# On Matrix Factorization

Donald Adams Rene Ardila David Hannasch
Audra Kosh Hanah McCarthy Vadim Ponomarenko*
Ryan Rosenbaum

*Department of Mathematics and Statistics
San Diego State University

AMS Sectional Meeting, Raleigh NC April 4, 2009

http://www-rohan.sdsu.edu/~vadim/matrix.pdf

San Diego State University

# Shameless advertising

Please encourage your students to apply to the

San Diego State University Mathematics REU.

http://www.sci.sdsu.edu/math-reu/index.html

These results are from 2008, and have already led to one scholarly paper (to appear in *Involve*).

# Motivation

Well-developed factorization theory exists for abelian semigroups, rings.

Non-abelian versions have received little attention.

This project: Calculate natural semigroup invariants of natural subsemigroups of $M_n(\mathbb{Z})$

# Motivation

Well-developed factorization theory exists for abelian semigroups, rings.

Non-abelian versions have received little attention.

This project: Calculate natural semigroup invariants of natural subsemigroups of $M_n(\mathbb{Z})$

# Motivation

Well-developed factorization theory exists for abelian semigroups, rings.

Non-abelian versions have received little attention.

This project: Calculate natural semigroup invariants of natural subsemigroups of $M_n(\mathbb{Z})$

# Natural Semigroup Invariants

Given $x$ in a (nonabelian) semigroup, there are natural analogues of abelian invariants $\mathfrak{L}(x), L(x), l(x), \rho(x), \Delta(x)$.

Global invariants: $\rho, \Delta$ (also $\rho_K, \lambda_K$)

No natural analogues: $d(x, y)$, hence $c, t$.

San Diego State University

# Natural Semigroup Invariants

Given $x$ in a (nonabelian) semigroup, there are natural analogues of abelian invariants $\mathfrak{L}(x), L(x), l(x), \rho(x), \Delta(x)$.

Global invariants: $\rho, \Delta$ (also $\rho_k, \lambda_k$)

No natural analogues: $d(x, y)$, hence $c, t$.

# Natural Semigroup Invariants

Given $x$ in a (nonabelian) semigroup, there are natural analogues of abelian invariants $\mathfrak{L}(x), L(x), l(x), \rho(x), \Delta(x)$.

Global invariants: $\rho, \Delta$ (also $\rho_k, \lambda_k$)

No natural analogues: $d(x, y)$, hence $c, t$.

# Bifurcus Semigroups

Let $S$ be an atomic semigroup (ring). We call $S$ *bifurcus* if:

Every element of $S$ that is the product of two or more atoms, is also the product of exactly two atoms.

Immediate consequences: $\mathcal{L}(x)$ is an interval, $2\rho(x) \in \mathbb{N} \cup \{\infty\}$, $\rho(S) = \infty$, $\Delta(S) = \{1\}$

This property was common in our context, but rare otherwise:

Block monoids, Krull monoids, Diophantine monoids, Numerical semigroups, Rings of integers of any algebraic number field are *NOT* bifurcus.

# Bifurcus Semigroups

Let $S$ be an atomic semigroup (ring). We call $S$ *bifurcus* if:

Every element of $S$ that is the product of two or more atoms, is also the product of exactly two atoms.

Immediate consequences: $\mathcal{L}(x)$ is an interval, $2\rho(x) \in \mathbb{N} \cup \{\infty\}$, $\rho(S) = \infty$, $\Delta(S) = \{1\}$

This property was common in our context, but rare otherwise:

Block monoids, Krull monoids, Diophantine monoids, Numerical semigroups, Rings of integers of any algebraic number field are *NOT* bifurcus.

# Bifurcus Semigroups

Let $S$ be an atomic semigroup (ring). We call $S$ *bifurcus* if:

Every element of $S$ that is the product of two or more atoms, is also the product of exactly two atoms.

Immediate consequences: $\mathfrak{L}(x)$ is an interval, $2\rho(x) \in \mathbb{N} \cup \{\infty\}$, $\rho(S) = \infty$, $\Delta(S) = \{1\}$

This property was common in our context, but rare otherwise:

Block monoids, Krull monoids, Diophantine monoids, Numerical semigroups, Rings of integers of any algebraic number field are *NOT* bifurcus.

# A Taste of Bifurcus

Every semigroup can be embedded into a bifurcus semigroup.

There are many examples of bifurcus rings, abelian or non-abelian, with or without zero divisors. All known examples lack 1.

Open problems: existence of bifurcus ring/domain with 1, existence of bifurcus semigroup with finitely many atoms

For details, please see *Bifurcus Semigroups and Rings*.

# A Taste of Bifurcus

Every semigroup can be embedded into a bifurcus semigroup.

There are many examples of bifurcus rings, abelian or non-abelian, with or without zero divisors. All known examples lack 1.

Open problems: existence of bifurcus ring/domain with 1, existence of bifurcus semigroup with finitely many atoms

For details, please see *Bifurcus Semigroups and Rings*.

# A Taste of Bifurcus

Every semigroup can be embedded into a bifurcus semigroup.

There are many examples of bifurcus rings, abelian or non-abelian, with or without zero divisors. All known examples lack 1.

Open problems: existence of bifurcus ring/domain with 1, existence of bifurcus semigroup with finitely many atoms

For details, please see *Bifurcus Semigroups and Rings*.

# A Taste of Bifurcus

Every semigroup can be embedded into a bifurcus semigroup.

There are many examples of bifurcus rings, abelian or non-abelian, with or without zero divisors. All known examples lack 1.

Open problems: existence of bifurcus ring/domain with 1, existence of bifurcus semigroup with finitely many atoms

For details, please see *Bifurcus Semigroups and Rings*.

# History

Jacobson & Wisner, *Matrix Number Theory I*, 1966

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 1.
   Two atoms, unique factorization

2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.
   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither

# History

Jacobson & Wisner, *Matrix Number Theory I*, 1966

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 1.
   Two atoms, unique factorization

2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.
   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither

# History

Jacobson & Wisner, *Matrix Number Theory I*, 1966

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 1.
   Two atoms, unique factorization

2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.
   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither

# Extending JW's results

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.
   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither
   $\rho = 2$ (not achieved), $\Delta = 1$.

2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 0.
   Not atomic (contains idempotents)

3. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 0.
   Bifurcus. $L(x) = 1 + r(gcd(x))$, where $gcd(x)$ denotes the greatest common divisor of the entries of $x$, $r(m)$ denotes the number of prime factors of $m$, counted by multiplicity.

# Extending JW's results

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.
   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither
   $\rho = 2$ (not achieved), $\Delta = 1$.
2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 0.
   Not atomic (contains idempotents)
3. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 0.
   Bifurcus. $L(x) = 1 + r(gcd(x))$, where $gcd(x)$ denotes the greatest common divisor of the entries of $x$, $r(m)$ denotes the number of prime factors of $m$, counted by multiplicity.

# Extending JW's results

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.
   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither
   $\rho = 2$ (not achieved), $\Delta = 1$.

2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 0.
   Not atomic (contains idempotents)

3. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 0.
   Bifurcus. $L(x) = 1 + r(gcd(x))$, where $gcd(x)$ denotes the greatest common divisor of the entries of $x$, $r(m)$ denotes the number of prime factors of $m$, counted by multiplicity.

# Extending JW's results

1. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 1.

   Smallest matrix entry is key: if 1, atom; if 2, unique product of two atoms; otherwise, neither

   $\rho = 2$ (not achieved), $\Delta = 1$.

2. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with determinant 0.

   Not atomic (contains idempotents)

3. $2 \times 2$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with determinant 0.

   Bifurcus. $L(x) = 1 + r(gcd(x))$, where $gcd(x)$ denotes the greatest common divisor of the entries of $x$, $r(m)$ denotes the number of prime factors of $m$, counted by multiplicity.

# Enlarging the Matrix

$n \times n$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with rank 1.

Bifurcus. $L(x) = 1 + r_n(gcd(x))$.
$r_n(m) = \max\{k : m = m_1 m_2 \cdots m_k r, m_i \geq n > r \geq 1\}$.

$r_2(m) = r(m)$, the number of prime factors of $m$.
$r_3(m) = r(m)$ less half of the number of 2 factors of $m$.

# Enlarging the Matrix

$n \times n$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with rank 1.

Bifurcus. $L(x) = 1 + r_n(gcd(x))$.
$r_n(m) = \max\{k : m = m_1 m_2 \cdots m_k r, m_i \geq n > r \geq 1\}$.

$r_2(m) = r(m)$, the number of prime factors of $m$.
$r_3(m) = r(m)$ less half of the number of 2 factors of $m$.

# Enlarging the Matrix

$n \times n$ matrices with entries over $\mathbb{Z}^{\geq 1}$, with rank 1.

Bifurcus. $L(x) = 1 + r_n(gcd(x))$.
$r_n(m) = \max\{k : m = m_1 m_2 \cdots m_k r, m_i \geq n > r \geq 1\}$.

$r_2(m) = r(m)$, the number of prime factors of $m$.
$r_3(m) = r(m)$ less half of the number of 2 factors of $m$.

# Special Rank 1 Matrix Semigroups

1. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with $n - 1$ all-zero rows.

   Bifurcus. $L(x) = r(gcd(x))$, if $gcd(x)$ is an entry in $x$; otherwise $L(x) = 1 + r(gcd(x))$.

2. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with all entries equal.

   Note: This is a commutative ring, without 1

   Let $[a]$ denote the matrix with all entries $a$. Then $L([a])$ equals the greatest power of $n$ dividing $a$. If $n = p^k$, then $\rho = 2 - 1/k$. Otherwise, the semigroup is bifurcus.

# Special Rank 1 Matrix Semigroups

1. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with $n-1$ all-zero rows.

   Bifurcus. $L(x) = r(gcd(x))$, if $gcd(x)$ is an entry in $x$; otherwise $L(x) = 1 + r(gcd(x))$.

2. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with all entries equal.
   Note: This is a commutative ring, without 1

   Let $[a]$ denote the matrix with all entries $a$. Then $L([a])$ equals the greatest power of $n$ dividing $a$. If $n = p^k$, then $\rho = 2 - 1/k$. Otherwise, the semigroup is bifurcus.

# Special Rank 1 Matrix Semigroups

1. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with $n-1$ all-zero rows.

   Bifurcus. $L(x) = r(gcd(x))$, if $gcd(x)$ is an entry in $x$; otherwise $L(x) = 1 + r(gcd(x))$.

2. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with all entries equal.

   Note: This is a commutative ring, without 1

   Let $[a]$ denote the matrix with all entries $a$. Then $L([a])$ equals the greatest power of $n$ dividing $a$. If $n = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

# Special Rank 1 Matrix Semigroups

1. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with $n-1$ all-zero rows.

   Bifurcus. $L(x) = r(gcd(x))$, if $gcd(x)$ is an entry in $x$; otherwise $L(x) = 1 + r(gcd(x))$.

2. $n \times n$ matrices with entries over $\mathbb{Z}^{\geq 0}$, with all entries equal.

   Note: This is a commutative ring, without 1

   Let $[a]$ denote the matrix with all entries $a$. Then $L([a])$ equals the greatest power of $n$ dividing $a$. If $n = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

# Matrices over $\mathbb{Z}$

Key result, proved with Smith Normal Form:

If $|A| = mn$, there exist $B, C$ with $|B| = m$, $|C| = n$, and $A = BC$.

The following matrix semigroups of $M_n(\mathbb{Z})$ are half-factorial:

- $M_n(\mathbb{Z})$ with determinant nonzero
- $M_n(\mathbb{Z})$ with determinant greater than 1
- Triangular matrices from $M_n(\mathbb{Z})$ with determinant nonzero
- Triangular matrices from $M_n(\mathbb{Z})$ with determinant greater than 1

# Matrices over $\mathbb{Z}$

Key result, proved with Smith Normal Form:

If $|A| = mn$, there exist $B, C$ with $|B| = m, |C| = n$, and $A = BC$.

The following matrix semigroups of $M_n(\mathbb{Z})$ are half-factorial:

- $M_n(\mathbb{Z})$ with determinant nonzero
- $M_n(\mathbb{Z})$ with determinant greater than 1
- Triangular matrices from $M_n(\mathbb{Z})$ with determinant nonzero
- Triangular matrices from $M_n(\mathbb{Z})$ with determinant greater than 1

# Odds and Ends

1. $M_n(\mathbb{Z})$ with determinant a nonzero multiple of some $m \in \mathbb{Z}$
   $L(x)$ is the greatest power of $m$ dividing $|x|$. If $m = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

2. Upper triangular matrices from $M_n(k\mathbb{Z})$.
   Bifurcus. $L(x)$ is the greatest power of $k$ dividing all entries of $x$.

3. $2 \times 2$ upper triangular matrices with entries from $\mathbb{Z}^{\geq 1}$.
   $\rho = \infty$. $\Delta$ contains $p - 1$, for every rational prime $p$.

# Odds and Ends

1. $M_n(\mathbb{Z})$ with determinant a nonzero multiple of some $m \in \mathbb{Z}$
   $L(x)$ is the greatest power of $m$ dividing $|x|$. If $m = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

2. Upper triangular matrices from $M_n(k\mathbb{Z})$.
   Bifurcus. $L(x)$ is the greatest power of $k$ dividing all entries of $x$.

3. $2 \times 2$ upper triangular matrices with entries from $\mathbb{Z}^{\geq 1}$.
   $\rho = \infty$. $\Delta$ contains $p - 1$, for every rational prime $p$.

# Odds and Ends

1. $M_n(\mathbb{Z})$ with determinant a nonzero multiple of some $m \in \mathbb{Z}$
   $L(x)$ is the greatest power of $m$ dividing $|x|$. If $m = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

2. Upper triangular matrices from $M_n(k\mathbb{Z})$.
   Bifurcus. $L(x)$ is the greatest power of $k$ dividing all entries of $x$.

3. $2 \times 2$ upper triangular matrices with entries from $\mathbb{Z}^{\geq 1}$.
   $\rho = \infty$. $\Delta$ contains $p - 1$, for every rational prime $p$.

San Diego State University

# Odds and Ends

1. $M_n(\mathbb{Z})$ with determinant a nonzero multiple of some $m \in \mathbb{Z}$
   $L(x)$ is the greatest power of $m$ dividing $|x|$. If $m = p^k$, then $\rho = 2 - {}^1\!/_k$. Otherwise, the semigroup is bifurcus.

2. Upper triangular matrices from $M_n(k\mathbb{Z})$.
   Bifurcus. $L(x)$ is the greatest power of $k$ dividing all entries of $x$.

3. $2 \times 2$ upper triangular matrices with entries from $\mathbb{Z}^{\geq 1}$.
   $\rho = \infty$. $\Delta$ contains $p - 1$, for every rational prime $p$.

San Diego State University

# Odds and Ends

1. $M_n(\mathbb{Z})$ with determinant a nonzero multiple of some $m \in \mathbb{Z}$
   $L(x)$ is the greatest power of $m$ dividing $|x|$. If $m = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

2. Upper triangular matrices from $M_n(k\mathbb{Z})$.
   Bifurcus. $L(x)$ is the greatest power of $k$ dividing all entries of $x$.

3. $2 \times 2$ upper triangular matrices with entries from $\mathbb{Z}^{\geq 1}$.
   $\rho = \infty$. $\Delta$ contains $p - 1$, for every rational prime $p$.

# Odds and Ends

1. $M_n(\mathbb{Z})$ with determinant a nonzero multiple of some $m \in \mathbb{Z}$
   $L(x)$ is the greatest power of $m$ dividing $|x|$. If $m = p^k$, then $\rho = 2 - {}^1/_k$. Otherwise, the semigroup is bifurcus.

2. Upper triangular matrices from $M_n(k\mathbb{Z})$.
   Bifurcus. $L(x)$ is the greatest power of $k$ dividing all entries of $x$.

3. $2 \times 2$ upper triangular matrices with entries from $\mathbb{Z}^{\geq 1}$.
   $\rho = \infty$. $\Delta$ contains $p - 1$, for every rational prime $p$.

# Conclusion

This talk:

http://www-rohan.sdsu.edu/~vadim/matrix.pdf

*Involve* paper:

http://www-rohan.sdsu.edu/~vadim/aahkmpr1.pdf

REU website:

http://www.sci.sdsu.edu/math-reu/index.html

My contact info:

http://www-rohan.sdsu.edu/~vadim/index.html