Elasticities of Almost Factorial Domains

Michael Fitzpatrick

Faculty Sponsor: Karl Kattchee, Mathematics Department

ABSTRACT

For a Krull ring R to be factorial (or a UFD), it is necessary and sufficient that the divisor class group $Cl(R)$ be trivial. When $Cl(R)$ is nontrivial, then of course R is not factorial, but in case $Cl(R)$ is finite and cyclic, then R is called *almost factorial* [F]. The elasticity function $\rho(R)$ provides a way to measure the extent to which unique factorization fails.

In this paper, we generalize a result of Kattchee regarding the elasticity of domains whose class group is cyclic of order $2p$. We use it to confirm a conjecture which arose from computer experimentation.

INTRODUCTION

To understand the multiplicative structure of a ring R, we must consider the relations of the form

$$a_1 \cdot a_2 \cdots a_n = b_1 \cdot b_2 \cdots b_m, \tag{1}$$

where the a_i, b_j are irreducible ring elements. In a unique factorization domain (UFD), the left- and right-hand sides of Eq (1) are always identical. UFD's are characterized precisely as all Krull domains with trivial divisor class group. For some domains, even though the left and right hand sides of Eq (1) are not necessarily identical, at least the *length* of each side is always the same, i.e. $n = m$. An integral domain R that has this property is called an HFD (half factorization domain), and the presence of this property may be encapsulated by the statement $\rho(R) = 1$, where ρ is the *elasticity function* defined as follows

Definition 1. Let R be an atomic integral domain. Then the elasticity of R is defined by

$$\rho(R) = \sup\{\frac{n}{m} \ : \ a_1 \cdot a_2 \cdots a_n = b_1 \cdot b_2 \cdots b_m\}.$$

The elasticity $\rho(R)$ is frequently greater than one, although according to Carlitz [Ca], this cannot happen until Cl(R) has order at least three.

A convenient way to find $\rho(R)$ is to first form the block monoid $\mathcal{B}(G, S)$, where G is the divisor class group $Cl(R)$, and $S \equiv S(R)$ is the subset of $Cl(R)$ consisting of the nontrivial divisor classes which contain a height-one prime, and it turns out that the arithmetic of the block monoid is essentially the same as the (multiplicative) arithmetic of the ring to which it is associated. In particular, we have

$$\rho(R) = \rho(\mathcal{B}(Cl(R), S(R))), \tag{2}$$

see [CG].

Remark 2. It is known that (G, S) is a *realizable pair*, i.e. satisfies $G = Cl(R)$ and $S = S(R)$, precisely when S generates G as a group. See [G].

The case $G = \mathbb{Z}_{p^k}$ has been dealt with in the literature, see [AC], [Kr], and [CS2].

In Kattchee's article [Ka2], existing methods were adapted to the case $G = \mathbb{Z}_{2p}$, and it was proved that

$$\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2 + p, 2, p\}) = \frac{2p - 1}{p}. \tag{3}$$

This paper aims to generalize Eq (3).

The following subsection is for the reader who is unfamiliar with the basics of block monoids and their elasticities.

BLOCK MONOIDS BASICS

If $g_1, \ldots, g_t$ are (not necessarily distinct) non-zero elements of a finite abelian group G such that $\sum_{i=1}^{t} g_i = 0$, then we refer to the system $g_1 g_2 g_3 \cdots g_t$ as a *zero-system* (or *block*) of G. We do not distinguish between two blocks if one can be obtained from the other by a permutation of elements. The

collection $\mathcal{B}(G)$ of all zero-systems of G is a commutative monoid under the operation of concatenation, and if S is a subset of $G \setminus \{0\}$, then we denote by $\mathcal{B}(G,S)$ the submonoid consisting of those blocks which involve only elements of S.

Remark 3. If $S = \{a_1, \ldots, a_k\}$, then we frequently write elements of $\mathcal{B}(G,S)$ in the form $\sigma = a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k}$, where e_i denotes the number of repetitions of a_i in the zero-system σ, or simply in the vector form $\sigma = (e_1, \ldots, e_k)$, provided an ordering of the set S is understood.

Now if we have a block monoid $\mathcal{B}(\mathbb{Z}_b, S)$, *how exactly* do we find its elasticity?

It is possible to find the irreducible nonzero elements of any block monoid $\mathcal{B}(G,S)$ by brute force. If $\#S = n$, and an order on S is fixed, then we may list the irreducibles

$$\text{Minimals}(\mathcal{B}(G,S)) = \{\beta_1, \ldots, \beta_m\}.$$

Viewing the β_i as column vectors, we can form an $n \times m$ matrix

$$B = [\beta_1 \ \beta_2 \ \ldots \ \beta_m]. \tag{4}$$

The set $\ker(B) \cap \mathbb{Z}^m$ is of interest. Each non-zero element of $\ker(B) \cap \mathbb{Z}^m$ encodes a relation among the irreducibles in $\mathcal{B}(G,S)$. In what follows, we shall always order the set $\text{Minimals}(\mathcal{B}(G,S))$ so that the matrix B is well-defined.

Example 4. If $G = \mathbb{Z}_3$ and $S = \{1,2\}$, then we have

$$\text{Minimals}(\mathcal{B}(G,S)) = \{(3,0),(1,1),(0,3)\},$$

and the matrix B turns out to be

$$\begin{bmatrix} 3 & 1 & 0 \\ 0 & 1 & 3 \end{bmatrix}.$$

Example 5. If $G = \mathbb{Z}_{10}$ and $S = \{7,2,5\}$, then we have

$$\text{Minimals}(\mathcal{B}(G,S)) = \{(10,0,0),(0,5,0),(0,0,2),(1,4,1),(2,3,0),(3,2,1),(4,1,0),(5,0,1)\},$$

and the matrix B turns out to be

$$\begin{bmatrix} 10 & 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 0 & 4 & 3 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Example 6. If $G = \mathbb{Z}_{14}$ and $S = \{11,2,7\}$, then the matrix B turns out to be

$$\begin{bmatrix} 14 & 0 & 0 & 1 & 2 & 3 & 6 & 7 & 10 \\ 0 & 7 & 0 & 5 & 3 & 1 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

The terminology in the next definition is from Sturmfels' book [Stu].

Definition 7. (1) Let $v = (v_1, \ldots, v_n)$ be a vector of real numbers. The *support* of v, denoted $\text{supp}(v)$, is defined as the subset of $\{1, \ldots, n\}$ which corresponds to the non-zero entries of v.

(2) Let Φ be a $d \times n$ integer matrix. An element $v \in \ker(\Phi) \cap \mathbb{Z}^n$ is called a *circuit* of Φ if the support of v is minimal with respect to the set of supports of the nontrivial elements of $\ker(\Phi)$, and the greatest common divisor of the entries of v equals 1.

The set of circuits of the matrix B (where B is as in Eq. (4) above) is of special interest. The following definition introduces some useful notation.

Definition 8. Let $v \in \ker(B) \cap \mathbb{Z}^m$, and write v in the canonical form $v^+ - v^-$, where $v_i^+ := \max\{v_i, 0\}$, $v_i^- := \max\{-v_i, 0\}$. The equation

$$\sum_{i=1}^{m} v_i^+ \beta_i = \sum_{i=1}^{m} v_i^- \beta_i \tag{5}$$

displays two distinct factorizations of an element of $M(A)$ which we denote λ_v, and we refer to Eq. (5) as equation Δ_v. Any equation

$$\lambda_1 + \lambda_2 + \cdots + \lambda_l = \mu_1 + \mu_2 + \cdots + \mu_m$$

involving only irreducible non-zero elements of a monoid H, where $l \geq m$, is said to *represent the elasticity* of the monoid, provided $\rho(H) = \frac{l}{m}$.

Theorem 9. [Ka3] *Let A be a $d \times n$ matrix of integers, and set $H = \ker(A) \cap \mathbb{Z}^n$. Then H is a Krull monoid with*

$$\rho(H) = \rho(\lambda_u),$$

for some circuit u of the matrix B whose columns comprise the irreducible nonzero elements of H.

The consequence of this theorem is that we need only investigate those elements of $\ker(B)$ which are also *circuits* of B, which is an advantage because circuits are identified by [Stu] as vectors in $\ker(B)$ have minimal support. In particular, any element of the kernel of a $d \times n$ matrix has $\#\text{supp} \leq d+1$ [Stu]. See [Ka3] for a statement of the algorithm.

Example 10. If $G = \mathbb{Z}_{10}$ and $S = \{7, 2, 5\}$, then

$$\rho(\mathcal{B}(G, S)) = \rho(\lambda_u) = \frac{9}{5},$$

where $u = (-3, 0, 1, -2, 0, 0, 8, 0) \in \ker(B) \cap \mathbb{Z}^8$. Note that u is a circuit of the matrix

$$\begin{bmatrix} 10 & 0 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 0 & 4 & 3 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

the equation Δ_u is given by

$$3(10, 0, 0) + 2(1, 4, 1) = (0, 0, 2) + 8(4, 1, 0),$$

and we have $\lambda_u = (32, 8, 2)$

Note that the result of this example agrees with the result in [Ka3].

Example 11. If $G = \mathbb{Z}_{14}$ and $S = \{11, 2, 7\}$, then

$$\rho(\mathcal{B}(G, S)) = \rho(\lambda_u) = \frac{13}{7},$$

where $u = (-1, 0, 3, -6, 10, 0, 0, 0, 0) \in \ker(B) \cap \mathbb{Z}^9$. Note that u is a circuit of the matrix

$$\begin{bmatrix} 14 & 0 & 0 & 1 & 2 & 3 & 6 & 7 & 10 \\ 0 & 7 & 0 & 5 & 3 & 1 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

the equation Δ_u is given by

$$(14, 0, 0) + 6(1, 5, 1) = 3(0, 0, 2) + 10(2, 3, 0),$$

and we have $\lambda_u = (20, 30, 6)$

This example will be dealt with more generally below.

Definition 12. Let $\lambda = g_1 g_2 g_3 \cdots g_t$ be an irreducible block of a finite abelian group G. The *cross number* $\mathrm{k}(\lambda)$ (a.k.a. *Zaks-Skula constant*) is defined by

$$\mathrm{k}(\lambda) = \sum_{i=1}^{t} \frac{1}{\mathrm{o}(g_i)},$$

where $\mathrm{o}(g_i)$ denotes the order of g_i in G.

If λ is written in the form $a_1^{e_1} a_2^{e_2} \cdots a_s^{e_s}$ (or in the vector form $(e_1, e_1, e_1, \cdots, e_1,)$), where the a_i are the distinct (ordered) elements in λ, then the cross number may be written

$$\mathrm{k}(\lambda) = \sum_{i=1}^{s} \frac{e_i}{\mathrm{o}(a_i)}.$$

Given a block monoid $H := \mathcal{B}(G, S)$, define the constants

$$Z(H) := \sup\{\mathrm{k}(\sigma) \ : \ \sigma \in \mathcal{B}(G, S) \text{ is non-zero and irreducible}\}$$

and

$$z(H) := \inf\{\mathrm{k}(\sigma) \ : \ \sigma \in \mathcal{B}(G, S) \text{ is non-zero and irreducible}\},$$

as in [CS1]. Krause's result [Kr] implies that if H is any monoid of the form $\mathcal{B}(\mathbb{Z}_{p^k}, S)$, then

$$\rho(\mathcal{B}(\mathbb{Z}_{p^k}, S)) = \frac{1}{z(H)}. \tag{6}$$

Thus, one need only inspect the cross numbers of the minimal elements and take the smallest one, and write the reciprocal as the elasticity of the monoid.

If b is *not* a prime power, then the cross number of the group $\mathbb{Z}_b$ is greater than 1, and it is not necessarily possible for the elasticity to be expressed as in Eq. (6).

Example 13. If $G = \mathbb{Z}_{14}$ and $S = \{11, 2, 7\}$, then $\mathrm{k}(1, 5, 1) = 9/7 > 1$. And while the smallest cross number is $\mathrm{k}(2, 3, 0) = 4/7$, the elasticity of the block monoid is not $7/4$, but rather $13/7$ (see EXAMPLE above).

RESULTS

We now state the main theorem.

Theorem 14. *(a)* $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) = \frac{c(2p+1-2c)}{p+c-1}$
if $p \equiv 1 (mod\ 2c)$ *and* $p > (2c-1)^2$
(b) $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) = \frac{2cp}{p+2c-1}$
if $p \equiv 1 (mod\ 2c)$ *and* $p < (2c-1)^2$
(c) $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) = \frac{c(2p-1)}{p+(4c-1)(c-1)}$
if $p \equiv -1 (mod\ 2c)$ *and* $p > 2c-1$
(d) $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) = 1$
if $p = 2c-1$

The remainder of this section is reserved for the verification of the following lemma. The proof of Theorem 14 will be completed in the following subsection.

Lemma 15. *(a)* $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) \geq \frac{c(2p+1-2c)}{p+c-1}$
if $p \equiv 1 (mod\ 2c)$ *and* $p > (2c-1)^2$
(b) $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) \geq \frac{2cp}{p+2c-1}$
if $p \equiv 1 (mod\ 2c)$ *and* $p < (2c-1)^2$
(c) $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) \geq \frac{c(2p-1)}{p+(4c-1)(c-1)}$
if $p \equiv -1 (mod\ 2c)$ *and* $p > 2c-1$
(d) $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) \geq 1$
if $p = 2c-1$

We eventually want to show that the inequalities of Lemma 15 are in fact equalities.

We begin by displaying a table of all irreducible blocks (and their respective cross numbers) in the monoid $\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})$, with $p \equiv 1 (\mathrm{mod}\ 2c)$.

irreducible blocks	cross numbers
$\alpha := (2p, 0, 0)$	1
$\beta := (0, p, 0)$	1
$\gamma := (0, 0, 2)$	1
$\beta_1 := (2, p-2c, 0)$	$\frac{p-(2c-1)}{p}$
$\beta_2 := (4, p-4c, 0)$	$\frac{p-2(2c-1)}{p}$
$\beta_3 := (6, p-6c, 0)$	$\frac{p-3(2c-1)}{p}$
$\vdots$	
$\sigma \equiv \beta_{\frac{p-1}{2c}} := (\frac{p-1}{c}, 1, 0)$	$\frac{p+2c-1}{2pc}$
$\tau \equiv \tau_0 := (1, p-c, 1)$	$\frac{3p-(2c-1)}{2p}$
$\tau_1 := (3, p-3c, 1)$	$\frac{3p-3(2c-1)}{2p}$
$\tau_2 := (5, p-5c, 1)$	$\frac{3p-5(2c-1)}{2p}$
$\vdots$	
$\epsilon \equiv \tau_{\frac{p-1-2c}{2c}} := (\frac{p-(c+1)}{c}, c+1, 1)$	$\frac{(p+2c-1)(c+1)}{2pc}$
$\delta := (p, 0, 1)$	1.

Before moving on, we shall take the time to show that the table above does indeed contain all of the irreducible blocks. It is easy to see that not only are the "primary" elements (α, β, γ, and δ) blocks, they are also irreducible. So let us focus our attention on irreducibles of the form β_j and τ_j.

Note that for blocks with no support in the third entry, the first entry must be even. That said, let us examine blocks of the form $\beta_j = (2j, p-2cj, 0)$. If we start with β and increase the first entry by 2 and decrease the second entry by 2c, we get another irreducible block. We can continue on with this method, stopping when we no longer get a positive number as the second entry. It is impossible to have any more irreducibles of this form because of our construction method.

Let us now consider irreducibles with support in all three entries, $\tau_j = (2j+1, p-c(2j+1), 1)$. We will start this time with $\tau_0 = (1, p-c, 1)$. Let us take the same approach as before: increasing the first entry by 2 while decreasing the second by 2c.

We should consider adding a τ element and a β element to get a different τ. It turns out that this never happens. Any β_j with a lesser first entry than a τ_i will have a greater second entry. So the list above is in fact the complete list of irreducibles.

We now proceed with the proof of parts (a) and (b) of the lemma, that is, the cases where $p \equiv 1 (\text{mod } 2c)$ We address the $p \equiv -1 (\text{mod } 2c)$ below.

In the monoid $\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})$, when $p \equiv 1 (\text{mod } 2c)$ note that

$$2c\tau + (p-1-c)\alpha = (2pc - 2c^2)\sigma + c\gamma \tag{7}$$

when $p > (2c-1)^2$, and

$$2cp\sigma = (p-1)\alpha + 2c\beta \tag{8}$$

when $p < (2c-1)^2$.

These are the necessary relations to complete the proof parts (a) and (b) of Lemma 15. The verification is routine. For example, the reader is invited to show that both sides of Eq. (7), in vector notation, equal $(2(p-c)(p-1), 2c(p-c), 2c)$ and that the quotient of the lengths of the factorizations in Eq. (7) equals $\frac{c(2p+1-2c)}{p+c-1}$, as desired.

Now we consider the monoid $\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})$, $p \equiv -1 (\text{mod } 2c)$. When $p > 2c-1$, the chart of minimal elements (and cross numbers) is as follows:

irreducible blocks	cross numbers
$\alpha := (2p, 0, 0)$	1
$\beta := (0, p, 0)$	1
$\gamma := (0, 0, 2)$	1
$\beta_1 := (2, p-2c, 0)$	$\frac{p-(2c-1)}{p}$
$\beta_2 := (4, p-4c, 0)$	$\frac{p-2(2c-1)}{p}$
$\beta_3 := (6, p-6c, 0)$	$\frac{p-3(2c-1)}{p}$
$\vdots$	
$\sigma \equiv \sigma_1 \equiv \beta_{\frac{p-(2c-1)}{2c}} := (\frac{p+1-2c}{c}, 2c-1, 0)$	$\frac{p+(2c-1)^2}{2pc}$
$\sigma_2 := (\frac{2(p+1)-2c}{c}, 2c-2, 0)$	$\frac{2p+(2c-1)(2c-2)}{2pc}$
$\sigma_3 := (\frac{3(p+1)-2c}{c}, 2c-3, 0)$	$\frac{3p+(2c-1)(2c-3)}{2pc}$
$\vdots$	
$\alpha \equiv \sigma_{2c} := (2p, 0, 0)$	1
$\tau \equiv \tau_0 := (1, p-c, 1)$	$\frac{3p-(2c-1)}{2p}$
$\tau_1 := (3, p-3c, 1)$	$\frac{3p-3(2c-1)}{2p}$
$\tau_2 := (5, p-5c, 1)$	$\frac{3p-5(2c-1)}{2p}$
$\vdots$	
$\epsilon \equiv \epsilon_1 \equiv \tau_{\frac{p-(2c-1)}{2c}} := (\frac{p+1-c}{c}, c-1, 1)$	$\frac{p(c+1)+(2c-1)(c-1)}{2pc}$
$\epsilon_2 := (\frac{2(p+1)-c}{c}, c-2, 1)$	$\frac{p(c+2)+(2c-1)(c-2)}{2pc}$
$\epsilon_3 := (\frac{3(p+1)-c}{c}, c-3, 1)$	$\frac{p(c+3)+(2c-1)(c-3)}{2pc}$
$\vdots$	
$\delta \equiv \epsilon_c := (p, 0, 1)$	1

Note that although the same symbols are used, the blocks for the $p \equiv -1 (\mathrm{mod}\ 2c)$ case are not necessarily equal to the blocks for the $p \equiv 1 (\mathrm{mod}\ 2c)$ case.

The equation

$$2c(2c-1)\tau + (p-(3c-1))\alpha = 2c(p-c)\sigma + c(2c-1)\gamma \tag{9}$$

proves part (c) of Lemma 15 in precisely the same way as (a) and (b) were established.

Part (d) of Lemma 15, $\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) \geq 1$ when $p = 2c-1$, is immediate, as the elasticity of a monoid is always at least 1.

Therefore, Lemma 15 is proved.

PROOF OF THE MAIN THEOREM

The following lemma, whose verification is elementary, records a few relations among the irreducible blocks in $\mathcal{B}(\mathbb{Z}_{2p}, \{2+p, 2, p\}$, for $p \equiv 1 (\mathrm{mod}\ 2c)$.

Lemma 16. *Let $\alpha, \beta, \gamma, \sigma, \beta_i, \tau,$ and τ_j be as in the table on page 5. Then the following equations hold:*

(a) $(p-1)\beta_t = (p-1-2ct)\beta + 2ct\sigma$
(b) $(p-c)\tau_t = t\alpha + ct\gamma + (p-c-2ct)\tau$
(c) $(p-1-c)\tau_t = (2ct+c)\epsilon + (p-2ct-1-2c)\beta + (\frac{p-1}{2} - ct - c)\gamma$
(d) $(p-1)\epsilon = (c)\beta + (\frac{p-1}{2})\gamma + (p-1-c)\sigma$
(e) $2\delta = \alpha + \gamma$
(f) $2p\tau = \alpha + 2(p-c)\beta + p\gamma$

(g) $2(p-1)\tau = 2(p-1-c)\beta + (p-1)\gamma + 2c\sigma$

These relations serve the purpose of providing a way to rephrase any equation which represents a non-unique factorization that may realize the elasticity.

Suppose now that $\frac{l}{m}$ is the elasticity of the monoid $\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})$, and $\lambda_i,\ \mu_j$ are irreducible blocks such that

$$\lambda_1 + \lambda_2 + \cdots + \lambda_l = \mu_1 + \mu_2 + \cdots + \mu_m. \tag{10}$$

That is, Eq (10) *represents* the elasticity of the monoid.

We will use the relations in Lemma 16 to build new equations which represent the same elasticity as Eq. (10). Before doing that, though, we mention the following Lemma, which gives some general information about Eq. (10). Namely, if one considers the cross number as a sort of weight function, then the next lemma says that the left-hand side of Eq. (10) consists of only "lighter" elements, and the right-hand side consists only of "heavier" ones.

Lemma 17. [Ka3] *In Eq (10), we have*

$$k(\lambda_i) \leq 1 \text{ for each } i, \text{ and } k(\mu_j) \geq 1 \text{ for each } j.$$

Now we are ready to use Lemma 16 to further reduce our scope in the search for Eq. (10). Let us begin with the case where $p \equiv 1 (\text{mod } 2c)$.

Lemma 18. *Eq. (10) may be replaced with an equation in which the only irreducible blocks that appear are from the following list (as found in the table on page 5):*

$$\alpha = (2p, 0, 0), \beta = (0, p, 0), \gamma = (0, 0, 2), \sigma = (\frac{p-1}{c}, 1, 0), \tau = (1, p-c, 1).$$

Proof. In this proof use the notation in the table on page 5. Suppose that

$\beta_i = (2i, p-2ci, 0)$ appears in Eq. (9), for some $i \in \{1, 2, 3, \ldots, \frac{p-1}{2c}\}$. Then we may multiply Eq. (10) through by $p-1$, and replace $(p-1)\beta_i$ with $(p-1-2ci)\beta + 2ci\sigma$, using Lemma 16 (a). Since $p-1 = (p-1-2ci)+2ci$, the result is another equation which represents the elasticity $\frac{l}{m}$, and if the process is repeated, we can iteratively eliminate all occurrences of β_i.

Similarly, suppose $\tau_j = (2j+1, p-c(2j+1), 1)$ appears in Eq. (10), for some $i \in \{1, 2, 3, \ldots, \frac{p-1}{2c}\}$. If $k(\tau_j) > 1$ then we may multiply through by $p-c$ and replace $(p-c)\tau_j$ with $j\alpha + cj\gamma + (p-c-2cj)\tau$, using Lemma 16 (b). Since $p-c > j+cj+(p-c-2cj)$, the result is an equation which represents a higher elasticity, which is impossible. If $k(\tau_j) < 1$, we can multiply through by $p-1-c$ and replace $(p-1-c)\tau_j$ with $(2cj+c)\epsilon + (p-2cj-1-2c)\beta + (\frac{p-1}{2} - cj - c)\gamma$. Since $(p-1-c) < (2cj+c)+(p-2cj-1-2c)+(\frac{p-1}{2}-cj-c)$, we would again obtain an equation that represents a higher elasticity. Therefore, τ_j does not appear in the equation.

We can also eliminate any copies of ϵ by means of similar methods and using the relation found in Lemma 16 (d).

Finally, suppose that δ appears in Eq. (10). In this case, we use Lemma 16 (e) to eliminate all occurrences of δ.

It is important to note that whenever an irreducible block σ_i, τ_j, ϵ, or δ is eliminated from Eq. (10), it is being replaced with elements from the list $\alpha, \beta, \gamma, \sigma, \tau$ only. Therefore, the process of eliminating all blocks other than the ones on the list does indeed have an end. □

Continuing the proof of Theorem 14, note that Eq. (10) is of the form Δ_v, for a suitable $v \in \ker(B) \cap \mathbb{Z}^m$. According to Lemma 18, we may assume that the support of v is contained in the set of indices which correspond to the $\alpha, \beta, \gamma, \sigma$, and τ columns of B. Now, by the same reasoning as in the proof of Theorem 9, we know that there must be a circuit u of B, *whose support is contained in* $\text{supp}(v)$, such that

$$\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) = \rho(\lambda_u).$$

Since the support of a circuit is minimal (see Definition 7), it can be verified that the equations in parts (f), (g), and of Lemma 16, Eq. (7), and Eq. (8) of Lemma 15, form the *complete list* of equations of the form Δ_u, where u is a circuit of B whose support is contained in the set of indices which correspond to the $\alpha, \beta, \gamma, \sigma$, and τ columns of B. Simple computations then show that equations Eq. (7) and Eq. (8) of

Lemma 15 are the ones which represent the largest elasticities, namely $\frac{c(2p+1-2c)}{p+c-1}$ when $p > (2c-1)^2$ and $\frac{2cp}{p+2c-1}$ when $p < (2c-1)^2$. This completes the proof of parts (a) and (b) of Theorem 14.

The following lemma records a few relations among the irreducible blocks in $\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})$, in case $p \equiv -1 (\text{mod } 2c)$ and $p > 2c-1$.

Lemma 19. *Let $\alpha, \beta, \gamma, \delta, \sigma, \beta_i, \tau, \tau_j$, and ϵ be as in the table on page 6. Then the following equations hold:*

(a) $(p-(2c-1))\beta_t = (p-(2c-1)-2ct)\beta + 2ct\sigma$
(b) $(2c-1)\sigma_t = t\alpha + (2c-1-t)\sigma$
(c) $(p-c)\tau_t = t\alpha + ct\gamma + (p-c-2ct)\tau$
(d) $(p+1-c)\tau_t = (2ct+c)\epsilon + (p-2ct+1-2c)\beta + (\frac{p+1}{2} - ct - c)\gamma$
(e) $2(c-1)\epsilon_t = t\alpha + t\gamma + 2(c-1-t)\epsilon$
(f) $2(2c-1)\epsilon = \alpha + (2c-1)\gamma + 2(c-1)\sigma$
(g) $2\delta = \alpha + \gamma$
(h) $2cp\sigma = (p+1-2c)\alpha + 2c(2c-1)\beta$
(i) $2p\tau = \alpha + 2(p-c)\beta + p\gamma$
(j) $2(p+1-2c)\tau = 2(p+1-3c)\beta + (p+1-2c)\gamma + 2c\sigma$

Lemma 20. *Eq. (10) may be replaced with an equation in which the only irreducible blocks that appear are from the following list (as on page 6):*

$$\alpha = (2p, 0, 0), \beta = (0, p, 0), \gamma = (0, 0, 2), \sigma = (\frac{p+1-2c}{c}, 2c-1, 0), \tau = (1, p-c, 1).$$

Proof. The proof of this Lemma is nearly identical to that of Lemma 18. □

Now, similar to the case where $p \equiv 1 (\text{mod } 2c)$, we can use Definition 7 along with Eq. (9) and parts (h), (i), and (j) of Lemma 19 to prove part (c) of Theorem 14.

Part (d) of Theorem 14 is the very special case where $p = 2c-1$. The monoid for this case turns out to be $\mathcal{B}(\mathbb{Z}_{2p}, \{1, 2, p\})$ and as the following table shows, all of the blocks in this monoid have cross number equal to 1.

irreducible blocks	cross numbers
$\alpha := (2p, 0, 0)$	1
$\beta := (0, p, 0)$	1
$\gamma := (0, 0, 2)$	1
$\beta_1 := (2, p-1, 0)$	1
$\beta_2 := (4, p-2, 0)$	1
$\beta_3 := (6, p-3, 0)$	1
$\vdots$	
$\beta_p \equiv \alpha := (2p, 0, 0)$	1
$\tau \equiv \tau_0 := (1, \frac{p-1}{2}, 1)$	1
$\tau_1 := (3, \frac{p-3}{2}, 1)$	1
$\tau_2 := (5, \frac{p-5}{2}, 1)$	1
$\vdots$	
$\tau_{\frac{p-1}{2}} \equiv \delta := (p, 0, 1)$	1

It is well known (see [CS2], for example) that when the cross number of every irreducible block in a monoid is 1, the monoid has elasticity 1. This proves part (d) and completes the proof of Theorem 14.

APPLICATION

Before our main theorem had a proof, the following fact was a conjecture gleaned from numerous computer-generated examples.

Theorem 21. *For* $p \equiv 3(mod\ 4)$

$$\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{\frac{3p+1}{2}, 2, p\})) = \rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2+p, 2, p\})) = \frac{2p-1}{p}$$

Proof. Note that $\frac{3p+1}{2} = \frac{2p+p+1}{2} = p + \frac{p+1}{2} = p + 2(\frac{p+1}{4})$. This is of the form $p + 2c$, So let $c = \frac{p+1}{4}$. We leave it to the reader to verify that $c = \frac{p+1}{4}$ is an integer and that $p \equiv -1 \bmod 2c$. Since $p \equiv -1 \bmod 2c$, we may use part (c) of our main theorem:

$$\rho(\mathcal{B}(\mathbb{Z}_{2p}, \{2c+p, 2, p\})) = \frac{c(2p-1)}{p + (4c-1)(c-1)}$$

if $p \equiv -1(\bmod 2c)$ and $p > 2c-1$. We simply make the substitution $c = \frac{p+1}{4}$. Observe:

$$\frac{c(2p-1)}{p+(4c-1)(c-1)} = \frac{\frac{p+1}{4}(2p-1)}{p + (4\frac{p+1}{4} - 1)(\frac{p+1}{4} - 1)} = \frac{(p+1)(2p-1)}{4p + p(p-3)} = \frac{(p+1)(2p-1)}{(p+1)p} = \frac{2p-1}{p}.$$

□

ACKNOWLEDGEMENTS

I would like to thank the UW-L College of Science and Health for funding the 2007 Dean's Distinguished Summer Fellowship program, during which most of this research was done.

REFERENCES

REFERENCES

[AC] D.F. Anderson, S.T. Chapman, On the Elasticities of Krull Domains with Finite Cyclic Divisor Class Group, *Communications in Algebra* 28(5) (2000), 2543-2553.

[Ca] Carlitz, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* 11: 391-392 (1960)

[CG] S.T. Chapman, A. Geroldinger, "On Cross Numbers of Minimal Zero-Sequences," *Australasian J. Comb.*, 14 (1996), 85-92.

[CG2] S.T. Chapman and A. Geroldinger, Krull monoids, their sets of lengths and associated combinatorial problems, *Factorization in Integral Domains*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker **189**(1997), 73–112.

[CGGR] S. Chapman, J. García-García, P. García-Sánchez, J. Rosales "Computing the Elasticity of a Krull Monoid," *Linear Algebra and its Applications*, 336 (2001), 191-200.

[CS1] S.T. Chapman, W.W. Smith, An Analysis Using the Zaks-Skula Constant of Element Factorizations in Dedekind Domains, *J. Algebra*, 159 (1993), 176-190.

[CS2] S.T. Chapman, W.W. Smith, On Factorization in Block Monoids Formed by $\{1, a\}$ in $\mathbb{Z}_n$, to appear in *Proc. Edinburgh Math. Soc.*

[F] R. Fossum, *The Divisor Class Group of a Krull Domain*, Springer-Verlag, New York, 1973.

[G] Grams, A.P. The distribution of prime ideals of a Dedekind domain, *Bull. Austral. Math. Soc.* 11(1974):429-441.

[Ka1] K. Kattchee "Monoids, Direct-Sum Decompositions, and Elasticity of Factorizations", Ph. D. dissertation, University of Nebraska–Lincoln, 2001.

[Ka2] K. Kattchee Monoids and direct-sum decompositions over local rings *J. Algebra* 256 (2002) 51-65

[Ka3] K. Kattchee Elasticities of Krull domains with finite divisor class group *Linear Alg. Appl.* 34 (2004) 171-185

[Ka4] K. Kattchee On factorization in Krull domains with divisor class group Z_{2k} *Arithmetical Properties of Commutative Rings and Monoids* Lecture Notes in Pure and Applied Mathematics 241 (2005) 325-336

[Ka] K. Kattchee, personal correspondence.

[Kr] U. Krause, A Characterization of Algebraic Number Fields with Cyclic Class Group of Prime Power Order, *Math Z.* 186(1984), 143-148.

[Sta] R. Stanley, "Combinatorics and Commutative Algebra, Second Edition", Birkhäuser, Boston, MA, 1996.

[Stu] B. Sturmfels, "Gröbner Bases and Convex Polytopes", University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.