

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 40 (1994)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: CORRIGENDUM TO "BARKER SEQUENCES AND DIFFERENCE SETS"
Autor: Eliahou, Shalom / Kervaire, Michel
DOI: <https://doi.org/10.5169/seals-61107>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 27.04.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

CORRIGENDUM TO "BARKER SEQUENCES
AND DIFFERENCE SETS"

by Shalom ELIAHOU and Michel KERVAIRE

Wayne Broughton has pointed out to us that Lemma 2 in our proof of Turyn's theorem (Theorem 1, page 354 of [EK], recalled below) is incorrect. Indeed, for $r = 3$, $s = 2$, the element $\alpha = 1 + x_3^4 \in \mathbf{Z}\Gamma_3$ yields a counter-example.

The correct version of Lemma 2 should read as follows:

LEMMA 2. *Let $\alpha \in \mathbf{Z}\Gamma_r (r \geq 1)$ be such that, for some $s \leq r$,*

$$\rho v_j(\alpha) \in 2^{j+1} \mathbf{Z}[\eta_{r-j}] \quad \text{for all } j = 0, \dots, s - 1 .$$

Then, $v_s(\alpha) \in 2^s \mathbf{Z}\Gamma_{r-s}$.

Here, the notation is the same as in [EK], namely: η_i is a primitive 2^i -th root of unity, Γ_i is the cyclic group of order 2^i with generator x_i , $v_j: \Gamma_i \rightarrow \Gamma_{i-j}$ is the map determined by $v_j(x_i) = x_{i-j}$, $0 \leq j \leq i$, and $\rho: \mathbf{Z}\Gamma_i \rightarrow \mathbf{Z}[\eta_i]$ is the map determined by $\rho(x_i) = \eta_i$.

This new version of the lemma involves stronger hypotheses and reaches the same conclusion as the previous one. The stronger hypotheses, however, still hold in the context of the proof of Turyn's theorem.

The proof of Lemma 2 is by induction on s . For $s = 0$, there is nothing to prove. For $s \geq 1$, we write $q = s - 1$, and let

$$v_q(\alpha) = \sum_{i=0}^{2^{r-q}-1} a_i x_{r-q}^i \quad (a_i \in \mathbf{Z}) .$$

By the induction hypothesis, we have $v_q(\alpha) \in 2^q \mathbf{Z}\Gamma_{r-q}$, and hence,

$$a_i \equiv 0 \pmod{2^q}$$

for all $i = 0, \dots, 2^{r-q} - 1$.

We compute $\rho v_q(\alpha)$, using $\eta_{r-q}^{2^{r-s}} = -1$ (recall $s = q + 1$):

$$\rho v_q(\alpha) = \sum_{i=0}^{2^{r-s}-1} (a_i - a_{i+2^{r-s}}) \eta_{r-q}^i.$$

By hypothesis, $\rho v_q(\alpha) \in 2^s \mathbf{Z}[\eta_{r-q}]$. Since $1, \eta_{r-q}, \dots, \eta_{r-q}^{2^{r-s}-1}$ form a \mathbf{Z} -basis of $\mathbf{Z}[\eta_{r-q}]$, it follows that

$$a_i \equiv a_{i+2^{r-s}} \pmod{2^s}$$

for all $i = 0, \dots, 2^{r-s} - 1$.

Now, let $v_s(\alpha) = \sum_{i=0}^{2^{r-s}-1} b_i x_{r-s}^i$. Since $v_s(\alpha) = v_1(v_q(\alpha))$, we have

$$b_i = a_i + a_{i+2^{r-s}}$$

for all $i = 0, \dots, 2^{r-s} - 1$. Thus,

$$b_i \equiv 2a_i \equiv 0 \pmod{2^s}$$

for all $i = 0, \dots, 2^{r-s} - 1$. It follows that $v_s(\alpha) \in 2^s \mathbf{Z}\Gamma_{r-s}$, and the proof of Lemma 2 is complete.

Turyn's theorem says that, *if $D \subset \mathbf{Z}/v\mathbf{Z}$ is a cyclic difference set with parameters $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$, then N is odd.*

The hypothesis that D is a difference set means that

$$\theta(x)\theta(x^{-1}) = N^2 + \lambda(1 + x + \dots + x^{v-1})$$

with $\theta(x) = \sum_{d \in D} x^d \in \mathbf{Z}C_v = \mathbf{Z}[x]/(x^v - 1)$.

We now go over the relevant part of the proof of Turyn's theorem, using the corrected version of Lemma 2.

Given any element z in some ring A such that $z^v = 1$, we denote by $\theta(z)$ the image of $\theta(x)$ under the map $\phi: \mathbf{Z}C_v \rightarrow A$ determined by $\phi(x) = z$.

Let $N = 2^t N_1$ with N_1 odd, and $r = 2t + 2$; thus 2^r is the highest power of 2 dividing $v = 4N^2$. We can suppose $t \geq 1$, for if $t = 0$ there is nothing to do.

Now, let $\alpha = \theta(x_r) \in \mathbf{Z}\Gamma_r$.

ASSERTION: $\rho v_j(\alpha) \in 2^{j+1} \mathbf{Z}[\eta_{r-j}]$ for all $j = 0, \dots, t - 1$.

Indeed, $\rho v_j(\alpha) = \theta(\eta_{r-j})$. Now

$$\theta(\eta_{r-j}) \overline{\theta(\eta_{r-j})} = \theta(\eta_{r-j}) \theta(\eta_{r-j}^{-1}) = N^2 \equiv 0 \pmod{2^{2t}} \text{ in } \mathbf{Z}[\eta_{r-j}].$$

This implies, as claimed, that $\theta(\eta_{r-j})$ is divisible by 2^t , hence by 2^{j+1} , in $\mathbf{Z}[\eta_{r-j}]$ (by Lemma 1, page 354 of [EK]).

Applying the corrected version of Lemma 2 with $s = t$, we conclude

$$\theta(x_{t+2}) = v_t(\alpha) \equiv 0 \pmod{2^t} \text{ in } \mathbf{Z}\Gamma_{t+2}.$$

The remainder of the proof of the theorem (following line 2 on page 356 of [EK]) remains unchanged.

For more comments on [EK], the reader is referred to a note by Wayne Broughton in this same volume, [B].

REFERENCES

- [B] BROUGHTON, W.J. A note on Table I of "Barker sequences and difference sets". *L'Ens. Math., this volume.*
- [EK] ELIAHOU, S. and M. KERVAIRE. Barker sequences and difference sets. *L'Ens. Math.* 38 (1992), 345-382.

(Reçu le 25 avril 1994)

Shalom Eliahou
Michel Kervaire

Section de Mathématiques
Université de Genève
Case Postale 240
1211 Genève 24

vide-leer-empty