Inversion of Matrices over Boolean Semirings

N. Sirasuntorn, S. Sombatboriboon and N. Udomsub

Abstract: It is well-known that a square matrix $A$ over a commutative ring $R$ with identity is invertible over $R$ if and only if $\det A$ is a multiplicatively invertible element of $R$. As a consequence, we have that a square matrix $A$ over a Boolean ring $R$ with identity 1 is invertible over $R$ if and only if $\det^+ A + \det^- A = 1$ where $\det^+ A$ and $\det^- A$ are the positive determinant and the negative determinant of $A$, respectively. This result is generalized to Boolean semirings with identity. By a Boolean semiring we mean a commutative semiring $S$ with zero in which $x^2 = x$ for all $x \in S$. By making use of Reutenauer and Sraubing’s work in 1984, we show that an $n \times n$ matrix $A$ over a Boolean semiring $S$ with identity 1 is invertible over $S$ if and only if $\det^+ A + \det^- A = 1$ and $2A_{ij}A_{ik} = 0 [2A_{ji}A_{ki} = 0]$ for all $i, j, k \in \{1, \ldots, n\}$ such that $j \neq k$.

Keywords: Boolean semiring, invertible matrix.

2000 Mathematics Subject Classification: 16Y60, 15A09.

1 Introduction

A semiring is a triple $(S, +, \cdot)$ such that $(S, +)$ and $(S, \cdot)$ are semigroups and $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$ for all $x, y, z \in S$. A semiring $(S, +, \cdot)$ is called additively [multiplicatively] commutative if $x+y = y+x [x \cdot y = y \cdot x]$ for all $x, y, z \in S$. We call $(S, +, \cdot)$ commutative if $(S, +, \cdot)$ is both additively and multiplicatively commutative. An element $0 \in S$ is called a zero of $(S, +, \cdot)$ if $x+0 = 0+x = x$ and $x \cdot 0 = 0 \cdot x = 0$ for all $x \in S$. By an identity of a semiring $(S, +, \cdot)$ we mean an element $1 \in S$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in S$. Notice that both a zero and an identity of a semiring are unique. An element $x$ of a semiring $S$ with zero $0$ [identity $1$] is said to be additively [multiplicatively] invertible in $S$ if there is an element $y \in S$ such that $x+y = y + x = 0 [xy = yx = 1]$. Such an element $y \in S$ is obviously unique.

Recall that a ring $R$ is called a Boolean ring if $x^2 = x$ for all $x \in R$. Then

Copyright © 2009 by the Mathematical Association of Thailand. All rights reserved.
every Boolean ring is commutative and \(-x = x\), that is, \(2x = 0\) for all \(x \in R\). If \(R\) is a Boolean ring with identity 1 and \(x, y \in R\) are such that \(xy = 1\), then
\[
x = x1 = x(xy) = x^2y = xy = 1.
\]
This shows that 1 is the only multiplicatively invertible element of a Boolean ring with identity 1.

**Example 1.1.** ([2], p. 120) If \(X\) is a set, \(\mathcal{P}(X)\) is the power set of \(X\), \(A + B = (A \setminus B) \cup (B \setminus A)\) and \(A \cdot B = A \cap B\) for all \(A, B \in \mathcal{P}(X)\).

Then \((\mathcal{P}(X), +, \cdot)\) is a Boolean ring having \(\emptyset\) and \(X\) as its zero and identity, respectively. We can see that \(X\) is the only multiplicatively invertible element of \((\mathcal{P}(X), +, \cdot)\).

By a **Boolean semiring** we mean a commutative semiring \(S\) with zero in which \(x^2 = x\) for all \(x \in S\). Then every Boolean ring is a Boolean semiring. In fact, Boolean semirings are a generalization of Boolean rings.

**Example 1.2.** Let \(X\) be a nonempty set. Define
\[
A + B = A \cup B \quad \text{and} \quad A \cdot B = A \cap B \quad \text{for all} \quad A, B \in \mathcal{P}(X).
\]

Then \((\mathcal{P}(X), +, \cdot)\) is clearly a Boolean semiring having \(\emptyset\) and \(X\) as its zero and identity, respectively. We can see that \(\emptyset\) is the only additively invertible element of \((\mathcal{P}(X), +, \cdot)\). Then \((\mathcal{P}(X), +, \cdot)\) is not a Boolean ring. Also, \(A + A = A\) for all \(A \in \mathcal{P}(X)\).

**Example 1.3.** Let \(S = \{0\} \cup \left[\frac{1}{2}, 1\right]\) and define
\[
\begin{align*}
  x \oplus 0 &= 0 \oplus x = x \quad \text{for all} \quad x \in S, \\
  x \oplus y &= \frac{1}{2} \quad \text{for all} \quad x, y \in \left[\frac{1}{2}, 1\right], \\
  x \odot y &= \min\{x, y\} \quad \text{for all} \quad x, y \in S.
\end{align*}
\]

It is straightforward to show that \((S, \oplus, \odot)\) is a Boolean semiring with zero \(0\) and identity 1. Moreover, 0 is the only additively invertible element of the semiring \((S, \oplus, \odot)\) and for \(x \in S\), \(x \oplus x = x\) if and only if either \(x = 0\) or \(x = \frac{1}{2}\).

Let \(S\) be a commutative semiring with zero 0 and identity 1 \(\neq 0\), \(n\) a positive integer and \(M_n(S)\) the set of all \(n \times n\) matrices over \(S\). Then under usual matrix addition and matrix multiplication, \(M_n(S)\) is an additively commutative semiring. The \(n \times n\) zero matrix and the \(n \times n\) identity matrix over \(S\) are the zero and the identity of \(M_n(S)\), respectively. If \(n > 1\), then \(M_n(S)\) is not multiplicatively commutative. For \(A \in M_n(S)\) and \(i, j \in \{1, \ldots, n\}\), let \(A_{ij}\) be the entry of \(A\) in the \(i\)th row and \(j\)th column. The transpose of \(A\) will be denoted by \(A^t\), that
is, $A_{ij} = A_{ji}$ for all $i, j \in \{1, \ldots, n\}$. Then for all $A, B \in M_n(S)$, $(A^t)^t = A$, $(A + B)^t = A^t + B^t$ and $(AB)^t = B^t A^t$. A matrix $A \in M_n(S)$ is called invertible over $S$ if $AB = BA = I_n$ for some $B \in M_n(S)$ where $I_n$ is the $n \times n$ identity matrix over $S$. Notice that $B$ is unique. Also, for $A \in M_n(S)$, $A$ is invertible over $S$ if and only if $A^t$ is invertible over $S$. In 1963, Rutherford [4] characterized invertible matrices over a Boolean algebra of 2 elements.

Let $S_n$ be the symmetric group of degree $n \geq 2$, $A_n$ the alternating group of degree $n$ and $B_n = S_n \setminus A_n$, that is,

\[ A_n = \{ \sigma \in S_n \mid \sigma \text{ is an even permutation} \}, \]
\[ B_n = \{ \sigma \in S_n \mid \sigma \text{ is an odd permutation} \}. \]

If $S$ is a commutative semiring with zero and identity and $n$ a positive integer greater than 1, then for $A \in M_n(S)$, the positive determinant and the negative determinant of $A$ are defined respectively by

\[ \det^+ A = \sum_{\sigma \in A_n} \left( \prod_{i=1}^n A_{\sigma(i)} \right), \]
\[ \det^- A = \sum_{\sigma \in B_n} \left( \prod_{i=1}^n A_{\sigma(i)} \right). \]

If $S$ is a commutative ring with identity, then for $A \in M_n(S)$, $\det A = \det^+ A - \det^- A$. Hence if $S$ is a Boolean ring with identity, then $\det A = \det^+ A + \det^- A$ for all $A \in M_n(S)$.

We can see that

\[ A_n = \{ \sigma^{-1} \mid \sigma \in A_n \} \quad \text{and} \quad B_n = \{ \sigma^{-1} \mid \sigma \in B_n \}, \]
\[ \det^+ I_n = 1 \quad \text{and} \quad \det^- I_n = 0 \quad \text{and} \quad \text{for} \ A \in M_n(S), \]
\[ \det^+ (A^t) = \sum_{\sigma \in A_n} \left( \prod_{i=1}^n A_{\sigma(i)}^t \right) \]
\[ = \sum_{\sigma \in A_n} \left( \prod_{i=1}^n A_{\sigma(i), i} \right) \]
\[ = \sum_{\sigma \in A_n} \left( \prod_{i=1}^n A_{\sigma^{-1}(i), i} \right) \]
\[ = \sum_{\sigma \in A_n} \left( \prod_{i=1}^n A_{\sigma^{-1}(i), \sigma^{-1}(i)} \right) \]
\[ = \sum_{\sigma \in A_n} \left( \prod_{i=1}^n A_{\sigma(i)} \right) \quad \text{since} \ \{ \sigma^{-1}(1), \ldots, \sigma^{-1}(n) \} = \{1, \ldots, n\} \]
\[ = \det^+ A. \]
It can be shown similarly that $\det^-(A^t) = \det^- A$.

In 1985, Reutenauer and Straubing [3] gave the following significant results.

**Theorem 1.4.** ([3]) Let $S$ be a commutative semiring with zero and identity and $n$ a positive integer $\geq 2$. If $A, B \in M_n(S)$, then there is an element $r \in S$ such that

\[
\det^+(AB) = (\det^+ A)(\det^+ B) + (\det^- A)(\det^- B) + r,
\]

\[
\det^-(AB) = (\det^+ A)(\det^- B) + (\det^- A)(\det^+ B) + r.
\]

**Theorem 1.5.** ([3]) Let $S$ be a commutative semiring with zero and identity and $n$ a positive integer. For $A, B \in M_n(S)$, if $AB = I_n$, then $BA = I_n$.

It is well-known that for a square matrix $A$ over a field $F$, $A$ is invertible over $F$ if and only if $\det A \neq 0$. The following known theorem is a generalization of this fact.

**Theorem 1.6.** ([1], p.160) Let $R$ be a commutative ring with identity. A square matrix $A$ over $R$ is invertible over $R$ if and only if $\det A$ is a multiplicatively invertible element of $R$.

By the properties of a Boolean ring with identity mentioned above, the following result is a direct consequence of Theorem 1.6.

**Corollary 1.7.** Let $R$ be a Boolean ring with identity 1 and $n$ a positive integer $\geq 2$. An $n \times n$ matrix $A$ over $R$ is invertible over $R$ if and only if $\det^+ A + \det^- A = 1$.

The purpose of this research is to generalize Corollary 1.7 to Boolean semirings with identity 1. We show that for a positive integer $n \geq 2$, an $n \times n$ matrix over a Boolean semiring with identity 1 is invertible if and only if

(i) $\det^+ A + \det^- A = 1$ and

(ii) $2A_{ij}A_{ik} = 0$ for all $i, j, k \in \{1, \ldots, n\}$ such that $j \neq k$.

The condition (ii) may be replaced by

(ii)' $2A_{ji}A_{ki} = 0$ for all $i, j, k \in \{1, \ldots, n\}$ such that $j \neq k$.

2 Invertible Matrices over Boolean Semirings

For a set $X$, $|X|$ denotes the cardinality of $X$.

In the remainder of this paper, let $n$ be a positive integer greater than 1. Recall that $|S_n| = n!$, $|A_n| = \frac{n!}{2}$, $|B_n| = \frac{n!}{3}$ and $\sigma A_n = B_n$ for all $\sigma \in B_n$.

The following lemma is needed.

**Lemma 2.1.** For distinct $i, j \in \{1, 2, \ldots, n\}$, \{$(\sigma(i), \sigma(j)) \sigma | \sigma \in A_n$\} = $B_n$. 

Proof. Let \( i, j \in \{1, \ldots, n\} \) be distinct. If \( \sigma \in \mathcal{A}_n \), then \( (\sigma(i) \sigma(j)) \in \mathcal{B}_n \), so \( \{(\sigma(i) \sigma(j)) \sigma \mid \sigma \in \mathcal{A}_n\} \subseteq \mathcal{B}_n \). Assume that \( \sigma_1, \sigma_2 \in \mathcal{A}_n \) and \( \sigma_1 \neq \sigma_2 \).

Case 1 : \( (\sigma_1(i) \sigma_1(j)) = (\sigma_2(i) \sigma_2(j)) \). By the cancellation property of \( \mathcal{S}_n \), we have \( (\sigma_1(i) \sigma_1(j)) \sigma_1 \neq (\sigma_2(i) \sigma_2(j)) \sigma_2 \).

Case 2 : \( (\sigma_1(i) \sigma_1(j)) \neq (\sigma_2(i) \sigma_2(j)) \). Then \( \{\sigma_1(i), \sigma_1(j)\} \neq \{\sigma_2(i), \sigma_2(j)\} \). We may assume without loss of generality that \( \sigma_1(i) \notin \{\sigma_2(i), \sigma_2(j)\} \). Then \( \sigma_1(i) \neq \sigma_2(i) \), so

\[
(\sigma_1(i) \sigma_1(j)) \sigma_1 = \sigma_1(i) = (\sigma_2(i) \sigma_2(j)) \sigma_2.
\]

This implies that \( (\sigma_1(i) \sigma_1(j)) \sigma_1 \neq (\sigma_2(i) \sigma_2(j)) \sigma_2 \).

This shows that \( \{(\sigma(i) \sigma(j)) \sigma \mid \sigma \in \mathcal{A}_n\} = |\mathcal{A}_n| = |\mathcal{B}_n| \). But since \( \{(\sigma(i) \sigma(j)) \sigma \mid \sigma \in \mathcal{A}_n\} \subseteq \mathcal{B}_n \), the equality holds, as desired. \( \Box \)

The following general properties of Boolean semirings are needed.

Lemma 2.2. Let \( S \) be a Boolean semiring. The following statements hold.

(i) For all \( x \in S \), \( 2x = 4x \).
(ii) If \( x \in S \) is an additively invertible element of \( S \), then \( 2x = 0 \).
(iii) If \( S \) has an identity \( 1 \), then \( 1 \) is the only multiplicatively invertible element of \( S \).

Proof. (i) If \( x \in S \), then \( 2x = x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x = 4x \).

(ii) Let \( x, y \in S \) be such that \( x + y = 0 \). Then \( 2x + 2y = 0 \). Since \( 4x = 2x \) by (i), we have

\[
2x = 2x + 0 = 2x + 2x + 2y = 4x + 2y = 2x + 2y = 0.
\]

(iii) The same proof is given for Boolean rings in Section 1. \( \Box \)

Lemma 2.3. Let \( S \) be a commutative semiring with zero \( 0 \) and identity \( 1 \). For \( A \in M_n(S) \), if \( A \) is invertible over \( S \), then \( A_{ij}A_{ik} \) is additively invertible in \( S \) for \( i, j, k \in \{1, \ldots, n\} \) such that \( j \neq k \).

Proof. It is clear that if \( a_1, \ldots, a_m \in S \) are additively invertible in \( S \), then so is \( c_1a_1 + \cdots + c_ma_m \) for all \( c_1, \ldots, c_m \in S \).

Let \( B \in M_n(S) \) be such that \( AB = BA = I_n \). Then for distinct \( p, q \in \{1, \ldots, n\} \),

\[
0 = (I_n)_{pq} = (BA)_{pq} = \sum_{l=1}^n B_{pl}A_{lq}.
\]
which implies that $B_{pl}A_{lq}$ is additively invertible in $S$ for all $p, q, l \in \{1, \ldots, n\}$ such that $p \neq q$. Let $i, j, k \in \{1, \ldots, n\}$ be such that $j \neq k$. Then

$$A_{ij}A_{ik} = A_{ij}A_{ik}(AB)_{ii}$$

$$= A_{ij}A_{ik}\left(\sum_{l=1}^{n} A_{il}B_{li}\right)$$

$$= A_{ik}^2(B_{ki}A_{ij}) + \sum_{\{l \neq i, l \neq k\}}^{n} A_{ij}A_{il}(B_{li}A_{ik}).$$

But $B_{ki}A_{ij}, B_{i1}A_{ik}, \ldots, B_{k-1,i}A_{ik}, B_{k+1,i}A_{ik}, \ldots, B_{ni}A_{ik}$ are additively invertible in $S$, so it follows that $A_{ij}A_{ik}$ is additively invertible in $S$.

**Theorem 2.4.** Let $S$ be a Boolean semiring with identity $1$ and $A \in M_n(S)$. Then $A$ is invertible over $S$ if and only if

(i) $\det^+ A + \det^- A = 1$ and

(ii) $2A_{ij}A_{ik} = 0$ for all $i, j, k \in \{1, \ldots, n\}$ such that $j \neq k$.

**Proof.** Assume that $A$ is invertible over $S$. Then $AB = BA = I_n$ for some $B \in M_n(S)$. By Theorem 1.4, there is an element $r \in S$ such that

$$\det^+(AB) = (\det^+ A)(\det^+ B) + (\det^- A)(\det^- B) + r,$$

$$\det^-(AB) = (\det^+ A)(\det^- B) + (\det^- A)(\det^+ B) + r.$$

Since $\det^+(AB) = \det^+(I_n) = 1$ and $\det^-(AB) = \det^-(I_n) = 0$, it follows that

$$\det^+(A)(\det^+ B) + (\det^- A)(\det^- B) + r = 1,$$

$$\det^+(A)(\det^- B) + (\det^- A)(\det^+ B) + r = 0. \quad (2)$$

Then (1)+(2) gives

$$(\det^+ A)(\det^+ B) + (\det^- A)(\det^- B) + (\det^+ A)(\det^- B) + (\det^- A)(\det^+ B) + 2r = 1$$

which implies that

$$(\det^+ A + \det^- A)(\det^+ B + \det^- B) + 2r = 1. \quad (3)$$

From (2), we have that $r$ is an additively invertible element of $S$, so by Lemma 2.2 (ii), $2r = 0$. It follows from (3) that

$$(\det^+ A + \det^- A)(\det^+ B + \det^- B) = 1. \quad (4)$$

Lemma 2.2 (iii) and (4) yield $\det^+ A + \det^- A = 1$. Thus (i) holds. Since $A$ is invertible over $S$, (ii) is obtained by Lemma 2.2(ii) and Lemma 2.3.
Conversely, assume that (i) and (ii) hold. Define $B \in M_n(S)$ by

$$B_{ij} = \sum_{\sigma \in S_n \atop \sigma(j) = i} \left( \prod_{k=1 \atop k \neq j}^{n} A_{k\sigma(k)} \right)$$

for all $i, j \in \{1, \ldots, n\}$. Claim that $AB = I_n$. If $i, j \in \{1, \ldots, n\}$, then

$$(AB)_{ij} = \sum_{t=1}^{n} A_{it} B_{tj}$$

$$= \sum_{t=1}^{n} A_{it} \left( \sum_{\sigma \in S_n \atop \sigma(j) = t} \left( \prod_{k=1 \atop k \neq j}^{n} A_{k\sigma(k)} \right) \right)$$

$$= \sum_{\sigma \in S_n \atop \sigma(j) = 1} A_{i1} \left( \prod_{k=1 \atop k \neq j}^{n} A_{k\sigma(k)} \right) + \cdots + \sum_{\sigma \in S_n \atop \sigma(j) = n} A_{in} \left( \prod_{k=1 \atop k \neq j}^{n} A_{k\sigma(k)} \right). \tag{5}$$

It is clear that $S_n = \{ \sigma \in S_n \mid \sigma(j) = 1 \} \cup \{ \sigma \in S_n \mid \sigma(j) = 2 \} \cup \cdots \cup \{ \sigma \in S_n \mid \sigma(j) = n \}$ which is a disjoint union. Then (5) gives

$$(AB)_{ij} = \sum_{\sigma \in S_n} A_{i\sigma(j)} \left( \prod_{k=1 \atop k \neq j}^{n} A_{k\sigma(k)} \right). \tag{6}$$

**Case 1 :** $i = j$. Then from (6), we have

$$(AB)_{ij} = \sum_{\sigma \in S_n} A_{i\sigma(i)} \left( \prod_{k=1 \atop k \neq i}^{n} A_{k\sigma(k)} \right)$$

$$= \sum_{\sigma \in S_n} \left( \prod_{k=1 \atop k \neq i}^{n} A_{k\sigma(k)} \right)$$

$$= \sum_{\sigma \in A_n} \left( \prod_{k=1}^{n} A_{k\sigma(k)} \right) + \sum_{\sigma \in B_n} \left( \prod_{k=1}^{n} A_{k\sigma(k)} \right)$$

$$= \det^+ A + \det^- A = 1.$$

**Case 2 :** $i \neq j$ and $n = 2$. Then either $i = 1$ and $j = 2$ or $i = 2$ and $j = 1$. Note that $S_2 = \{(1, 1), (1, 2)\}$. It follows from (6) and (ii) that

$$(AB)_{12} = A_{12}A_{11} + A_{11}A_{12} = 2A_{11}A_{12} = 0,$$

$$(AB)_{21} = A_{21}A_{22} + A_{22}A_{21} = 2A_{21}A_{22} = 0.$$
Case 3: \( i \neq j \) and \( n > 2 \). It follows from (6) that

\[
(AB)_{ij} = \sum_{\sigma \in A_n} A_{i\sigma(j)} A_{i\sigma(i)} \left( \prod_{k=1 \atop k \neq i,j} A_{k\sigma(k)} \right)
\]

\[
= \sum_{\sigma \in A_n} A_{i\sigma(j)} A_{i\sigma(i)} \left( \prod_{k=1 \atop k \neq i,j} A_{k\sigma(k)} \right) + \sum_{\sigma \in B_n} A_{i\sigma(j)} A_{i\sigma(i)} \left( \prod_{k=1 \atop k \neq i,j} A_{k\sigma(k)} \right).
\]

(7)

For each \( \sigma \in A_n \) let \( \bar{\sigma} = (\sigma(i) \sigma(j)) \sigma \). By Lemma 2.1 and (7), we have

\[
(AB)_{ij} = \sum_{\sigma \in A_n} \left( A_{i\sigma(j)} A_{i\sigma(i)} \left( \prod_{k=1 \atop k \neq i,j} A_{k\sigma(k)} \right) + A_{i\sigma(j)} A_{i\bar{\sigma}(i)} \left( \prod_{k=1 \atop k \neq i,j} A_{k\bar{\sigma}(k)} \right) \right).
\]

(8)

But for every \( \sigma \in A_n \), \( \bar{\sigma}(i) = (\sigma(i) \sigma(j)) \sigma(i) = \sigma(j) \), \( \bar{\sigma}(j) = (\sigma(i) \sigma(j)) \sigma(j) = \sigma(i) \) and for \( k \in \{1, \ldots, n\} \setminus \{i, j\} \), \( \bar{\sigma}(k) = (\sigma(i) \sigma(j)) \sigma(k) = \sigma(k) \), so it follows from (8) and (ii) that

\[
(AB)_{ij} = \sum_{\sigma \in A_n} 2A_{i\sigma(j)} A_{i\sigma(i)} \left( \prod_{k=1 \atop k \neq i,j} A_{k\sigma(k)} \right) = 0.
\]

This proves that \( AB = I_n \). By Theorem 1.5, \( BA = I_n \). Hence \( A \) is invertible over \( S \).

As mentioned previously, \( \det^+ A^t = \det^+ A \), \( \det^- A^t = \det^- A \) and \( A \) is invertible over \( S \) if and only if \( A^t \) is invertible over \( S \). Then as a consequence of Theorem 2.4, we have

Corollary 2.5. Let \( S \) be a Boolean semiring with identity \( 1 \) and \( A \in M_n(S) \). Then \( A \) is invertible over \( S \) if and only if

(i) \( \det^+ A + \det^- A = 1 \) and

(ii) \( 2A_{ji}A_{ki} = 0 \) for all \( i, j, k \in \{1, \ldots, n\} \) such that \( j \neq k \).

References

Inversion of Matrices over Boolean Semirings


(Received 5 June 2009)

N. Sirasuntorn and S. Sombatboriboon
Chulalongkorn University
Department of Mathematics
Faculty of Science
Bangkok 10330, Thailand.
e-mail: n.sirasuntorn@gmail.com

N. Udomsub
Rambhai Barni Rajabhat University
Department of Mathematics and Statistics
Faculty of Science and Technology
Chantaburi 22000, Thailand
email: ppmathschula@yahoo.co.th