Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Digital Near-Rings over the Galois Field GF (2) and Their Applications to Logic Circuits, Finite Automata, and Cryptography

K.V Rama Rao[1], K.Anuradha[2]

[1]Professor [2]Asst Professor
Department of Mathematics
RK College of Engineering, Vijayawada Andhra Pradesh

Abstract
This paper introduces the concept of **digital near-rings** defined over the Galois field GF(2) = {0, 1}, the algebraic foundation of digital electronics. We investigate the algebraic properties of finite digital near-rings, construct several examples, derive their **Cayley tables**, and study their **ideals and homomorphisms**. Applications to **logic circuits, finite automata, cryptography, and coding theory** are presented. The work demonstrates that digital near-rings provide a unified mathematical framework for binary computation and secure information processing.

Keywords
Digital Near-Ring, Galois Field, GF(2), Binary Algebra, Logic Gates, Finite Automata, Cryptography, Digital Electronics.

1. Introduction

Digital electronics rests on a two-element universe {0, 1}. Every gate, register and state transition is ultimately a map on binary tuples. The classical algebraic model for this universe is the **Galois field GF(2)**, in which addition is the exclusive-or operation and multiplication is conjunction. While GF(2) explains linear binary behaviour extremely well, a large part of digital practice is deliberately **nonlinear**: feedback functions, S-boxes, state-transition maps and control logic obey only one distributive law, not both.
A **near-ring** is precisely the algebraic structure obtained when one distributive law is dropped. It therefore models nonlinear binary behaviour more faithfully than a field does. In this paper we define and study **digital near-rings**: near-rings whose underlying set is GF(2) or a finite power of it, with the additive group generated by XOR.

Research Contributions

This paper introduces:

1. **A formal definition of digital near-rings over GF(2)**
2. **A classification of the digital near-rings on the two-element set**
3. **Binary Cayley table constructions and verification algorithms**
4. **Applications to logic circuits, finite automata and coding theory**
5. **Near-ring based cryptographic primitives**

2. Literature Review

The theory of near-rings was systematised by Pilz, who established the structure theory, the notions of N-groups, ideals and the radical theory of near-rings. Smith developed the links between near-rings and the groups from which they arise, in particular the near-ring of all self-maps of a group under pointwise addition and composition.

On the applied side, Lidl and Niederreiter give the standard account of finite fields and their use in coding theory and cryptography, while Stinson develops the cryptographic use of GF(2)-linear and nonlinear transformations. Hopcroft, Motwani and Ullman formalise finite automata as transition maps on finite state sets, and Mano and Ciletti, together with Brown and Vranesic, describe the gate-level behaviour of combinational and sequential circuits.

What is missing from this literature is an explicit algebraic bridge: the near-ring structures studied abstractly are rarely specialised to the two-element carrier that digital engineering actually uses, and the digital-design literature rarely names the algebraic object it is manipulating. The present work supplies that bridge.

3. Preliminaries

3.1 Binary Algebra

Let $B = \{0, 1\}$. The elementary binary operations are conjunction (AND, written $a \cdot b$), disjunction (OR, written $a \vee b$), exclusive-or (XOR, written $a \oplus b$) and complementation (NOT, written $a' = 1 \oplus a$). Every function from B^n to B can be written using these operations.

3.2 The Galois Field GF(2)

GF(2) is the set $\{0, 1\}$ with addition $\oplus$ (XOR) and multiplication $\cdot$ (AND). It is the unique field of order two: $(GF(2), \oplus)$ is a group with identity 0 in which every element is its own inverse, and $(GF(2) \setminus \{0\}, \cdot)$ is the trivial multiplicative group.

3.3 Near-Rings

A **right near-ring** is a triple $(N, +, \cdot)$ such that $(N, +)$ is a group (not necessarily abelian), $(N, \cdot)$ is a semigroup, and only the right distributive law is required to hold:

$$(a + b)\cdot c = a\cdot c + b\cdot c \quad \text{for all } a, b, c \in N$$

The left distributive law $a\cdot(b + c) = a\cdot b + a\cdot c$ is not assumed. A near-ring in which both laws hold is exactly an associative ring.

4. Digital Near-Rings over GF(2)

Definition 4.1 (Digital Near-Ring)

A digital near-ring is an algebraic structure

$$(N, +, \cdot)$$

where

- $N = \{0, 1\}$;
- $(N, +)$ is a group under XOR;

- multiplication is a binary operation on N;
- only one distributive law is required.

Example 4.1
Addition (XOR)

+	**0**	**1**
0	0	1
1	1	0

Multiplication (AND)

·	**0**	**1**
0	0	0
1	0	1

These operations form the field GF(2), which also serves as the simplest digital near-ring: both distributive laws happen to hold, so GF(2) is a degenerate — but perfectly valid — member of the class.

5. Construction of Digital Near-Rings

Fix the additive group $(N, \oplus) = C_2$ and let the multiplication be an arbitrary associative binary operation $\mu : N \times N \to N$ satisfying right distributivity. There are exactly four maps on $\{0,1\}$ in each variable, and the constraints eliminate most of them. The surviving multiplications are:

1. **Zero multiplication:** $a \cdot b = 0$ for all a, b.
2. **AND multiplication:** $a \cdot b = a \wedge b$.
3. **Left projection:** $a \cdot b = a$.
4. **Right projection:** $a \cdot b = b$.

Each of these yields a digital near-ring on GF(2); only the AND multiplication yields a field. The projection near-rings are the genuinely non-ring examples, since for the left projection $a \cdot (b \oplus c) = a$ while $a \cdot b \oplus a \cdot c = 0$, so left distributivity fails whenever $a = 1$.

Definition 5.1 (Digital Near-Ring of Degree n)
Let $N = GF(2)^n$ with componentwise XOR as addition, and let $f : GF(2)^n \times GF(2)^n \to GF(2)^n$ be right distributive and associative. Then $(GF(2)^n, \oplus, f)$ is a digital near-ring of degree n. Taking f to be composition of Boolean self-maps recovers the classical transformation near-ring on the group C_2^n.

6. Cayley Tables

The four multiplications of Section 5 have the following Cayley tables.

Zero multiplication

·	**0**	**1**
0	0	0
1	0	0

Left projection

·	**0**	**1**
0	0	0
1	1	1

Right projection

·	**0**	**1**
0	0	1
1	0	1

Together with the AND table of Example 4.1 these exhaust the digital near-rings on the two-element set, up to the choice of multiplication.

7. Algebraic Properties

- Finiteness: every digital near-ring over GF(2) has exactly two elements.
- Additive structure: $(N, \oplus) \cong C_2$, cyclic of order two, hence abelian.
- Characteristic: 2, since $a \oplus a = 0$ for every $a \in N$.
- Idempotence: in the AND and both projection near-rings, $a \cdot a = a$ for all a.
- Zero-symmetry: the zero, AND and left-projection near-rings satisfy $0 \cdot a = 0$; the right projection does not, so it is not zero-symmetric.

8. Ideals and Homomorphisms

Definition 8.1
A subset I of a digital near-ring N is an ideal if $(I, \oplus)$ is a normal subgroup of $(N, \oplus)$, $N \cdot I \subseteq I$, and $(a \oplus i) \cdot b \ominus a \cdot b \in I$ for all $a, b \in N$ and $i \in I$.

Theorem 8.1
The only ideals of a digital near-ring over GF(2) are $\{0\}$ and N.
Proof. An ideal is in particular a subgroup of C_2, and C_2 has only the trivial subgroups. Both satisfy the remaining conditions vacuously or trivially. ■

Definition 8.2
A map $h : N \to M$ between digital near-rings is a homomorphism if $h(a \oplus b) = h(a) \oplus h(b)$ and $h(a \cdot b) = h(a) \cdot h(b)$.

Theorem 8.2
Every digital near-ring over GF(2) is simple, and every non-zero homomorphism between digital near-rings with the same multiplication is an isomorphism.
Proof. The kernel of a homomorphism is an ideal; by Theorem 8.1 it is $\{0\}$ or N. If it is N the map is zero; otherwise the map is injective, and since both sets have two elements it is bijective. ■

9. Digital Logic Circuit Applications

- Modelling the AND, OR, XOR and NOT gates as near-ring operations.
- Analysis of combinational and sequential circuits.
- Simplification of Boolean expressions.

Explicitly, with $\oplus$ as addition and $\cdot$ as multiplication: $a \wedge b = a \cdot b$, $a' = 1 \oplus a$, $a \vee b = a \oplus b \oplus a \cdot b$, and $a \oplus b$ is addition itself. A combinational circuit with n inputs is therefore a polynomial expression over the digital near-ring, and two circuits are functionally equivalent exactly when their expressions agree as near-ring terms.

10. Finite Automata Applications

- Binary state transitions.
- Transition algebra represented using near-ring operations.
- Modelling deterministic finite automata.

Let $A = (Q, \Sigma, \delta)$ be a deterministic automaton with $Q = GF(2)^n$ and $\Sigma = GF(2)$. Each input symbol σ induces a state map $\delta\sigma : Q \to Q$. Under pointwise XOR and composition these maps form a near-ring, and the reachable behaviour of the automaton is the sub-near-ring generated by $\{\delta_0, \delta_1\}$. Right distributivity corresponds to the fact that composing after a state sum distributes, while composing before it need not.

11. Cryptographic Applications

- Stream ciphers based on XOR.
- Nonlinear transformations using near-ring multiplication.
- Construction of substitution and mixing layers.

A stream cipher encrypts by $c = m \oplus k$, which is addition in the digital near-ring; involutivity of XOR gives decryption for free. Confusion is then supplied by the multiplicative part: because only one distributive law holds, near-ring multiplication is not GF(2)-linear and thus resists linear cryptanalysis in a way that pure field arithmetic does not. Substitution layers can be specified as near-ring polynomial maps on $GF(2)^n$.

12. Coding Theory Applications

- Linear binary codes over GF(2).
- Error detection and correction.
- Cyclic code construction.

A binary linear code of length n is a subgroup of $(GF(2)^n, \oplus)$, that is, an additive sub-structure of a digital near-ring of degree n. Syndrome decoding is evaluation of a near-ring homomorphism, and cyclic codes arise from the shift map, which is an additive endomorphism and hence an element of the associated transformation near-ring.

13. Algorithms for Binary Operations

Algorithm 1: Cayley Table Generation

1. Input: a binary operation μ on $N = \{0, 1\}$.
2. For each $a \in N$ and each $b \in N$, evaluate $\mu(a, b)$.
3. Write the results into a 2×2 array indexed by a and b.

4. Output: the Cayley table of μ.

Algorithm 2: Right-Distributivity Test

1. Input: operations $\oplus$ and μ on N.
2. For every triple (a, b, c) $\in N^3$, compare $\mu(a \oplus b, c)$ with $\mu(a, c) \oplus \mu(b, c)$.
3. If all eight triples agree, report that (N, $\oplus$, μ) is a right near-ring; otherwise report the failing triple.

Algorithm 3: Near-Ring Encryption Round

1. Input: message block m $\in GF(2)^n$, key block k $\in GF(2)^n$.
2. Compute $t = m \oplus k$ (additive masking).
3. Compute $c = \mu(t, k)$ using the near-ring multiplication (nonlinear mixing).
4. Output: ciphertext block c.

14. Theorems and Proofs

Theorem 1
Every digital near-ring over GF(2) is finite.
Proof. Since GF(2) contains exactly two elements, every near-ring constructed on this set is finite.

Theorem 2
The additive group of every digital near-ring over GF(2) is cyclic of order two.
Proof. The addition operation is XOR, whose Cayley table is that of the cyclic group C_2. Hence the additive structure is cyclic.

Theorem 3
The logic gates AND, OR, XOR and NOT can be represented algebraically using digital near-rings.
Proof. Each logic gate corresponds to a binary operation on {0, 1}. These operations satisfy algebraic identities that can be expressed within the digital near-ring framework: $a \wedge b = a \cdot b$, $a \oplus b$ is the additive operation, $a' = 1 \oplus a$, and $a \vee b = a \oplus b \oplus a \cdot b$.

Theorem 4
There are exactly four digital near-rings on the set {0, 1} with additive group C_2, namely those with zero, AND, left-projection and right-projection multiplication.
Proof. There are sixteen binary operations on a two-element set. Associativity removes those that are not semigroup operations, and right distributivity applied to the eight triples of N^3 removes the remainder. Exhaustive verification by Algorithm 2 leaves the four tables listed in Section 6.

Theorem 5
A digital near-ring over GF(2) is a ring if and only if its multiplication is the zero operation or the AND operation.
Proof. Both of these satisfy the left distributive law by direct check. For the left projection, $1 \cdot (1 \oplus 1) = 1 \cdot 0 = 1$ while $1 \cdot 1 \oplus 1 \cdot 1 = 0$, so left distributivity fails; the right projection fails similarly.

15. Future Research Directions

- Classification of digital near-rings of degree n over $GF(2)^n$ for small n.

- Near-ring based S-box design and its resistance to differential cryptanalysis.
- Minimisation of sequential circuits using near-ring congruences.
- Digital near-rings over GF(2^m) and their relation to composite-field arithmetic.
- Category-theoretic formulation of the automaton–near-ring correspondence.

16. Conclusion

We have defined digital near-rings over the Galois field GF(2), classified those carried by the two-element set, derived their Cayley tables, and established their basic structural properties, including simplicity and the triviality of their ideal lattice. We then showed how logic gates, deterministic finite automata, stream ciphers and binary linear codes all sit naturally inside this framework.

The essential point is that dropping one distributive law is not a loss but a gain in expressive power: it is exactly the step that lets a single algebraic object describe both the linear and the nonlinear parts of digital computation. Digital near-rings therefore provide a unified mathematical framework for binary computation and secure information processing.

References

1. G. Pilz, Near-Rings: The Theory and Its Applications, North-Holland, Amsterdam.
2. J. D. H. Smith, Near-Rings and Their Links with Groups.
3. Rudolf Lidl and Harald Niederreiter, Finite Fields, Cambridge University Press.
4. Thomas W. Hungerford, Algebra, Springer-Verlag.
5. Douglas R. Stinson, Cryptography: Theory and Practice, CRC Press.
6. John E. Hopcroft, Rajeev Motwani and Jeffrey D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley.
7. M. Morris Mano and Michael D. Ciletti, Digital Design, Pearson.
8. Stephen Brown and Zvonko Vranesic, Fundamentals of Digital Logic with Verilog Design, McGraw-Hill.