DIVISIBILITY IN THE STONE-ČECH COMPACTIFICATION

Boris Šobot

Department of Mathematics and Informatics, Faculty of Sciences, Novi Sad

AAA90

The Stone-Čech compactification

N - discrete topological space on the set of natural numbers
Ultrafilter: nonempty $p \subseteq P(N)$ such that:
(1) $A, B \in p \Rightarrow A \cap B \in p$;
(2) $A \in p, A \subseteq B \Rightarrow B \in p$;
(3) $A \subseteq N \Rightarrow A \in p \veebar A^c \in p$.
βN - the set of ultrafilters on N
Base sets for topology on βN: $\bar{A} = \{p \in \beta N : A \in p\}$ for $A \subseteq N$

The Stone-Čech compactification

N - discrete topological space on the set of natural numbers
Ultrafilter: nonempty $p \subseteq P(N)$ such that:
(1) $A, B \in p \Rightarrow A \cap B \in p$;
(2) $A \in p, A \subseteq B \Rightarrow B \in p$;
(3) $A \subseteq N \Rightarrow A \in p \veebar A^c \in p$.
βN - the set of ultrafilters on N
Base sets for topology on βN: $\bar{A} = \{p \in \beta N : A \in p\}$ for $A \subseteq N$

The Stone-Čech compactification

N - discrete topological space on the set of natural numbers
Ultrafilter: nonempty $p \subseteq P(N)$ such that:
(1) $A, B \in p \Rightarrow A \cap B \in p$;
(2) $A \in p, A \subseteq B \Rightarrow B \in p$;
(3) $A \subseteq N \Rightarrow A \in p \veebar A^c \in p$.
βN - the set of ultrafilters on N
Base sets for topology on βN: $\bar{A} = \{p \in \beta N : A \in p\}$ for $A \subseteq N$

The Stone-Čech compactification

N - discrete topological space on the set of natural numbers
Ultrafilter: nonempty $p \subseteq P(N)$ such that:
(1) $A, B \in p \Rightarrow A \cap B \in p$;
(2) $A \in p, A \subseteq B \Rightarrow B \in p$;
(3) $A \subseteq N \Rightarrow A \in p \veebar A^c \in p$.
βN - the set of ultrafilters on N
Base sets for topology on βN: $\bar{A} = \{p \in \beta N : A \in p\}$ for $A \subseteq N$

The Stone-Čech compactification (continued)

Principal ultrafilters $\{A \subseteq N : n \in A\}$ are identified with respective elements $n \in N$

$N^* = \beta N \setminus N$

If C is a compact topological space, every (continuous) function $f : N \to C$ can be extended uniquely to $\tilde{f} : \beta N \to C$

In particular, every function $f : N \to N$ can be extended uniquely to $\tilde{f} : \beta N \to \beta N$

The Stone-Čech compactification (continued)

Principal ultrafilters $\{A \subseteq N : n \in A\}$ are identified with respective elements $n \in N$

$N^* = \beta N \setminus N$

If C is a compact topological space, every (continuous) function $f : N \to C$ can be extended uniquely to $\tilde{f} : \beta N \to C$

In particular, every function $f : N \to N$ can be extended uniquely to $\tilde{f} : \beta N \to \beta N$

The Stone-Čech compactification (continued)

Principal ultrafilters $\{A \subseteq N : n \in A\}$ are identified with respective elements $n \in N$

$N^* = \beta N \setminus N$

If C is a compact topological space, every (continuous) function $f : N \to C$ can be extended uniquely to $\tilde{f} : \beta N \to C$

In particular, every function $f : N \to N$ can be extended uniquely to $\tilde{f} : \beta N \to \beta N$

The Stone-Čech compactification (continued)

Principal ultrafilters $\{A \subseteq N : n \in A\}$ are identified with respective elements $n \in N$

$N^* = \beta N \setminus N$

If C is a compact topological space, every (continuous) function $f : N \to C$ can be extended uniquely to $\tilde{f} : \beta N \to C$

In particular, every function $f : N \to N$ can be extended uniquely to $\tilde{f} : \beta N \to \beta N$

Algebra in the Stone-Čech compactification

$(N, \cdot)$ - semigroup provided with discrete topology

For $A \subseteq N$ and $n \in N$:

$$A/n = \{m \in N : mn \in A\} = \left\{\frac{a}{n} : a \in A, n \mid a\right\}$$

The semigroup operation can be extended to βN as follows:

$$A \in p \cdot q \Leftrightarrow \{n \in N : A/n \in q\} \in p.$$

Then $(\beta N, \cdot)$ is a semigroup, but not commutative.

Algebra in the Stone-Čech compactification

$(N, \cdot)$ - semigroup provided with discrete topology
For $A \subseteq N$ and $n \in N$:

$$A/n = \{m \in N : mn \in A\} = \left\{\frac{a}{n} : a \in A, n \mid a\right\}$$

The semigroup operation can be extended to βN as follows:

$$A \in p \cdot q \Leftrightarrow \{n \in N : A/n \in q\} \in p.$$

Then $(\beta N, \cdot)$ is a semigroup, but not commutative.

Algebra in the Stone-Čech compactification

$(N, \cdot)$ - semigroup provided with discrete topology
For $A \subseteq N$ and $n \in N$:

$$A/n = \{m \in N : mn \in A\} = \left\{\frac{a}{n} : a \in A, n \mid a\right\}$$

The semigroup operation can be extended to βN as follows:

$$A \in p \cdot q \Leftrightarrow \{n \in N : A/n \in q\} \in p.$$

Then $(\beta N, \cdot)$ is a semigroup, but not commutative.

Algebra in the Stone-Čech compactification

$(N, \cdot)$ - semigroup provided with discrete topology
For $A \subseteq N$ and $n \in N$:

$$A/n = \{m \in N : mn \in A\} = \left\{\frac{a}{n} : a \in A, n \mid a\right\}$$

The semigroup operation can be extended to βN as follows:

$$A \in p \cdot q \Leftrightarrow \{n \in N : A/n \in q\} \in p.$$

Then $(\beta N, \cdot)$ is a semigroup, but not commutative.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.

(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mid q$ if $\forall A \in p\ \rho[A] \in q$.

Where $\mid [A] = \{m \in N : \exists a \in A\ a \mid m\}$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mid q$ if $\forall A \in p \ \rho[A] \in q$.

Where $\mid [A] = \{m \in N : \exists a \in A \ a \mid m\}$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mid q$ if $\forall A \in p \ \rho[A] \in q$.

Where $\mid [A] = \{m \in N : \exists a \in A \ a \mid m\}$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mathrel{\widetilde{\mid}} q$ if $\forall A \in p\ \rho[A] \in q$.

Where $\mid [A] = \{m \in N : \exists a \in A\ a \mid m\}$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mathrel{\widetilde{|}} q$ if $\forall A \in p\ \rho[A] \in q$.

Where $\mid [A] = \{m \in N : \exists a \in A\ a \mid m\}$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mid q$ if $\forall A \in p \; \rho[A] \in q$.

Where $\mid [A] = \{m \in N : \exists a \in A \; a \mid m\}$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \,\tilde{\mid}\, q$ if $\forall A \in p \;\; \mid [A] \in q$.

$p \mid_L q$ iff $\beta N q \subseteq \beta N p$.
$p \mid_R q$ iff $q \beta N \subseteq p \beta N$.
$p \mid_M q$ iff $\beta N q \beta N \subseteq \beta N p \beta N$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mathrel{\widetilde{\mid}} q$ if $\forall A \in p \ \ \mid[A] \in q$.

$p \mid_L q$ iff $\beta N q \subseteq \beta N p$.
$p \mid_R q$ iff $q \beta N \subseteq p \beta N$.
$p \mid_M q$ iff $\beta N q \beta N \subseteq \beta N p \beta N$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \,\widetilde{\mid}\, q$ if $\forall A \in p \ \mid [A] \in q$.

$p \mid_L q$ iff $\beta N q \subseteq \beta N p$.
$p \mid_R q$ iff $q \beta N \subseteq p \beta N$.
$p \mid_M q$ iff $\beta N q \beta N \subseteq \beta N p \beta N$.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \mid q$ if $\forall A \in p \ \ \mid [A] \in q$.

These are preorders on βN so we view them as orders on equivalence classes of Green relations.

Extensions of the divisibility relation

Definition

Let $p, q \in \beta N$.
(a) q is left-divisible by p, $p \mid_L q$, if there is $r \in \beta N$ such that $q = rp$.
(b) q is right-divisible by p, $p \mid_R q$, if there is $r \in \beta N$ such that $q = pr$.
(c) q is mid-divisible by p, $p \mid_M q$, if there are $r, s \in \beta N$ such that $q = rps$.
(d) $p \,\widetilde{\mid}\, q$ if $\forall A \in p \; \rho[A] \in q$.

$$\begin{array}{l} \mid_L \\ \\ \mid_R \end{array} \begin{array}{c} \subset \\ \subset \end{array} \mid_M \subset \widetilde{\mid}$$

Divisibility by elements of N

$nN = \{nm : m \in N\}$

Lemma

If $n \in N$, each of the statements: (i) $n \mid_L p$, (ii) $n \mid_R p$, (iii) $n \mid_M p$, (iv) $n \,\widetilde{\mid}\, p$ and (v) $nN \in p$ are equivalent.

Theorem

Let $A \subseteq N$ be downward closed for $\mid$ and closed for the operation of least common multiple. Then there is $x \in \beta N$ divisible by all $n \in A$, and not divisible by any $n \notin A$.

Divisibility by elements of N

$nN = \{nm : m \in N\}$

Lemma

If $n \in N$, each of the statements: (i) $n \mid_L p$, (ii) $n \mid_R p$, (iii) $n \mid_M p$, (iv) $n \;\widetilde{\mid}\; p$ and (v) $nN \in p$ are equivalent.

Theorem

Let $A \subseteq N$ be downward closed for $\mid$ and closed for the operation of least common multiple. Then there is $x \in \beta N$ divisible by all $n \in A$, and not divisible by any $n \notin A$.

Divisibility of elements of N

Proposition

N^* is an ideal of βN.

For $n \in N$ and $p \in N^*$ each of $p \mid_L n$, $p \mid_R n$, $p \mid_M n$, $p \,\widetilde{\mid}\, q$ is impossible.

Divisibility of elements of N

Proposition

N^* is an ideal of βN.

For $n \in N$ and $p \in N^*$ each of $p \mid_L n$, $p \mid_R n$, $p \mid_M n$, $p \widetilde{\mid} q$ is impossible.

Equivalent conditions for divisibility

For $p \in \beta N$:
$C(p) = \{A \subseteq N : \forall n \in N \; A/n \in p\}$
$C(p)$ is a filter and $C(p) \subseteq p$

Theorem

The following conditions are equivalent:
(i) $p \mid_L q$;
(ii) $C(p) \subseteq q$;
(iii) $C(p) \subseteq C(q)$.

Equivalent conditions for divisibility

For $p \in \beta N$:
$C(p) = \{A \subseteq N : \forall n \in N\ A/n \in p\}$
$C(p)$ is a filter and $C(p) \subseteq p$

Theorem

The following conditions are equivalent:
(i) $p \mid_L q$;
(ii) $C(p) \subseteq q$;
(iii) $C(p) \subseteq C(q)$.

Equivalent conditions for divisibility

For $p \in \beta N$:
$C(p) = \{A \subseteq N : \forall n \in N \; A/n \in p\}$
$C(p)$ is a filter and $C(p) \subseteq p$

Theorem

The following conditions are equivalent:
(i) $p \mid_L q$;
(ii) $C(p) \subseteq q$;
(iii) $C(p) \subseteq C(q)$.

Equivalent conditions for divisibility

For $p \in \beta N$:

$D(p) = \{A \subseteq N : \{n \in N : A/n = N\} \in p\}$

$D(p)$ is a filter and $D(p) \subseteq p$

$\mathcal{U} = \{S \subseteq N : S \text{ is upward closed for } \mid\}$

Theorem

The following conditions are equivalent:
(i) $p \,\tilde{\mid}\, q$, *i.e. for all* $A \subseteq N$, $A \in p$ *implies* $\mid [A] \in q$;
(ii) $p \cap \mathcal{U} \subseteq q \cap \mathcal{U}$;
(iii) $D(p) \subseteq D(q)$;
(iv) $D(p) \subseteq q$.

Equivalent conditions for divisibility

For $p \in \beta N$:
$D(p) = \{A \subseteq N : \{n \in N : A/n = N\} \in p\}$
$D(p)$ is a filter and $D(p) \subseteq p$
$\mathcal{U} = \{S \subseteq N : S \text{ is upward closed for } \mid\}$

Theorem

The following conditions are equivalent:
(i) $p \,\widetilde{\mid}\, q$, *i.e. for all* $A \subseteq N$, $A \in p$ *implies* $\mid[A] \in q$;
(ii) $p \cap \mathcal{U} \subseteq q \cap \mathcal{U}$;
(iii) $D(p) \subseteq D(q)$;
(iv) $D(p) \subseteq q$.

Equivalent conditions for divisibility

For $p \in \beta N$:
$D(p) = \{A \subseteq N : \{n \in N : A/n = N\} \in p\}$
$D(p)$ is a filter and $D(p) \subseteq p$
$\mathcal{U} = \{S \subseteq N : S \text{ is upward closed for } \mid\}$

Theorem

The following conditions are equivalent:
(i) $p \,\widetilde{\mid}\, q$, *i.e. for all* $A \subseteq N$, $A \in p$ *implies* $\mid[A] \in q$;
(ii) $p \cap \mathcal{U} \subseteq q \cap \mathcal{U}$;
(iii) $D(p) \subseteq D(q)$;
(iv) $D(p) \subseteq q$.

Equivalent conditions for divisibility

For $p \in \beta N$:
$D(p) = \{A \subseteq N : \{n \in N : A/n = N\} \in p\}$
$D(p)$ is a filter and $D(p) \subseteq p$
$\mathcal{U} = \{S \subseteq N : S \text{ is upward closed for } \mid\}$

Theorem

The following conditions are equivalent:
(i) $p \,\tilde{\mid}\, q$*, i.e. for all* $A \subseteq N$*,* $A \in p$ *implies* $\mid [A] \in q$*;*
(ii) $p \cap \mathcal{U} \subseteq q \cap \mathcal{U}$*;*
(iii) $D(p) \subseteq D(q)$*;*
(iv) $D(p) \subseteq q$*.*

Applications?

The idea: translate problems of infinite character in elementary number theory to $(\beta N, \cdot)$

Example 1

Problem: are there infinitely many perfect numbers?

If the answer is "yes", then there is $p \in N^*$ such that $\{n \in N : \sigma(n) = 2n\} \in p$, so $\widetilde{\sigma}(p) = 2p$.

Applications?

The idea: translate problems of infinite character in elementary number theory to $(\beta N, \cdot)$

Example 1

Problem: are there infinitely many perfect numbers?

If the answer is "yes", then there is $p \in N^*$ such that $\{n \in N : \sigma(n) = 2n\} \in p$, so $\widetilde{\sigma}(p) = 2p$.

Applications?

The idea: translate problems of infinite character in elementary number theory to $(\beta N, \cdot)$

Example 1

Problem: are there infinitely many perfect numbers?

If the answer is "yes", then there is $p \in N^*$ such that $\{n \in N : \sigma(n) = 2n\} \in p$, so $\widetilde{\sigma}(p) = 2p$.

Applications?

Example 1

Problem: are there infinitely many perfect numbers?

$f : N \to N$ is quasimultiplicative if $f(mn) = f(m)f(n)$ for relatively prime $m, n \in N$.

$p, q \in \beta N$ are relatively prime if there is no $r \neq 1$ such that $r \,\widetilde{\mid}\, p$ and $r \,\widetilde{\mid}\, q$.

Theorem

If $f : N \to N$ is (quasi)multiplicative, then so is $\widetilde{f}$.

Applications?

Example 1

Problem: are there infinitely many perfect numbers?

$f : N \to N$ is quasimultiplicative if $f(mn) = f(m)f(n)$ for relatively prime $m, n \in N$.

$p, q \in \beta N$ are relatively prime if there is no $r \neq 1$ such that $r \,\widetilde{\mid}\, p$ and $r \,\widetilde{\mid}\, q$.

Theorem

If $f : N \to N$ is (quasi)multiplicative, then so is $\widetilde{f}$.

Applications?

Example 1

Problem: are there infinitely many perfect numbers?

$f : N \to N$ is quasimultiplicative if $f(mn) = f(m)f(n)$ for relatively prime $m, n \in N$.

$p, q \in \beta N$ are relatively prime if there is no $r \neq 1$ such that $r \mathrel{\widetilde{|}} p$ and $r \mathrel{\widetilde{|}} q$.

Theorem

If $f : N \to N$ is (quasi)multiplicative, then so is $\widetilde{f}$.

Applications?

Example 2

Problem: are there infinitely many Wieferich primes?

p is a Wieferich prime if $p^2 \mid 2^{p-1} - 1$.

Theorem

Let $f : N \to N$ and $g : N \to N$ be functions. If $p \in \beta N$ and the set $S = \{m \in N : f(m) \mid g(m)\}$ belongs to p, then $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

If the answer is "yes", $f(n) = n^2$ and $g(n) = 2^{n-1} - 1$, then there is $p \in N^*$ such that $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

Applications?

Example 2

Problem: are there infinitely many Wieferich primes?

p is a Wieferich prime if $p^2 \mid 2^{p-1} - 1$.

Theorem

Let $f : N \to N$ and $g : N \to N$ be functions. If $p \in \beta N$ and the set $S = \{m \in N : f(m) \mid g(m)\}$ belongs to p, then $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

If the answer is "yes", $f(n) = n^2$ and $g(n) = 2^{n-1} - 1$, then there is $p \in N^*$ such that $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

Applications?

Example 2
Problem: are there infinitely many Wieferich primes?

p is a Wieferich prime if $p^2 \mid 2^{p-1} - 1$.

Theorem

Let $f : N \to N$ and $g : N \to N$ be functions. If $p \in \beta N$ and the set $S = \{m \in N : f(m) \mid g(m)\}$ belongs to p, then $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

If the answer is "yes", $f(n) = n^2$ and $g(n) = 2^{n-1} - 1$, then there is $p \in N^*$ such that $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

Applications?

Example 2

Problem: are there infinitely many Wieferich primes?

p is a Wieferich prime if $p^2 \mid 2^{p-1} - 1$.

Theorem

Let $f : N \to N$ and $g : N \to N$ be functions. If $p \in \beta N$ and the set $S = \{m \in N : f(m) \mid g(m)\}$ belongs to p, then $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

If the answer is "yes", $f(n) = n^2$ and $g(n) = 2^{n-1} - 1$, then there is $p \in N^*$ such that $\widetilde{f}(p) \,\widetilde{\mid}\, \widetilde{g}(p)$.

References

R. C. Walker: *The Stone-Čech compactification*

W. W. Comfort, S. Negrepontis: *The theory of ultrafilters*

N. Hindman, D. Strauss: *Algebra in the Stone-Čech compactification, theory and applications*

B. Šobot: *Divisibility in the Stone-Čech compactification*, submitted

B. Šobot: *Divisibility orders in the Stone-Čech compactification*, in preparation

Thank you for your attention!