# A generalized notion of cross number and applications to monoids of weighted zero-sum sequences


Wolfgang Schmid, joint with Kamil Merito and Oscar Ordaz

LAGA, Université Paris 8



July 12th, 2023
Rings and Factorizations 2023, Graz

# Outline

Zero-sum sequences

Weighted zero-sum sequences

Cross number of a sequence

Arithmetic results for (plus-minus) weighted zero-sum sequences

A notion of cross number for certain C-monoids

# Zero-sum sequences

For a (finite) abelian group $(G, +, 0)$ and a sequences $S$ of elements $g_1 \dots g_k$ from $G$ one says that $S$ is a zero-sum sequence if

$$g_1 + \cdots + g_k = 0 \in G$$

Given two zero-sum sequences $S$ and $T$ their concatenation is again a zero-sum sequences. Thus zero-sum sequences form a monoid. One can study the arithemtic of these monoids (Baginski, Chapman, Gao, Geroldinger, Grynkiewicz, Halter-Koch, Zhong, etc).
Usually one identifies sequences that differ only in the ordering of the terms. I.e., sequences are in fact elements of the free *commutative* monoid over $G$ or multisets.

# The monoid of zero-sum sequences, aka the block monoid, $\mathcal{B}(G_0)$

Let $(G, +, 0)$ be a (finite) abelian group. Let $G_0 \subset G$. A *sequence* $S$ over $G_0$ is an element of $\mathcal{F}(G_0)$ the free abelian monoid with basis $G_0$.
Thus a sequences is a (formal, commutative) product

$$S = \prod_{i=1}^{l} g_i = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}.$$

The sequence $S$ is called a *zero-sum sequence* if its *sum*

$$\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G_0} \mathsf{v}_g(S) g \in G$$

equals 0.
The monoid of zero-sum sequences over $G_0$ is defined as

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \colon \sigma(S) = 0\}.$$

# Study the arithmetic: sets of lengths

A monoid $H$ (commutative, cancellative), for example the multiplicative monoid of a domain, is called *atomic* if each non-zero element $a$ is the product (of finitely many) irreducible elements.
If

$$a = a_1 \dots a_n$$

with irreducible $a_i$, then $n$ is called a length of $a$.

$$\mathsf{L}(a) = \{n \colon n \text{ is a length }\}.$$

For $a$ invertible set $\mathsf{L}(a) = \{0\}$.
The *system of sets of lengths* is

$$\mathcal{L}(H) = \{\mathsf{L}(a) \colon a \in H\}.$$

In general, sets of lengths can be infinite. Yet often they are *finite*. The property is called BF (bounded factorization). We only discuss BF.
If all sets of lengths are singletons, the structure is called half-factorial (Zaks, 1976).

# Applications of monoids of zero-sum sequences

Various monoids and domains of interest admit a transfer-homorphism to monoids of zero-sum sequences (or other auxiliary monoids).

Let $H$ and $\mathcal{B}$ be monoids. A monoid homomorphism $\Theta : H \to \mathcal{B}$ is called a transfer homorphism when it has the following two properties:

- T1 $\mathcal{B} = \Theta(H)\mathcal{B}^\times$ and $\Theta^{-1}(\mathcal{B}^\times) = H^\times$.
- T2 If $u \in H$ and $b, c \in \mathcal{B}$ with $\Theta(u) = bc$, then there exist $v, w \in H$ such that $u = vw$, $\Theta(v) \simeq b$ and $\Theta(w) \simeq c$.

They preserve sets of lengths.

# Sets of lengths via block monoids

For a Krull monoid $H$ sets of lengths just depend on the class group $\mathcal{C}(H) = G$ and the set $G_0$ of classes containing primes (the distribution of prime $v$-ideals).
More precisely, there exists a monoid epimorphism (the block homomorphism)

$$\beta : H \to \mathcal{B}(G_0)$$

such that

$$\mathsf{L}_H(a) = \mathsf{L}_{\mathcal{B}(G_0)}(\beta(a))$$

for each $a \in H$.
More specifically, $\beta(a) = [p_1] \dots [p_k]$ where $\phi(a) = p_1 \dots p_k$ (essentially unique!).

# A classical special case from number theory

Let $K$ be a number field with class group $G$. There is a transfer homomorphism $\beta$ from $\mathcal{O}_K^*$ to $\mathcal{B}(G)$, the monoid of zero-sum sequences over the class group of $K$.
More specifically, $\beta(a) = [p_1] \dots [p_k]$ where $(a) = p_1 \dots p_k$ is the factorization into prime ideals (essentially unique!).

# Weighted zero-sum sequences

Let $(G, +, 0)$ be a (finite) abelian group. Let $G_0 \subset G$. Let $\Omega$ be "a set of weights." Let $S = \prod_{i=1}^{l} g_i$ be a sequence.
Then any elements of the form

$$\sum_{i=1}^{l} \omega_i g_i$$

with $\omega_i \in \Omega$ is called an $\Omega$-weighted sum of $S$.
What do we take as set of weights?

1. Subset of the integers, or of $\{0, 1, \ldots, \exp(G) - 1\}$.
2. Subset of the endomorhisms of $\mathrm{End}(G)$ (more general).
3. One can also generalize further for example subset of $\hom(G, G')$ for some other groups $G'$.

Let $\sigma_\Omega(S)$ denote the set of all elements that are an $\Omega$-weighted sum of $S$.
We say that $S$ is a $\Omega$-weighted zero-sum sequence.
Note: The sequences is not 'weighted', the sum is.

# Weighted zero-sum sequences, II

There are plenty of papers on weighted zero-sum constants (Adhikari and many others).
Davenport constant with weights: What is the smallest integer $l$ such that each sequence $S$ over $G$ of lenght $l$ has a subsequence that is an $\Omega$-weighted zero-sum sequence.
Erdős–Ginzburg–Ziv constant with weights: What is the smallest integer $l$ such that each sequence $S$ over $G$ of lenght $l$ has a subsequence of length $\exp(G)$ that is an $\Omega$-weighted zero-sum sequence.
Etc.
The purpose of this talk is to talk about something else though namely the *monoid* of $\Omega$-weighted zero-sum sequences over $G_0$, which is defined as

$$\mathcal{B}_\Omega(G_0) = \{S \in \mathcal{F}(G_0) \colon \sigma_\Omega(S) \ni 0\}.$$

# Recap: the monoid of $\Omega$-weighted zero-sum sequences

$$\mathcal{B}_\Omega(G) = \{S \in \mathcal{F}(G) \colon 0 \in \sigma_\Omega(S)\} \subset \mathcal{F}(G)$$

be the set of all sequences that have zero as a $\Omega$-weighted sum.
$\mathcal{B}_\Omega(G)$ is a submonoid of $\mathcal{F}(G)$.
Moreover $\mathcal{B}(G) \subset \mathcal{B}_\Omega(G)$.

# Factorizations in monoids of norms

Let $K$ denote a Galois number field. Let $\mathcal{O}_K$ denote its ring of algebraic integers.
Let $\mathsf{N} : \mathcal{O}_K^* \to \mathbb{N}$ denote the absolute norm.
Then $\mathsf{N}(\mathcal{O}_K^*)$ is a submonoid of $(\mathbb{N}^*, \cdot)$. We want to study the arithmetic of that monoid.
Again, one wants to use uniqueness of factorization into prime ideals. A complication is that different prime ideals can have the same norm. To treat this problem one needs 'weighted' zero-sum sequences (initially noted by Halter-Koch).

# Factorizations in monoids of norms, II

**Theorem (Boukheche, Merito, Ordaz, S.)**

*Let $K$ be a Galois number field with Galois group $\Gamma$ and class group $G$. There is a transfer homomorphism from $\mathsf{N}(\mathcal{O}_K^*)$, the monoid of absolute norms of non-zero algebraic integers of $K$, to $\mathcal{B}_\Gamma(G)$, the monoid of $\Gamma$-weighted zero-sum sequences over the class group of $K$.*

Recall that the Galois group acts on the class group; thus it makes sense to talk about $\Gamma$-weighted zero-sum sequences over the class group of $K$.

Further developed by Geroldinger, Halter-Koch, Zhong.

# Length of a sequence

For a sequences $S$ of elements $g_1 \dots g_k$ from $G$ one says that the length of $S$ is $k$, denoted $|S|$.
It is a monoid homorphism from $\mathcal{F}(G)$ to $\mathbb{N}_0$.
This is a simple but useful invariant of the sequence.

- For example if $S \in \mathcal{B}(G)$ then obviously $\max \mathsf{L}(S) \leq |S|$.
- If $S$ does not contain 0, then even $\max \mathsf{L}(S) \leq |S|/2$.

# The cross number of a sequence

For a sequences $S$ of elements $g_1 \dots g_k$ from $G$ one says that the cross number of $S$ is

$$\sum_{i=1}^{k} \frac{1}{\operatorname{ord} g_i}$$

denoted $\mathrm{k}(S)$.
It is a monoid homorphism from $\mathcal{F}(G)$ to $\mathbb{Q}_{\geq 0}$.
Introduced by Skula, Sliwa, Zaks independently (1976).

**Theorem**

*For a subset $G_0 \subset G$ one has that $\mathcal{B}(G_0)$ is half-factorial if and only if $\mathrm{k}(A) = 1$ for each $A \in \mathcal{A}(\mathcal{B}(G_0))$.*

Early contribution by Krause (who introduced the name cross number).

# Proof

Suppose all atoms have cross number 1.
If $S = A_1 \dots A_k = U_1 \dots U_l$ with atoms $A_i, U_j$, then $\mathsf{k}(S) = k$ and $\mathsf{k}(S) = l$, so $k = l$.
Conversely assume there is some $A = g_1 \dots g_r$ with $\mathsf{k}(A) \neq 1$.
We have

$$A^{\exp(G)} = \prod_{i=1}^{r} (g_i^{\operatorname{ord} g_i})^{\exp(G)/\operatorname{ord} g_i}$$

On the right this is a factorization of length $\exp(G)\mathsf{k}(A) \neq \exp(G)$.
Observation: For an atom $A$ one has $\{\exp(G), \exp(G)\mathsf{k}(A)\} \subset \mathsf{L}(A^{\exp(G)})$.

# Sets of lengths

Recall: sets of lengths
If

$$a = a_1 \dots a_n$$

with irreducible $a_i$, then $n$ is called a length of $a$.

$$\mathsf{L}(a) = \{n \colon n \text{ is a length }\}.$$

For $a$ invertible set $\mathsf{L}(a) = \{0\}$.
The *system of sets of lengths* is

$$\mathcal{L}(H) = \{\mathsf{L}(a) \colon a \in H\}.$$

If each set is a singleton we say the monoid is half-factorial.
Otherwise $\mathcal{L}(H)$ contains arbitrarily large sets.

# Sets of lengths, II

For $A \subseteq \mathbb{Z}$, we denote by $\Delta(A)$ the set of (successive) distances of $A$, that is the set of all $d \in \mathbb{N}$ for which there exists $\ell \in A$ such that $A \cap [\ell, \ell + d] = \{\ell, \ell + d\}$. Clearly, $\Delta(A) \subseteq \{d\}$ if and only if $A$ is an arithmetical progression with difference $d$.
For a monoid $H$ we set $\Delta(H) = \bigcup_{a \in H} \Delta(\mathsf{L}(a))$ the set of distances,
and $\Delta^*(H) = \{\min \Delta(H') \colon H' \subset H \text{ divisor-closed, and not HF}\}$ the set of minmal distances.
Introduced by Gao and Geroldinger (2000).

# A fundamental lemma

It is known that $\min \Delta(H) = \gcd \Delta(H)$. (Geroldinger)

## Lemma

*Let $G_0$ be a subset of a finite abelian group.*

$$\min \Delta(\mathcal{B}(G_0)) \mid \gcd\{\exp(G)(\mathsf{k}(A) - 1) \colon A \in \mathcal{A}(\mathcal{B}(G_0))\}$$

Also true for non abelian groups (Geroldinger, Grynkiewicz, Oh, Zhong, 2022)

# A few arithmetic results for weighted zero-sum sequences

We present some similar results with weights.

# The (ir-)reducible elements of $\mathcal{B}_\Omega(G)$

A non-empty/non-invertible $S \in \mathcal{B}_\Omega(G)$ is reducible if there are two non-empty elements $S_1, S_2 \in \mathcal{B}_\Omega(G)$ such that $S = S_1 S_2$.
That is, $S$ can be decomposed into two non-empty $\Omega$-weighted zero-sum sequences $S_1$ and $S_2$.
That is, $S = S_1 S_2$ with $0 \in \sigma_\Omega(S_1)$ and $0 \in \sigma_\Omega(S_2)$.
**Note:** Contrary to the case without weights, it does not suffice that there exist some proper divisor $S_1$ of $S$ with $0 \in \sigma_\Omega(S_1)$, because $0 + a = 0$ implies $a = 0$, but $0 \in A_1$ and $0 \in A_1 + A_2$ does not imply $0 \in A_2$.
We denote by $\mathcal{A}(\mathcal{B}_\Omega(G))$ the set of irreducible $\Omega$-weighted zero-sum sequences.
These monoids are usually not Krull, but are C-monoids (see later).

# A direct consequence of the previous considerations

It is not hard to see that minimal weighted zero-sum sequencs cannot get arbitrarily long. Thus the monoid is finitely generated. As $\mathcal{B}_{\Omega}(G)$ is finitely generated, various arithmetical finiteness results hold.

# A few conequencs of finitely generated

Let $G$ be a finite abelian group and let $G_0 \subseteq G$. Let $\Omega \subseteq \mathsf{End}(G)$ be a set of weights. Let $H = \mathcal{B}_\Omega(G_0)$.

1. We have that $\Delta(H)$ is finite.
2. There is some $M \in \mathbb{N}_0$ such that each set of lengths $L$ of $H$ with $|L| \geq 2$ is an almost arithmetical multiprogression with bound $M$ and difference $d \in \Delta^*(H)$, that is, $L = y + (L_1 \cup L^* \cup L_2) \subset y + \mathcal{D} + d\mathbb{Z}$ with $y \in \mathbb{N}_{\not{\leftarrow}}$, $\{0, d\} \subset \mathcal{D} \subset [0, d]$, $L_1, -L_2 \subset [1, M]$, $\min L^* = 0$ and $L^* = [0, \max L^*] \cap \mathcal{D} + d\mathbb{Z}$.

# Minimal distances for $\mathcal{B}_{\pm}(G)$

We saw that sets of lengths are AAMPs. We might want to undertand their differences. To this end one needs to study minimal distances $\Delta^*$.
What are the divisor-closed submonoids?
These are, as without weights, $\mathcal{B}_{\pm}(G_0)$ for $G_0 \subset G$.
(Geroldinger, Halter-Koch, Zhong)

# A result for groups of odd order

**Theorem (Merito, Ordaz, S.)**

*If* $|G|$ *odd then* $\max \Delta^*(\mathcal{B}_{\pm}(G)) = \exp(G) - 2$*.*

For comparison $\max \Delta^*(\mathcal{B}(G)) = \max\{\exp(G) - 2, \mathrm{r}(G) - 1\}$ (Geroldinger, Zhong), but that's much harder to prove.
In the case of groups of even order $\max \Delta^*(\mathcal{B}_{\pm}(G))$ can exceed $\max \Delta^*(\mathcal{B}(G))$, and can be as large as (the conjectured) $\max \Delta(\mathcal{B}(G))$.

# A simple lemma

## Lemma

*Let* $A \in \mathcal{A}(\mathcal{B}_{\pm}(G))$ *and* $A \neq 0$. *Then* $\{2, |A|\} \subset \mathsf{L}(A^2)$.

Proof: Let $A = g_1 \dots g_k$. Then

$$A^2 = g_1^2 \cdot g_2^2 \dots g_k^2$$

is a factorization as $0 = (+1)g_i + (-1)g_i$.

# Another simple lemma

### Lemma

*Assume that the order of $g$ is odd, then $g^{\mathrm{ord}(g)} \in \mathcal{A}(\mathcal{B}_{\pm}(G))$.*

Proof: While $g^2$ is an atom we cannot factor $g^{\mathrm{ord}(g)}$ into copies of $g^2$,
since $\mathrm{ord}(g)$ is odd.
Basicailly the same situation as for the (numerical) semigroup $\langle 2, \mathrm{ord}(g) \rangle$.

# Somewhat stronger version of the result

### Theorem

*Let $G$ be a finite abelian group exponent $n$ and let $H = \mathcal{B}_{\pm}(G)$. Assume that $n \geq 3$ is odd. Let $D_1 = \{d - 2 \colon d \mid n, d \geq 3\}$ and let $D_2 = \{d' \mid d \colon d \in D_1\}$. Then $D_1 \subseteq \Delta^*(H) \subseteq D_2$. In particular, $\max \Delta^*(H) = n - 2$.*

# A consequence

## Corollary

*Let $p$ be a prime such that $p-2$ is prime. Then for $G = C_p^r$ one has $\Delta^*(\mathcal{B}_{\pm}(G)) = \{1, p-2\}$. In particular, for $p = 3$ one has $\Delta^*(\mathcal{B}_{\pm}(G)) = \{1\}$.*

Note that these results allow quite directly to characterize some (most) of those groups via sets of lengths.
Note for $p = 2$ one has $\Delta^*(\mathcal{B}_{\pm}(G)) = \{1, 2, \ldots, r-1\}$.

# What about the case of even exponent?

Basic construction

**Lemma**

*Let $G$ be a finite abelian group and let $e_1, \dots, e_r$ be independent elements of even order, say $\operatorname{ord}(e_i) = 2m_i$. Assume that $m_1 + \cdots + m_r \geq 2$. Let $e_0 = m_1 e_1 + \cdots + m_r e_r$, $G_0 = \{e_0, e_1, \dots, e_r\}$ and $H = \mathcal{B}_{\pm}(G_0)$. Then $\Delta(H) = \{m_1 + \cdots + m_r - 1\}$ and $\mathsf{c}(H) = m_1 + \cdots + m_r + 1$.*

Proof: $A = e_0 e_1^{m_1} \dots e_r^{m_r}$ is an atom. The only other atoms are $e_i^2$. So $\mathsf{L}(A^2) = \{2, |A|\}$.

# What about the case of even exponent? II

Note that $m_1 + \cdots + m_r - 1$ can significantly exceed $\exp(G) - 2$ and $\mathsf{r}(G)$.
Various results can be obtained but they are not really ready, and I did not yet talk about a generalized cross number at all!

# A notion of cross number for certain C-monoids

Let $H$ be a finitely generated and reduced submonoid of a free monoid $\mathcal{F}(P)$ such that for every $p \in P$ there is an $a \in H$ such that $\mathsf{v}_p(a) > 0$ and such that for every $a \in \mathcal{F}(P)$ there is an $n_a \in \mathbb{N}$ such that $a^{n_a} \in H$. By a result of Cziszter, Domokos and Geroldinger this means that $H$ is a $C$-monoid.
Since $P$ is finite there is an $e$ such that $p^e$ in $H$ for each $p \in P$, for example we can take the least common multiples of the $n_p$ as defined above.
For $p \in P$ let $m_{e,p} \in \mathsf{L}_H(p^e)$ and let $\overline{m}_e = (m_{e,p})_{p \in P}$.
Let $\mathsf{k}_{\overline{m}_e} : \mathcal{F}(P) \to (\mathbb{Q}, +)$ be the monoid homomorphism obtained by extension of $\mathsf{k}_{\overline{m}_e}(p) = m_{e,p}/e$ for each $p \in P$.

# The basic use-case

## Lemma

*Let $H$ be a monoid as specified above, then with the notations introduced above the following holds. For each $a \in \mathcal{A}(H)$ we have $\{e, e\mathsf{k}_{\overline{m}_e}(a)\} \subset \mathsf{L}_H(a^e)$; moreover, we have*

$$\min \Delta(H) \mid \gcd\{e(\mathsf{k}_{\overline{m}_e}(a) - 1) \colon a \in \mathcal{A}(H)\}.$$

# What does this mean for $\mathcal{B}_{\pm}(G)$?

For $\mathcal{B}_{\pm}(G)$ we can take $e = 2$. Then $m_{e,g} = 1$ for $g \neq 0$ and $m_{e,0} = 2$.
Thus the cross number of a sequences $S$ not containing 0 is just $|S|/2$, and

$$|A| - 2 = e(\mathrm{k}(A) - 1)$$

# A generalized notion of cross number and applications to monoids of weighted zero-sum sequences


Wolfgang Schmid, joint with Kamil Merito and Oscar Ordaz

LAGA, Université Paris 8


July 12th, 2023
Rings and Factorizations 2023, Graz