There are some simple properties which hold for introduced notation:

1. $i \leftrightarrow j \Leftrightarrow -i \leftrightarrow -j$,

2. $i \leftrightarrow jk \Leftrightarrow -i \leftrightarrow kj$,

3. $ij \leftrightarrow ks \Leftrightarrow ji \leftrightarrow sk$,

4. $ij \leftrightarrow is \Leftrightarrow j \leftrightarrow s$.

Proof of rule 1: If $i \leftrightarrow j$, then $\eta^{x_i} + \eta^{x_j} = 0$, thus $\eta^{x_i} = -\eta^{x_j}$. After taking the inverse we get $\eta^{-x_i} = -\eta^{-x_j}$, so $\eta^{-x_i} + \eta^{-x_j} = 0$, so $-i \leftrightarrow -j$. Similarly other implication goes.

Proof of rule 2: If $i \leftrightarrow jk$, then $\eta^{x_i} + \eta^{x_j - x_k} = 0$. After inverting $\eta^{-x_i} + \eta^{x_k - x_j} = 0$.

Proof of rule 3: Statement $ij \leftrightarrow ks$ means $\eta^{x_i - x_j} + \eta^{x_k - x_s} = 0$. After taking the inverse we get $\eta^{x_j - x_i} + \eta^{x_s - x_k} = 0$. Therefore $ji \leftrightarrow sk$. Another implication goes similarly.

Proof of rule 4: If $ij \leftrightarrow is$ then $\eta^{x_i - x_j} + \eta^{x_i - x_s} = 0$. If we divide previous equation by η^{x_i} we get $\eta^{-x_j} + \eta^{-x_s} = 0$, thus $\eta^{x_j} + \eta^{x_s} = 0$. So, indeed $j \leftrightarrow s$.

Let us introduce more notation. If $\eta^x + \eta^y = 0$, then $\eta^{x-y} = -1 = \eta^{2^{n-1}}$. Hence $x \equiv y + 2^{n-1} \pmod{2^n}$. This can be represented as equation in $\mathbb{Z}_{2^n}$ in a way $x = y + \delta$, $(\delta = 2^{n-1})$. Notice that $\delta + \delta = 2\delta = 2^n = 0$. Furthermore, if $x = y + \delta$, then $x + \delta = y + \delta + \delta = y$.

Now, we need to list some rules and properties which will be used in process of classification of all possible abbreviations in $P + T = 0$.

Claim 1: Powers in (2) satisfy $2x_i \neq 0$.

If $2x_i = 0$, then $\eta^{2x_i} = 1$. Thus $1 + \eta^{x_i} = 0$ or $-1 + \eta^{x_i} = 0$. Contradiction.

Claim 2: Equations $i \leftrightarrow -i,\ ij \leftrightarrow ji$ can't hold at the same time.

Assume the opposite. First equation would give us $x_i = -x_i + \delta$, while using the second one we would get $x_i - x_j = x_j - x_i + \delta$. Therefore $2x_i = \delta$ and $2x_i = 2x_j + \delta$. But, then $2x_j = 0$, which is not possible due to previous claim.

Claim 3: Equality $i \leftrightarrow ik$ is not possible.

Again, we are using the same approach. Let us assume that the opposite is true. Then, we would have $\eta^{x_i} + \eta^{x_i - x_k} = 0$. Thus $1 + \eta^{x_k} = 0$, which is obvious contradiction.

Claim 4: Equalities $ij \leftrightarrow ji,\ ik \leftrightarrow ki$ are not fulfilled at the same time.

We are assuming that the opposite is true. Then we would have $x_i - x_j = x_j - x_i + \delta$ and $x_i - x_k = x_k - x_i + \delta$. Therefore, $2x_i = 2x_j + \delta$, and $2x_i = 2x_k + \delta$, so $2x_j = 2x_k$. Reached conclusion leads us to $\eta^{x_j} + \eta^{x_k} = 0$ or $\eta^{x_j} = \eta^{x_k}$. In both cases we have a contradiction.

Claim 5: Equalities $i \leftrightarrow ji,\ k \leftrightarrow jk$ are not true at the same time.

Assume the opposite. Then $x_i = x_j - x_i + \delta$ and $x_k = x_j - x_k + \delta$. Therefore $2x_i = x_j + \delta,\ 2x_k = x_j + \delta$. Now we have $2x_i = 2x_k$, for which has been already proved that it is a contradiction.

Claim 6: Equalities $i \leftrightarrow ji,\ k \leftrightarrow ik,\ j \leftrightarrow kj$ are not true at the same time.

On the contrary, we would have $x_i = x_j - x_i + \delta$, $x_k = x_i - x_k + \delta$ and $x_j = x_k - x_j + \delta$. Therefore $2x_i = x_j + \delta,\ 2x_k = x_i + \delta$ and $2x_j = x_k + \delta$. From the second equation we get $4x_k = 2x_i + 2\delta = 2x_i = x_j + \delta$. Thus, $8x_k = 2x_j = x_k + \delta$, so $7x_k = \delta$. This gives us that $\eta^{7x_k} = -1$. We get that order of η^{x_k} divides 7. Thus, we have a contradiction.

Claim 7: Equalities $k \leftrightarrow ji,\ j \leftrightarrow ik$ can not be fulfilled at the same time.

If opposite, we would have $x_k = x_j - x_i + \delta,\ x_j = x_i - x_k + \delta$. After summing, we get $2x_k = 0$, and that contradicts Claim 1.

Claim 8: Following equations can not occur at the same time: $i \leftrightarrow -i,\ jk \leftrightarrow kj,\ k \leftrightarrow ij$.

On the contrary, we would have $2x_i = \delta,\ x_j - x_k = x_k - x_j + \delta,\ x_k = x_i - x_j + \delta$.

From second equation we would have $2x_j = 2x_k + \delta$, while using the third one we get $2x_k = 2x_i - 2x_j$. Therefore $2x_j = 2x_i - 2x_j + \delta$. If we use $2x_i = \delta$ we get $4x_j = 0$. Then $2x_j = 0$ or $2x_j = \delta$. If $2x_j = 0$, then $\eta^{x_j} = 1$, so $\eta^{x_j} = 1$ or $\eta^{x_j} = -1$. In the first case we have a contradiction, since we would have two equal roots. While, in the second case we also have a contradiction, since we would get two roots which can be canceled. If $2x_j = \delta$, then from $2x_k = 2x_i - 2x_j$ and $2x_j = \delta$ we get $2x_k = 0$. This conclusion leads to a contradiction in similar way.

Claim 9: Statements $i \leftrightarrow -i,\ jk \leftrightarrow kj,\ k \leftrightarrow ji$ can not be true at the same time.

Proof is similar to a proof of Claim 8.

Claim 10: Statements $i \leftrightarrow -i,\ k \leftrightarrow ji,\ j \leftrightarrow ki$ can not be true at the same time.

Suppose that claim is not true. Then $2x_i = \delta,\ x_k = x_j - x_i + \delta,\ x_j = x_k - x_i + \delta$. Summing last two equations we get $2x_i = 0$, which is a contradiction.

Now we have to determine possibilities of pairwise abbreviation in (3). Our analysis depend on number of pairs which can be canceled within P.

Case 1: Three pairs are canceled within P. Then $P = 0$, thus $T = 0$. Let us analyze which six terms in P could be abbreviated (in pairs). Let us assume that in P we have $1 \leftrightarrow -1$ i $2 \leftrightarrow -2$, then also $3 \leftrightarrow -3$. Therefore $2x_1 = 2x_2 = 2x_3 = \delta$, which leads us to a conclusion that at least two roots η^{x_i} are equal. Contradiction.

If $1 \leftrightarrow -2,\ 2 \leftrightarrow -3,\ 3 \leftrightarrow -1$, then $\eta^{x_1} = \eta^{x_3}$, and again we get a contradiction.

Notice that premise $i \leftrightarrow -j,\ j \leftrightarrow -k$, for mutually different i, j, k immediately leads us to a contradiction with assumption that all roots are mutually different.

If $1 \leftrightarrow -1$, then the only option is that $2 \leftrightarrow -3$ and $3 \leftrightarrow -2$. From $T = 0$ we get that possibilities for canceling are: $12 \leftrightarrow 21$ and $13 \leftrightarrow 31,\ 23 \leftrightarrow 32$. By Claim 2 (or similarly by Claim 4) that can not happen.

Second possibility would be $12 \leftrightarrow 31,\ 23 \leftrightarrow 32$. Then, we would have $2x_1 = \delta,\ x_2 + x_3 = \delta,\ x_1 - x_2 = x_3 - x_1 + \delta,\ x_2 - x_3 = x_3 - x_2 + \delta$. Using last two equalities we get $2x_1 + 2x_2 = 3x_3 + x_2$. On the other hand, the first one gives $x_2 + \delta = 3x_3$. Using second equation we have $\delta + x_2 + x_3 = 4x_3$. Then $4x_3 = 0$. Therefore, $2x_3 = \delta$. But, we have already seen that this leads us to a contradiction.

Case 2: Two pairs in P are abbreviated.

Without losing generality we may assume that $1 \leftrightarrow -2$. Hence $2 \leftrightarrow -1$. By Claim 3, possibilities for abbreviations of x_3 are: $3 \leftrightarrow 12,\ 3 \leftrightarrow 13,\ 3 \leftrightarrow 23$.

Let $3 \leftrightarrow 12$. If $23 \leftrightarrow 32$, then $13 \leftrightarrow 31$. By Claim 4 we have a contradiction. Also, we need to cover the cases $23 \leftrightarrow 31$ and $32 \leftrightarrow 13$. Then $x_3 = x_1 - x_2 + \delta,\ x_1 + x_2 = \delta,\ x_2 - x_3 = x_3 - x_1 + \delta$, therefore $2x_3 = 0$, but by Claim 1, again, we have a contradiction.

Let $3 \leftrightarrow 13$. If we assume that $23 \leftrightarrow 32$ and $12 \leftrightarrow 21$, then by Claim 4 we are done. It remains to check the case $23 \leftrightarrow 12$ and $32 \leftrightarrow 21$. Then $x_2 - x_3 = x_1 - x_2 + \delta,\ x_1 + x_2 = \delta,\ x_3 = x_1 - x_3 + \delta$. From first and second equality we get $x_3 = 3x_2$. Using the third one, we have $6x_2 = x_1 + \delta$, then $7x_2 = 0$. This is contradiction since the order of η is of power 2. Possibility $3 \leftrightarrow 23$ is the same as previous one (just replace 1 by 2).

Therefore, all options which arise from assumption that there are two pairs which can be abbreviated in P lead us to a contradiction.

Case 3: Only one pair abbreviates in P, while other two are abbreviating with some terms in T.

Without loosing generality we may assume that $1 \leftrightarrow -1$. If, for example $1 \leftrightarrow 2$, then $-1 \leftrightarrow -2$. So, we have more then one pair which abbreviates within P. The same happens if we assume $1 \leftrightarrow 3$ or $1 \leftrightarrow -2$ or $1 \leftrightarrow -3$.

Hence, η^{x_2} is canceled by some term from T. The same holds also for η^{x_3}. Thus, we have following options for canceling η^{x_2}: $2 \leftrightarrow 12, 2 \leftrightarrow 13, 2 \leftrightarrow 31, 2 \leftrightarrow 32$.

If $2 \leftrightarrow 12$, then $3 \leftrightarrow 13$ or $3 \leftrightarrow 23$. Firs possibility is eliminated by Claim 8, while the second one is also eliminated by Claim 2.

If $2 \leftrightarrow 13$, then $3 \leftrightarrow 12$ or $3 \leftrightarrow 21$. In both cases it contradicts to Claim 8. It remains to check $3 \leftrightarrow 23$. But this can be resolved by applying Claim 2.

If $2 \leftrightarrow 31$, then we have one of the following: $3 \leftrightarrow 12, 3 \leftrightarrow 21, 3 \leftrightarrow 23$. First possibility is eliminated by Claim 9, and also the second one by Claim 2.

If $2 \leftrightarrow 32$, then we have to cover the cases: $3 \leftrightarrow 12, 3 \leftrightarrow 21, 3 \leftrightarrow 13$. Using Claims 2 and 9 we get a contradiction. Hereby all options are now covered, and each one of those leads to a contradiction.

Case 4: Now, let us assume that there are no pairs in P which can be abbreviated. In that case, each term in P would be canceled by some from T.

First possibility is that we have maximum number of 'neighbors' meaning $1 \leftrightarrow 21,\ 2 \leftrightarrow 32,\ 3 \leftrightarrow 13$. Claim 6 shows that assumed is not possible. Notice that case $1 \leftrightarrow 21, 2 \leftrightarrow 12$ immediately gives a contradiction, otherwise we would have $x_1 = x_2 - x_1 + \delta$ and $x_2 = x_1 - x_2 + \delta$. After simplifying, $2x_1 = x_2 + \delta$. Hence, $x_2 = 2x_1 + \delta$. After we apply this one can get $2(2x_1 + \delta) = x_1 + \delta$. So, $3x_1 = \delta$. Therefore we would get conclusion that η^{x_1} is of order 2. Contradiction.

Now, we will investigate case when we have two neighbors meaning $i \leftrightarrow ki,\ j \leftrightarrow ij$ ili $i \leftrightarrow ki,\ j \leftrightarrow kj$. First case leads as to $k \leftrightarrow jk$, but then we get the case with the maximum number of neighbors, while for the second option it can be shown, using Claim 5, that also leads us to a contradiction.

Finally, it remains to observe the last case, when we have just one neighbor. Assume that $i \leftrightarrow ji,\ j \leftrightarrow ki$ or $i \leftrightarrow ji, j \leftrightarrow ik$. But, both options links to a previous case (because of necessary condition $k \leftrightarrow jk$). By this, we are done with covering all possible options for pairwise abbreviations in Case 4. Since each one of those possibilities gives a contradiction, proof has been done. □

References

[1] Beth, T., D. Jungnickel, H. Lenz, *Design Theory*. Manheim–Wien–Zürich, EU: Bibliographisches Institut, 1985.

[2] Dillon, J. F., A survey of difference sets in 2-groups. *Proc. of Marshall Hall Memorial Conference*, Vermont, Canada, 1990.

[3] Jungnickel, D., A. Pott, K. W. Smith, Difference Sets. In: Colburn, C. J., J. H. Dinitz, editors. *The Handbook of Combinatorial Designs*, Second Edition, NY, USA: CRC Press, 2007, 419–435.

[4] Leung, K. H., S. L. Ma, Partial difference triples, *J. Algebr. Comb.*, Vol. 2, 1993, 397–409.

[5] Leung, K. H., B. Schmidt, Asymptotic Nonexistence of Difference Sets in Dihedral Groups, *J. Combin. Theory Ser. A.*, Vol. 99, 2002, 261–280.

[6] Leung, K. H., B. Schmidt, The field descent method, *Des. Codes Crypt.*, Vol. 36, 2005, 171–188.

[7] Liebler, R. A., K. W. Smith, On difference sets in certain 2-groups. In: Jungnickel, D., S. A. Vanstone, Editors. *Coding Theory, Design Theory, Group Theory*. NY, USA: Wiley, 1993, 195–212.

[8] Schmidt, B., *Characters and Cyclotomic Fields in Finite Geometry*. Berlin–Heidelberg, Germany: Springer, 2002.

[9] Pott, A., *Finite Geometry and Character Theory*. Berlin–Heidelberg, Germany: Springer–Verlag, 1995.

[10] Turyn, R. J., Character sums and difference sets. *Pacific J. Math.*, Vol. 15, 1965, 319–346.