How do you measure primality?

Christopher O'Neill

Texas A&M University

coneill@math.tamu.edu

Joint with Thomas Barron and Roberto Pelayo

September 26, 2014

Definition (ω -primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^r u_i$ for r > m, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Definition (ω -primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^r u_i$ for r > m, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Fact

 $\omega(x) = 1$ if and only if x is prime (i.e. $x \mid ab$ implies $x \mid a$ or $x \mid b$).

Definition (ω -primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^r u_i$ for r > m, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Fact

 $\omega(x) = 1$ if and only if x is prime (i.e. $x \mid ab$ implies $x \mid a$ or $x \mid b$).

Fact

M is factorial if and only if every irreducible element $u \in M$ is prime. Moreover, $\omega(p_1 \cdots p_r) = r$ for any primes $p_1, \ldots, p_r \in M$.

Definition (ω -primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^r u_i$ for r > m, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Definition (ω -primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^r u_i$ for r > m, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Definition

A bullet for $x \in M$ is a product $u_1 \cdots u_r$ of irreducible elements such that (i) x divides $u_1 \cdots u_r$, and (ii) x does not divide $u_1 \cdots u_r/u_i$ for each $i \leq r$. The set of bullets of x is denoted bul(x).

Definition (ω -primality)

Fix a cancellative, commutative, atomic monoid M. For $x \in M$, $\omega(x)$ is the smallest positive integer m such that whenever $x \mid \prod_{i=1}^r u_i$ for r > m, there exists a subset $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ such that $x \mid \prod_{i \in T} u_i$.

Definition

A bullet for $x \in M$ is a product $u_1 \cdots u_r$ of irreducible elements such that (i) x divides $u_1 \cdots u_r$, and (ii) x does not divide $u_1 \cdots u_r/u_i$ for each $i \leq r$. The set of bullets of x is denoted bul(x).

Proposition

$$\omega_M(x) = \max\{r : u_1 \cdots u_r \in \mathsf{bul}(x)\}.$$

Definition

A numerical monoid S is an additive submonoid of $\mathbb N$ with $|\mathbb N\setminus S|<\infty$.

Definition

A numerical monoid S is an additive submonoid of $\mathbb N$ with $|\mathbb N\setminus S|<\infty.$

Fact

Any numerical monoid S has a unique minimal generating set $g_1,\ldots,g_k.$

Definition

A numerical monoid S is an additive submonoid of \mathbb{N} with $|\mathbb{N} \setminus S| < \infty$.

Fact

Any numerical monoid S has a unique minimal generating set $g_1,\ldots,g_k.$

Example

 $\textit{McN} = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}.$

Definition

A numerical monoid S is an additive submonoid of \mathbb{N} with $|\mathbb{N} \setminus S| < \infty$.

Fact

Any numerical monoid S has a unique minimal generating set $g_1,\ldots,g_k.$

Example

 $\textit{McN} = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}.$ "McNugget Monoid"

Definition

A numerical monoid S is an additive submonoid of \mathbb{N} with $|\mathbb{N} \setminus S| < \infty$.

Fact

Any numerical monoid S has a unique minimal generating set $g_1,\ldots,g_k.$

Example

 $\textit{McN} = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}. \text{ "McNugget Monoid"}$

$n \in McN$	$\omega(n)$	bullet	$n \in McN$	$\omega(n)$	bullet
6	3	3 · 20	20	10	10 · 6
9	3	3 · 20	21	5	5 · 6
12	3	3 · 20	24	4	4 · 6
15	4	4 · 6	26	11	$11 \cdot 6$
18	3	3 · 6	27	6	6 · 6

 ω -primality in a numerical monoid S:

 ω -primality in a numerical monoid S:

• Bullets in S: $b_1g_1 + \cdots + b_kg_k \longleftrightarrow \vec{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$.

 ω -primality in a numerical monoid S:

- Bullets in S: $b_1g_1 + \cdots + b_kg_k \longleftrightarrow \vec{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$.
- For each $i \leq k$, we have $c_i \vec{e_i} \in \text{bul}(n)$ for some $c_i > 0$.

 ω -primality in a numerical monoid S:

- Bullets in S: $b_1g_1 + \cdots + b_kg_k \longleftrightarrow \vec{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$.
- For each $i \le k$, we have $c_i \vec{e_i} \in \text{bul}(n)$ for some $c_i > 0$.
- bul(n) $\subset \prod_{i=1}^k [0, c_i]$.

 ω -primality in a numerical monoid S:

- Bullets in S: $b_1g_1 + \cdots + b_kg_k \longleftrightarrow \vec{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$.
- For each $i \le k$, we have $c_i \vec{e_i} \in \text{bul}(n)$ for some $c_i > 0$.
- bul(n) $\subset \prod_{i=1}^k [0, c_i]$.

Algorithm

Search $\prod_{i=1}^{k} [0, c_i]$ for bullets, compute $\omega(n) = \max\{|\vec{b}| : \vec{b} \in \text{bul}(n)\}$.

 ω -primality in a numerical monoid S:

- Bullets in S: $b_1g_1 + \cdots + b_kg_k \longleftrightarrow \vec{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$.
- For each $i \le k$, we have $c_i \vec{e_i} \in \text{bul}(n)$ for some $c_i > 0$.
- bul(n) $\subset \prod_{i=1}^k [0, c_i]$.

Algorithm

Search $\prod_{i=1}^{k} [0, c_i]$ for bullets, compute $\omega(n) = \max\{|\vec{b}| : \vec{b} \in \text{bul}(n)\}$.

Remark

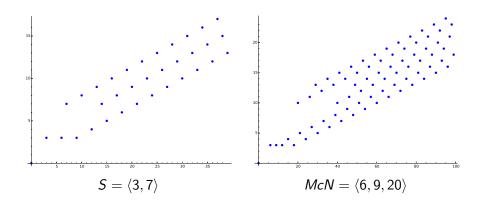
Several improvements on this algorithm exist.

Theorem ((O.–Pelayo, 2013), (García-García et.al., 2013))

 $\omega_S(n) = \frac{1}{g_1}n + a_0(n)$ for $n \gg 0$, where $a_0(n)$ periodic with period g_1 .

Theorem ((O.–Pelayo, 2013), (García-García et.al., 2013))

 $\omega_S(n) = \frac{1}{g_1}n + a_0(n)$ for $n \gg 0$, where $a_0(n)$ periodic with period g_1 .



Dissonance point: minimum N_0 such that $\omega(n)$ is quasilinear for $n > N_0$.

Dissonance point: minimum N_0 such that $\omega(n)$ is quasilinear for $n > N_0$.

Question (O.-Pelayo, 2013)

The upper bound for dissonance point is large. Can we do better?

Dissonance point: minimum N_0 such that $\omega(n)$ is quasilinear for $n > N_0$.

Question (O.-Pelayo, 2013)

The upper bound for dissonance point is large. Can we do better?

Roadblock

Existing algorithms are slow for large n.

Dissonance point: minimum N_0 such that $\omega(n)$ is quasilinear for $n > N_0$.

Question (O.-Pelayo, 2013)

The upper bound for dissonance point is large. Can we do better?

Roadblock

Existing algorithms are slow for large n.

Question (O.-Pelayo, 2014)

Can we dynamically (inductively) compute several ω -values at once?

Dissonance point: minimum N_0 such that $\omega(n)$ is quasilinear for $n > N_0$.

Question (O.-Pelayo, 2013)

The upper bound for dissonance point is large. Can we do better?

Roadblock

Existing algorithms are slow for large n.

Question (O.-Pelayo, 2014)

Can we dynamically (inductively) compute several ω -values at once?

Answer (Barron-O.-Pelayo, 2014)

Yes!

For $n \in S$, let $Z(n) = {\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n}$.

For $n \in S$, let $Z(n) = {\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n}$. For each $i \leq k$,

For
$$n \in S$$
, let $Z(n) = \{\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n\}$.
For each $i \leq k$,

$$\phi_i: \mathsf{Z}(n-g_i) \longrightarrow \mathsf{Z}(n)$$
 $\vec{a} \longmapsto \vec{a} + \vec{e_i}.$

For $n \in S$, let $Z(n) = {\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n}$. For each $i \leq k$,

$$\phi_i: \mathsf{Z}(n-g_i) \longrightarrow \mathsf{Z}(n)$$
 $\vec{a} \longmapsto \vec{a} + \vec{e_i}.$

In particular,

$$\mathsf{Z}(n) = \bigcup_{i \leq k} \phi_i(\mathsf{Z}(n-g_i))$$

For $n \in S$, let $Z(n) = {\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n}$. For each $i \leq k$,

$$\phi_i: \mathsf{Z}(n-g_i) \longrightarrow \mathsf{Z}(n)$$
 $\vec{a} \longmapsto \vec{a} + \vec{e_i}.$

In particular,

$$\mathsf{Z}(n) = \bigcup_{i \le k} \phi_i(\mathsf{Z}(n-g_i))$$

Definition/Proposition (Cover morphisms)

Fix $n \in S$ and $i \le k$. The *i-th cover morphism for n* is the map

$$\psi_i: \mathsf{bul}(n-g_i) \longrightarrow \mathsf{bul}(n)$$

For $n \in S$, let $Z(n) = \{\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n\}$. For each $i \leq k$,

$$\phi_i: \mathsf{Z}(n-g_i) \longrightarrow \mathsf{Z}(n)$$
 $\vec{a} \longmapsto \vec{a} + \vec{e_i}.$

In particular,

$$\mathsf{Z}(n) = \bigcup_{i \le k} \phi_i(\mathsf{Z}(n-g_i))$$

Definition/Proposition (Cover morphisms)

Fix $n \in S$ and $i \le k$. The *i-th cover morphism for n* is the map

$$\psi_i : \mathsf{bul}(n - g_i) \longrightarrow \mathsf{bul}(n)$$

given by

$$\vec{b} \longmapsto \begin{cases} \vec{b} + e_i & \sum_{j=1}^k b_j g_j - n - g_i \notin S \\ \vec{b} & \sum_{j=1}^k b_j g_j - n - g_i \in S \end{cases}$$

For $n \in S$, let $Z(n) = \{\vec{a} \in \mathbb{N}^k : \sum_{i=1}^k a_i g_i = n\}$. For each $i \leq k$,

$$\phi_i: \mathsf{Z}(n-g_i) \longrightarrow \mathsf{Z}(n)$$
 $\vec{a} \longmapsto \vec{a} + \vec{e_i}.$

In particular,

$$\mathsf{Z}(n) = \bigcup_{i \le k} \phi_i(\mathsf{Z}(n-g_i))$$

Definition/Proposition (Cover morphisms)

Fix $n \in S$ and $i \le k$. The *i-th cover morphism for n* is the map

$$\psi_i : \mathsf{bul}(n - g_i) \longrightarrow \mathsf{bul}(n)$$

given by

$$\vec{b} \longmapsto \begin{cases} \vec{b} + e_i & \sum_{j=1}^k b_j g_j - n - g_i \notin S \\ \vec{b} & \sum_{j=1}^k b_j g_j - n - g_i \in S \end{cases}$$

Moreover, bul(n) = $\bigcup_{i < k} \psi_i(\text{bul}(n - g_i))$.**

Definition (ω -primality in numerical monoids)

Fix a numerical monoid S and $n \in S$.

Definition (ω -primality in numerical monoids)

Fix a numerical monoid S and $n \in S$.

 $\omega_S(n)$ is the minimal m such that whenever $(\sum_{i=1}^r g_{j_i}) - n \in S$ for r > m, there exists $T \subset \{1, \dots, r\}$ with $|T| \le m$ and $(\sum_{i \in T} g_{i_i}) - n \in S$.

Definition (ω -primality in numerical monoids)

Fix a numerical monoid S and $n \in S$.

 $\omega_S(n)$ is the minimal m such that whenever $(\sum_{i=1}^r g_{j_i}) - n \in S$ for r > m, there exists $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ and $(\sum_{i \in T} g_{j_i}) - n \in S$.

Definition (ω -primality in numerical monoids)

Fix a numerical monoid S and $n \in \mathbb{Z} = q(S)$. $\omega_S(n)$ is the minimal m such that whenever $(\sum_{i=1}^r g_{j_i}) - n \in S$ for r > m, there exists $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ and $(\sum_{i \in T} g_{j_i}) - n \in S$.

Toward a dynamic algorithm...the base case

Definition (ω -primality in numerical monoids)

Fix a numerical monoid S and $n \in \mathbb{Z} = q(S)$. $\omega_S(n)$ is the minimal m such that whenever $(\sum_{i=1}^r g_{j_i}) - n \in S$ for r > m, there exists $T \subset \{1, \ldots, r\}$ with $|T| \leq m$ and $(\sum_{i \in T} g_{j_i}) - n \in S$.

Remark

All properties of ω extend from S to \mathbb{Z} .

Toward a dynamic algorithm...the base case

Definition (ω -primality in numerical monoids)

Fix a numerical monoid S and $n \in \mathbb{Z} = q(S)$. $\omega_S(n)$ is the minimal m such that whenever $(\sum_{i=1}^r g_{j_i}) - n \in S$ for r > m, there exists $T \subset \{1, \ldots, r\}$ with $|T| \le m$ and $(\sum_{i \in T} g_{i_i}) - n \in S$.

Remark

All properties of ω extend from S to \mathbb{Z} .

Proposition

For $n \in \mathbb{Z}$, the following are equivalent:

- (i) $\omega(n) = 0$,
- (ii) bul(n) = $\{\vec{0}\}$,
- (iii) $-n \in S$.

Example

 $\textit{McN} = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}.$

$$\begin{aligned} \textit{McN} &= \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}. \\ &\underline{n \in \mathbb{Z} \quad \omega(n) \quad \text{bul}(n)} \quad \underline{n \in \mathbb{Z} \quad \omega(n) \quad \text{bul}(n)} \end{aligned}$$

$$\begin{aligned} \textit{McN} &= \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}. \\ &\underbrace{\begin{array}{ccc} \textit{n} \in \mathbb{Z} & \omega(\textit{n}) & \text{bul}(\textit{n}) \\ \leq -44 & 0 & \{\vec{0}\} \end{aligned}}_{} & \underbrace{\begin{array}{ccc} \textit{n} \in \mathbb{Z} & \omega(\textit{n}) & \text{bul}(\textit{n}) \\ \end{array}}_{} \end{aligned}$$

$$\begin{aligned} \textit{McN} &= \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}. \\ &\underbrace{ \begin{matrix} n \in \mathbb{Z} & \omega(n) & \text{bul}(n) \\ \leq -44 & 0 & \{\vec{0}\} \\ -43 & 1 & \{\vec{e_1}, \vec{e_2}, \vec{e_3} \} \end{matrix} }_{ } \underbrace{ \begin{matrix} n \in \mathbb{Z} & \omega(n) & \text{bul}(n) \\ \end{matrix} }_{ } \end{aligned}$$

$$McN = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots\}.$$

$$\frac{n \in \mathbb{Z} \quad \omega(n) \quad \text{bul}(n)}{\leq -44 \quad 0 \quad \{\vec{0}\} \\ -43 \quad 1 \quad \{\vec{e_1}, \vec{e_2}, \vec{e_3}\} \\ -42 \quad 0 \quad \{\vec{0}\}$$

$$McN = \langle 6, 9, 20 \rangle = \{0, 6, 9, 12, 15, 18, 20, 21, \ldots \}.$$
 $n \in \mathbb{Z} \quad \omega(n) \quad \text{bul}(n) \quad n \in \mathbb{Z} \quad \omega(n) \quad \text{bul}(n)$

Runtime comparison

Runtime comparison

S	$n \in S$	$\omega_{\mathcal{S}}(n)$	Existing	Dynamic
$\langle 6, 9, 20 \rangle$	1000	170	0m 67s	0.4s
$\langle 6, 9, 20 \rangle$	2000	340	17m 20s	3.1s
$\langle 31, 39, 45, 52 \rangle$	1000	40	0m 39s	0.3s
(31, 39, 45, 52)	2000	71	24m 31s	2.0s
$\langle 54,67,69,73,75\rangle$	1000	23	2m 02s	0.7s
$\langle 54,67,69,73,75\rangle$	1500	33	22m 50s	2.3s
$\langle 54, 67, 69, 73, 75 \rangle$	3000	61		44.3s
(54, 67, 69, 73, 75)	5000	98		8m 59.0s

Runtime comparison

S	$n \in S$	$\omega_{\mathcal{S}}(n)$	Existing	Dynamic
$\langle 6, 9, 20 \rangle$	1000	170	0m 67s	0.4s
$\langle 6, 9, 20 \rangle$	2000	340	17m 20s	3.1s
$\langle 31, 39, 45, 52 \rangle$	1000	40	0m 39s	0.3s
$\langle 31, 39, 45, 52 \rangle$	2000	71	24m 31s	2.0s
$\langle 54,67,69,73,75\rangle$	1000	23	2m 02s	0.7s
$\langle 54,67,69,73,75\rangle$	1500	33	22m 50s	2.3s
$\langle 54,67,69,73,75\rangle$	3000	61		44.3s
$\langle 54,67,69,73,75\rangle$	5000	98		8m 59.0s

Sage: Open Source Mathematics Software, available at ${\tt www.sagemath.org}.$

GAP Numerical Semigroups Package, available at

http://www.gap-system.org/Packages/numericalsgps.html.

What about more general (finitely generated) monoids M?

• Characterization of ω_M in terms of maximal length bullets?

What about more general (finitely generated) monoids M?

• Characterization of ω_M in terms of maximal length bullets? \checkmark

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)?

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark
- Iterative construction of bullets from cover maps?

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark
- Iterative construction of bullets from cover maps? ✓

What about more general (finitely generated) monoids M?

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark
- Iterative construction of bullets from cover maps? ✓

Problem:

What about more general (finitely generated) monoids M?

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark
- Iterative construction of bullets from cover maps? ✓

Problem: the base case!

What about more general (finitely generated) monoids M?

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark
- Iterative construction of bullets from cover maps? ✓

Problem: the base case!

Problem

Find a dynamic algorithm to compute ω -primality in M.

What about more general (finitely generated) monoids M?

- Characterization of ω_M in terms of maximal length bullets? \checkmark
- Extension of ω_M to q(M)? \checkmark
- Iterative construction of bullets from cover maps? ✓

Problem: the base case!

Problem

Find a dynamic algorithm to compute ω -primality in M.

Question

Are there dynamic algorithms for computing other factorization invariants?

References



Alfred Geroldinger (1997)

Chains of factorizations in weakly Krull domains.

Collog. Math. 72 (1997) 53 - 81.



David Anderson, Scott Chapman, Nathan Kaplan, and Desmond Torkornoo (2011) An algorithm to compute ω -primality in a numerical monoid.

Semigroup Forum 82 (2011), no. 1, 96 – 108.



Christopher O'Neill, Roberto Pelayo (2014)

How do you measure primality?

American Mathematical Monthly, forthcoming.



Thomas Barron, Christopher O'Neill, Roberto Pelayo (2014)

On the computation of delta sets and $\omega\text{-primality}$ in numerical monoids. preprint.

References



Alfred Geroldinger (1997)

Chains of factorizations in weakly Krull domains.

Collog. Math. 72 (1997) 53 - 81.



David Anderson, Scott Chapman, Nathan Kaplan, and Desmond Torkornoo (2011) An algorithm to compute ω -primality in a numerical monoid.

Semigroup Forum 82 (2011), no. 1, 96 – 108.



Christopher O'Neill, Roberto Pelayo (2014)

How do you measure primality?

American Mathematical Monthly, forthcoming.



Thomas Barron, Christopher O'Neill, Roberto Pelayo (2014)

On the computation of delta sets and ω -primality in numerical monoids. preprint.

Thanks!