Systems of sets of lengths

W.A. Schmid[1]

LAGA, Université Paris 8, France

September 2014 / Graz

[1] Supported by the ANR project CAESAR

Sets of lengths

A monoid H (commutative, cancellative), for example the multiplicative monoid of a domain, is called

1. *atomic* if each non-zero element a is the product (of finitely many) irreducible elements.
2. *factorial* if there is an essentially unique factorization into irreducibles (i.e., up to ordering and associates).

If the structure is not factorial, one still wants to "understand" the arithmetic.

Sets of lengths, II

For example, study *sets of lengths*.

If

$$a = a_1 \dots a_n$$

with irred. 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

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

Sets of lengths, III

In general, sets of lengths can be infinite.
Yet, for Krull monoids, Dedekind domains, numerical monoids, ... they are *finite*.
The property is called BF (bounded factorization). We only discuss BF.
Note: Each set of lengths is finite, but still in general there are infinitely many sets,
So

$$\mathcal{L}(H) \subset \mathbb{P}_{\text{fin}}(\mathbb{N}_0).$$

General properties of systems of sets of lengths (of BF)

We have

$$\mathcal{L}(H) \subset \mathbb{P}_{\text{fin}}(\mathbb{N}_0).$$

What else?
Let $L, L' \in \mathcal{L}(H)$.

- If $0 \in L$, then $L = \{0\}$.
- If $1 \in L$, then $L = \{1\}$.
- Let $S = L + L' = \{l + l' : l \in L,\ l' \in L'\}$. There exists some $L'' \in \mathcal{L}(H)$ such that $S \subset L''$.

We have $\mathsf{L}(a) + \mathsf{L}(b) \subset \mathsf{L}(ab)$.

General properties of systems of sets of lengths, II

Direct consequences:

- $\{\{0\}\} \subset \mathcal{L}(H)$ and equality holds if and only if H is a group.
- If H is not a group, then $|\mathcal{L}(H)|$ infinite.
- If $\mathcal{L}(H)$ contains some L with $|L| \geq 2$, then $\mathcal{L}(H)$ contains arbitrarily large sets.

Moreover

$$\mathcal{L}(H) \subset \{\{0\}, \{1\}\} \cup \mathbb{P}_{\text{fin}}(\mathbb{N}_{\geq 2}).$$

Dichotomy (for BF-structures)

- Either $|\mathsf{L}(a)| = 1$ for each a,
- or for each n there exists a a_n such that $|\mathsf{L}(a_n)| \geq n$.

If the former (and H not a group), then

$$\mathcal{L}(H) = \{\{n\} : n \in \mathbb{N}_0\}.$$

(Consider a^n for n irreducible.)
Such an H is called *half-factorial*.

Interlude: Why *half*-factorial?

Factorial: if $u_1 \dots u_n = v_1 \dots v_m$, then

- $n = m$,
- and there exist a permutation π such that u_i and $v_{\pi(i)}$ are associates.

For *half*-factorial, we only have the first 'half' of the definition.
What if I want the other half?
So, if if $u_1 \dots u_n = v_1 \dots v_n$, then there exist a permutation π such that u_i and $v_{\pi(i)}$?
Coykendall and Smith: For domains (yet not monoids) other half-factorial implies factorial.

Interlude II: Which structures are half-factorial?

Theorem (Carlitz, 1960)

The ring of algebraic integers of a number field is half-factorial if and only if the class group has at most two elements.

However, already eg, for non-maximal orders and for Krull monoids/Dedekind domains the problem to characterize half-factoriality is subtle.

Interlude II: Which structures are half-factorial?

Theorem (Skula/Śliwa/Zaks 1976)

A Krull monoid with prime cyclic class group is half factorial if an only if only one non-zero class contains prime divisors.

Analogue known for cyclic groups of prime power order, but already for general cyclic groups the problem is open and ‘non-uniform.’

Note: Krull monoids with arbitrarily large class group can be half-factorial.

Question: Can every abelian group be the class group of a half-factorial monoid?

Partial results due to Geroldinger–Göbel.

Interlude II: Which structures are half-factorial?

Theorem (Halter-Koch, 1981)

Let K be a quadratic number field, $\mathcal{O}_K$ its maximal order and $\mathcal{O}_{K,f}$ the unique order of index $f \geq 2$. The following statements are equivalent.

- *$\mathcal{O}_{K,f}$ is half-factorial.*
- *$\mathcal{O}_K$ is half-factorial, $\mathcal{O}_K = \mathcal{O}_K^\times \mathcal{O}_{K,f}$ and f is prime or twice an odd prime.*

Various further investigations on the general problem.

How do (non-trivial) systems of sets look like?

We focus on Krull monoids where each class contains a prime divisor.

- Start by recalling some “complete” results.
- Brief discussion of the general framework to study such problems.
- Results on the general case.

Small class group (Geroldinger 1990)

Let H be a Krull monoid with class group G such that each class contains a prime divisor.

If $G = C_3$ then

$$\mathcal{L}(H) = \{y + 2k + [0, k] : y, k \in \mathbb{N}_0\}$$

If $G = C_2 \oplus C_2$ then

$$\mathcal{L}(H) = \{y + 2k + [0, k] : y, k \in \mathbb{N}_0\}$$

If $G = C_4$ then

$$\begin{aligned}\mathcal{L}(H) = &\{y + 2k + 2 \cdot [0, k] : y, k \in \mathbb{N}_0\} \cup \\ &\{y + k + 1 + [0, k] : y, k \in \mathbb{N}_0\}\end{aligned}$$

If $G = C_2^3$ then

$$\begin{aligned}\mathcal{L}(H) = &\{y + k + 1 + [0, k] : y \in \mathbb{N}_0, k = 0, 1, 2\} \cup \\ &\{y + k + [0, k] : y \in \mathbb{N}_0, k \geq 3\} \cup \\ &\{y + 2k + 2 \cdot [0, k] : y, k \in \mathbb{N}_0\}\end{aligned}$$

Infinite class group (Kainrath, 1999)

Let H be a Krull monoid with class group G such that each class contains a prime divisor.
If G is infnite then

$$\mathcal{L}(H) = \{\{0\}, \{1\}\} \cup \mathbb{P}_{\text{fin}}(\mathbb{N}_{\ge 2}).$$

In other words $\mathcal{L}(H)$ is as large as possible. Or:
“Every” set is is a set of lengths.

Transfer to block monoids

These (and many other) results are proved via “transferring” the arithemtic problem to an auxilliary monoid and then studying the question there.
For a Krull monoid there is a transfer homorphism to the block monoid over the sets of ideal classes containing prime divisors.
A transfer homomorphism preserves sets of lengths.
Note: There are also other (non-commutative) structures that admit a tranfer to these block monoids. (Smertnig, 2013)

Reminder “Krull monoid”

A (comm.) monoid is called a Krull monoid if there exists a free monoid $\mathcal{F}(P)$ and a divisor homomorphism

$$\phi : H \to \mathcal{F}(P),$$

i.e., ϕ is a monoid homomorphism such that

$$a \mid b \quad \iff \quad \phi(a) \mid \phi(b).$$

ϕ is called a divisor theory if $\mathcal{F}(P)$ is “minimal.”
($f = \gcd(\phi(a_1), \ldots, \phi(a_r))$ for each $f \in \mathcal{F}(P)$)
For ϕ a divisor theory of H (unique up to iso.),

$$\mathcal{C}(H) = \mathsf{q}(\mathcal{F}(P))/\mathsf{q}(\operatorname{im}\phi)$$

is called the class group and

$$G_0 = \{g \in \mathcal{C}(H) \colon g \cap P \neq \emptyset\}$$

the subset of classes containing primes.

Reminder “Krull monoid”, II

In fact, one can choose P to equal

$$\mathfrak{X}(H) = v - \max(H) = v - \operatorname{spec}(H) \setminus \{\emptyset\}.$$

I.e., a divisor theory is given by

$$H \to \mathcal{H}(H) \hookrightarrow \mathcal{I}_v^*(H) = \mathcal{F}(\mathfrak{X}(H))$$

($\mathcal{I}_v^*(H)$ monoid of v-invertible v-ideals)
Alternatively, H is Krull if it is Mori (v-noetherian) and completely integrally closed; ...
A domain R is a Krull domain if and only if $(R \setminus \{0\}, \cdot)$ is a Krull monoid. (Krause, 89)

Block monoid $\mathcal{B}(G_0)$

Let $(G, +, 0)$ be an 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 *block monoid* over G_0 is defined as

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

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, $\beta(a) = [p_1] \ldots [p_k]$ where $\phi(a) = p_1 \ldots p_k$ (essentially unique!).

Let us construct some sets of lengths!

Let G be some group. What type of sets of lengths can we construct (easily)?

- Arithmetic progressions.
- Almost arithmetic progressions.
- Arithmetic multiprogressions.

(Note the above examples are all multidemsional AP, but this could be avoided.)

Almost arithmetical multiprogression

We say, L is an AAMP if

$$L = y + (L' \cup L^* \cup L'') \subset y + \mathcal{D} + d\mathbb{Z}$$

with

- $\{0, d\} \subset \mathcal{D} \subset [0, d]$ (period)
- $L^* = [0, l'] \cap (\mathcal{D} + d\mathbb{Z})$ (central part)
- $L' \subset [-M, -1]$ and $L'' \subset [l' + 1, l' + M]$ (initial and end part)

Structure Theorem of Lengths

Geroldinger (1988) showed, later various generalizations and refinements by Freiman, Gerlodinger, Grynkiewicz, Halter-Koch, ...

Theorem

Let H be a Krull monoid where only finitely many classes contain prime divisors. Then there exists a finite set Δ^* and some M such that for each $a \in H$ the set $\mathsf{L}(a)$ is an AAMP with difference $d \in \Delta^*$ and bound m.

Is this the right way to describe sets of lengths?
Several reasons to believe it.

A sort of converse to STSL (S. 2009)

Let $M \in \mathbb{N}_0$ and $\emptyset \neq \Delta^* \subset \mathbb{N}$ finite. Exists a finite abelian group G s.t.:
for every AAMP L with difference $d \in \Delta^*$ and bound M there is some $y_{G,L}$ such that

$$y + L \in \mathcal{L}(G) \text{ for all } y \geq y_{G,L}.$$

Explicit version

$M \in \mathbb{N}$ and $\emptyset \neq \Delta^* \subset \mathbb{N}$, $D = \max \Delta^*$. Let G be a finite abelian group. $\mathcal{L}(G)$ contains (up to shift) each AAMP with difference $d \in \Delta^*$ and bound M if

- G has a subgroup of the form

$$\Big(\bigoplus_{j=1}^{r} \langle e_j \rangle\Big) \oplus \langle f \rangle \oplus \bigoplus_{d \in \Delta^*} \Big(\oplus_{i=0}^{\lceil (M+d-1)/d \rceil} \langle e_i^d \rangle\Big),$$

  where $r \geq 12(M^2 + D)$, $\operatorname{ord} e_j \geq 5$, $\operatorname{ord} f \geq 24(M^2 + D)$ and $\operatorname{ord} e_i^d = d(\lceil (M + d - 1)/d \rceil + i) + 2$, or
- for some prime $p \geq 5$ the p-rank of G is at least $21(M^2 + D)$.

When are AAMPs not necessary?

(Geroldinger 1990; 2014)

Theorem

The following statements are equivalent

(a) *All sets of lengths in $\mathcal{L}(G)$ are arithmetical progressions.*

(b) $G \in \{C_1, C_2, C_2^2, C_2^3, C_3, C_3^2, C_4\}$

Theorem

The following statements are equivalent:

(a) *There is a constant $M \in \mathbb{N}$ such that all sets of lengths in $\mathcal{L}(G)$ are AAPs with bound M.*

(b) *G is a subgroup of C_4^3 or a subgroup of C_3^3.*

When are AAMPs not necessary?, II

Theorem

The following statements are equivalent:

(a) *All sets of lengths in* $\mathcal{L}(G)$ *are* AMPs *with difference in* $\Delta^*(G)$.

(b) G *is cyclic of order* $|G| \le 5$ *or a subgroup of* $\{C_3 \oplus C_3, C_2 \oplus C_2 \oplus C_2\}$.

Which differences do appear?

It is known that the STSL holds for

$$\Delta^*(H)$$

the set of minimal distances of all divisor-closed submonoids of H; and that is the 'right' set to use.

Minimal distance

Let $L = \{\ell_1 < \ell_2 < \cdots < \ell_r\}$, then

$$\Delta(L) = \{\ell_2 - \ell_1, \ell_3 - \ell_2, \ldots, \ell_r - \ell_{r-1}\}.$$

For H BF-monoid, let

$$\Delta(H) = \bigcup_{a \in H} \Delta(\mathsf{L}(a))$$

the set distances of H. And,

$$\min \Delta(H)$$

the minimal distance of H.

Goal: Describe this set $\Delta^*(H)$ explicitly as good as possible!

Transfer

By standard transfer results, we actually are faced with following problem:
Let $(G, +)$ be a finite abelian group (the class group). For a subset $G_0 \subset G$ study

$$\min \Delta(\mathcal{B}(G_0));$$

where $\mathcal{B}(G_0)$ is the monoid of zero-sum sequences over G_0. Set

$$\Delta^*(G) = \{\min \Delta(\mathcal{B}(G_0)) \colon G_0 \subset G\}.$$

(Note: If each class contains a prime divisor $\Delta^*(H) = \Delta^*(G)$. else $\Delta^*(D) \subset \Delta^*(G)$.)

Some elements in $\Delta^*(G)$

- Let $3 \leq d \mid \exp(G)$, then $d-2 \in \Delta^*(G)$.
- Let $r \leq \mathrm{r}(G)$, then $r-1 \in \Delta^*(G)$.

Also, $1 \in \Delta^*(G)$.
In particular, $\min \Delta^*(G) = 1$ and

$$\max \Delta^*(G) \geq \max\{\exp(G)-2, \mathrm{r}(G)-1\}.$$

What about $\max \Delta^*(G)$?

Geroldinger–Zhong 2014

$$\max \Delta^*(G) = \max\{\mathsf{exp}(G) - 2, \mathsf{r}(G) - 1\}.$$