Vector space of bit vectors

Ralf Poeppel
mailto:ralf@poeppel-familie.de

2026-01-28

Abstract

This article is a supplementary documentation to the Go package `gf2vs` [4]. The package implements data types and functions for the vector space of bit vectors.

1 Introduction

Bit vectors are very common in computer science. They are used in for integers, combinatorial algorithms and cryptography. Usually bit vectors are used for logical or arithmetic operations. The vector space of bit vectors is examined relatively rarely.

Bits are based on the the finite set of integers of order 2. This set with the operations addition and multiplication modulo 2 satisfy the axioms of a field. This finite field is named Galois Field [9][1] $GF(2) = \mathbb{F}_2$. On this field there is the vector space $\mathbb{F}_2^n$.

The aim of this article is to document the properties of the vector space of bit vectors $\mathbb{F}_2^n$, as implemented in the Go package `gf2vs`. His is a brief reference of the properties collected from several sources.

2 Field $GF(2)$

2.1 Supporting Set

The supporting set of $GF(2) = \mathbb{F}_2$ is

$$\mathbb{Z}_2 = \mathbb{Z}/\mathbb{Z}2 = \{0, 1\} \subset \mathbb{Z} \tag{1}$$

the subset $\mathbb{Z}_2$ of $\mathbb{Z}$. This set is equal to $\mathbb{Z}/\mathbb{Z}2$ the cyclic set of order 2. This set hold the values of a bit in computer science. In logic we have the boolean values False $F = 0$ and True $T = 1$ [2].

2.2 Operations

The operations of $\mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}2$ are defined modulo 2 see [1] ch. 2.2.6.

The operations addition and multiplication of the field $\mathbb{F}_2$ satisfies the group axioms [10], both operations are commutative.

[1] We cite Wikipedia for reused wordings.

2.2.1 Negation

$$- : \mathbb{F}_2 \to \mathbb{F}_2, \quad -x = x, \quad -0 = 0, \quad -1 = 1. \tag{2}$$

The negation of 1 in $\mathbb{F}_2$ is computed as $(-1) \mod 2 = 1$

2.2.2 Complement

$$\neg : \mathbb{F}_2 \to \mathbb{F}_2, \quad \neg x = 1 - x, \quad \neg 0 = 1, \quad \neg 1 = 0. \tag{3}$$

2.2.3 Absolut-value

We define the mapping absolute-value $|x|$ of an element x of $\mathbb{F}_2$:

$$|x| : \mathbb{F}_2 \to \mathbb{Z}, \quad |0| = 0, \quad |1| = 1. \tag{4}$$

2.2.4 Addition

The addition is named exclusive disjunction in logic and XOR [2, 8] in computer science. The definition of addition is given in equation 5 obeying $(1 + 1) \mod 2 = 0$.

$$+ : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2, \quad 0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0, \tag{5}$$

The group axioms [1] ch. 2.2.8 for the Group $G = \mathbb{F}_2$ and the operation addition are satisfied:

Associativity
$\forall a, b, c \in G : (a + b) + c = a + (b + c)$.

Identity element $e = 0$
$\exists e \in G, \forall a \in G : e + a = a$ and $a + e = a$, $e = 0$, e is unique.

Inverse element $(-a) = a$
$\forall a \in G \;\; \exists (-a) \in G : a + (-a) = e$ and $(-a) + a = e$, e identity element, $(-a) = a$ is unique for each a.

Commutativity
$a + b = b + a$.

So $\mathbb{F}_2$ with the operation addition is an abelian group.

2.2.5 Multiplication

The multiplication is named conjunction in logic and AND [2, 12] in computer science. The multiplication is identically defined as in $\mathbb{Z}$.

$$\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2, \quad 0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1. \tag{6}$$

We may use the notation ab instead of $a \cdot b$, omitting the multiplication sign if there is no ambiguity.

The group axioms for the Group $G = \mathbb{F}_2$ and the operation multiplication are satisfied:

Associativity
$\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Identity element $e = 1$
$\exists e \in G, \forall a \in G : e \cdot a = a$ and $a \cdot e = a$, $e = 1$, e is unique.

Inverse element $a^{-1} = a$
$\forall a \in G, a \neq 0, \ \exists a^{-1} \in G : a \cdot a^{-1} = e$ and $a^{-1}b \cdot a = e$, e identity element, $a^{-1} = 1$ is the only inverse element.

Commutativity
$a \cdot b = b \cdot a$.

So $\mathbb{F}_2$ with the operation multiplication is an abelian group.

2.2.6 Disjunction

In boolean logic we have the operation disjunction, named OR in computer science [2, 13].

$$\vee : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2, \quad 0 \vee 0 = 0, \quad 0 \vee 1 = 1, \quad 1 \vee 0 = 1, \quad 1 \vee 1 = 1 \tag{7}$$

The operation $\vee$ does not satisfy the group axioms; there is no inverse element.

2.3 Field axioms

The set $K := \mathbb{F}_2$ with the operations addition and multiplication satisfies the field axioms [1] ch. 2.3.3. We use K as symbol for any field satisfying the field axioms.

K1 K with the addition + is an abelian group.

K2 $K^* := K \setminus \{0\}$ with the multiplication $\cdot$ for every element of K^* is an abelian group.

K3 distributive property [6] is satisfied $\forall a, b, c \in K$

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c, \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned} \tag{8}$$

3 Vector space $\mathbb{F}_2^n$

3.1 Vectors

Bit vectors are the elements of the vector space. We define a bit vector x of size n as a tupel (x_i) or vector x of values $x_i \in \mathbb{F}_2$:

$$x := (x_i) := (x_1, x_2, \ldots, x_n), \quad \forall x_i \in \mathbb{F}_2 \tag{9}$$

We define the set of all bit vectors of size n see [1] 2.4.1:

$$\mathbb{F}_2^n := \{x = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2\} \tag{10}$$

In addition we define two distinguished constant elements of $\mathbb{F}_2^n$:

Zero
$\mathbb{0}$ zero vector, all components are 0.

Ones
$\mathbb{1}$ ones vector, all components are 1.

3.2 Operations on vectors

We define bitwise operations on the bit vectors x, y, z see [1] 2.4.1 and [3] (1), (2), (3).

$$\left.\begin{array}{rrcr} \sim\colon \mathbb{F}_2^n \to \mathbb{F}_2^n, & \sim x = y & \Leftrightarrow & \neg x_i = y_i \\ |\,|\colon \mathbb{F}_2^n \to \mathbb{Z}^n, & |x| = y & \Leftrightarrow & x_i = y_i, \\ \oplus\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n, & x \oplus y = z & \Leftrightarrow & x_i + y_i = z_i, \\ \&\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n, & x\&y = z & \Leftrightarrow & x_i \cdot y_i = z_i, \\ |\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n, & x|y = z & \Leftrightarrow & x_i \vee y_i = z_i, \\ \cdot\colon \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^n, & \lambda \cdot x = y & \Leftrightarrow & \lambda \cdot x_i = y_i, \end{array}\right\} i = 1, \ldots, n. \tag{11}$$

We adopt the main identities from [3] (4), . . . , (14) for bit vectors of size n here:

$$x \oplus y = y \oplus x, \quad x\&y = y\&x, \quad x|y = y|x; \tag{12}$$
$$(x \oplus y) \oplus z = x \oplus (y \oplus z), \quad (x\&y)\&z = x\&(y\&z), \quad (x|y)|z = x|(y|z); \tag{13}$$
$$(x \oplus y)\&z = (x\&z) \oplus (y\&z); \tag{14}$$
$$(x\&y)|z = (x|z)\&(y|z), \quad (x|y)\&z = (x|z)\&(y|z); \tag{15}$$
$$x \oplus y = (x\&y) \oplus (x|y); \tag{16}$$
$$(x\&y)|x = x, \quad (x|y)\&x = x; \tag{17}$$
$$\sim \mathbb{0} = \mathbb{1}, \quad \sim \mathbb{1} = \mathbb{0}; \tag{18}$$
$$x \oplus \mathbb{0} = x, \quad x\&\mathbb{0} = \mathbb{0}, \quad x|\mathbb{0} = x; \tag{19}$$
$$x \oplus x = \mathbb{0}, \quad x\&x = x, \quad x|x = x; \tag{20}$$
$$x \oplus \mathbb{1} = \sim x, \quad x\&\mathbb{1} = x, \quad x|\mathbb{1} = \mathbb{1}; \tag{21}$$
$$x \oplus (\sim x) = \mathbb{1}, \quad x\&(\sim x) = \mathbb{0}, \quad x|(\sim x) = \mathbb{1}; \tag{22}$$
$$-(x \oplus y) = (\sim x) \oplus y = x \oplus (\sim y), \quad \sim (x\&y) = (\sim x)|(\sim y), \quad \sim (x|y) = (\sim x)\&(\sim y); \tag{23}$$

3.3 Axioms of vector space

The set $\mathbb{F}_2^n$ with the binary operation of vector addition $\oplus$ and the binary function of scalar multiplication $\cdot$, as given in (11), defines a vector space see [1, 15].

The axioms of a vector space are satisfied:

Associativity of vector addition
$u \oplus (v \oplus w) = (u \oplus v) \oplus w, \ \ \forall u, v, w \in \mathbb{F}_2^n$.

Commutativity of vector addition
$u \oplus v = v \oplus u, \ \ \forall u, v \in \mathbb{F}_2^n$.

Identity element of vector addition
$\exists \mathbb{0} \in \mathbb{F}_2^n : v \oplus \mathbb{0} = v, \ \ \forall v \in \mathbb{F}_2^n$.

Inverse elements of vector addition
$\forall v \in \mathbb{F}_2^n \ \ \exists -v \in \mathbb{F}_2^n : v \oplus (-v) = \mathbb{0}$, and $-v = v$, i.e. each vector is its own additive inverse.

Compatibility of scalar multiplication with field multiplication
$\lambda(\eta v) = (\lambda\eta)v, \;\; \lambda, \eta \in \mathbb{F}_2, \; v \in \mathbb{F}_2^n.$

Identity element of scalar multiplication
$1v = v, \;\; 1 \in \mathbb{F}_2, \; v \in \mathbb{F}_2^n$, where 1 is the multiplicative identity of $\mathbb{F}_2$.

Distributivity of scalar multiplication with respect to vector addition
$\lambda(u \oplus v) = \lambda u \oplus \lambda v, \;\; \lambda \in \mathbb{F}_2, \; u, v \in \mathbb{F}_2^n.$

Distributivity of scalar multiplication with respect to field addition
$(\lambda + \eta)v = \lambda v + \eta v, \;\; \lambda, \eta \in \mathbb{F}_2, \; v \in \mathbb{F}_2^n.$

In the vector space $\mathbb{F}_2^n$ we are not limited to the operations vector addition and scalar multiplication. We can use the Boolean operations as well.

Negation, Complement, Not
$\sim v = \mathbb{1} - v = \mathbb{1} \oplus v$, swap all bits.

Disjunction, Or
$u \vee v = (u_i) \vee (v_i) = (u_i \vee v_i)$, element-wise Or.

Exclusive or, Xor
$u \oplus v = u \oplus v = (u_i) \oplus (v_i) = (u_i \oplus v_i)$, element-wise Xor, equal to vector addition.

Conjunction, And
$u \wedge v = (u_i) \cdot (v_i) = (u_i \cdot v_i)$, element-wise And.

As we apply the operations element-wise, we satisfy the laws of associativity and commutativity.

3.4 Vector space base

We give here the definition of the basis, the norm and the scalar product implemented in the Go package.

Unit vector
We define the unit vectors e_i, $i = 1, \ldots, n$, of the vector space as the vectors where the ith element is $x_i = 1$ and all other elements are 0.

$e_i = (x_k)$,

$$x_k = \begin{cases} 1, & k = i, \quad \text{identity element of multiplication,} \\ 0, & k \neq i, \quad \text{identity element of addition,} \end{cases} \qquad x_k \in K, \;\; e_i \in K^n.$$

Please note the e_i are linearly independent.

We observe the unit vectors are identical to the unit vectors of the vector spaces $\mathbb{F}_2^n, \mathbb{Z}^n, \mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$, all over a field K.

Generating system
We define the subset $\mathbb{E} := \{e_i\}$, $\mathbb{E} \subset \mathbb{F}_2^n$, of unit vectors e_i. The subset $\mathbb{E}$ forms a generating system. Each vector v of $\mathbb{F}_2^n$ is a linear combination of scalars a_i and the e_i:

$$v = \sum_{i=1}^{n} a_i e_i, \;\; a_i \in \mathbb{F}_2, \;\; e_i \in \mathbb{E}, \quad \forall v \in \mathbb{F}_2^n. \tag{24}$$

Here the addition is modulo 2.

Equation (24) is used equally for each vector space on any field K using the operation addition as defined for the field K and the 1 the identity element of the operation multiplication.

Thus the subset $\mathbb{E}$ spans $\mathbb{F}_2^n$. In this vector space it is one spanning set, and the decomposition of a vector v into a linear combination of unit vectors e_i is unique.

Basis

The subset $\mathbb{E}$ is one basis of the vector space $\mathbb{F}_2^n$ as it is a basis of every vector space over a field K.

Index

We call $i = 1, \ldots, n$ the index of the unit vector e_i in the basis.

Norm

The addition in the field $\mathbb{F}_2^n$ is the addition modulo 2. Hence each summation gives one of the values 0 or 1.

$$\sum_i^n x_i = \begin{cases} 0, & n \mod 2 = 0, \quad n\ even, \\ 1, & n \mod 2 = 1, \quad n\ odd. \end{cases} \tag{25}$$

So each sum will have either the value 0 or the value 1. From this it follows we cannot use any usual definition of a norm for computing the length of a vector in $\mathbb{F}_1^n$.

If we first apply operation $|\ |$ we map a vector from $\mathbb{F}_2^n \to \mathbb{Z}$. On vectors in $\mathbb{Z}^n$ norms are defined. For example the L^1-norm [5] of a vector $\|x\|$ sometimes called absolute-value norm [14].

We define the norm as a function p of a vector $v \in \mathbb{F}_2^n$ to be its absolute-value norm using the absolute-value function (4). This is called the Hamming weight [11], see equation (26). This is the number of ones in the vector. In some programming languages like C the function is named popcount().

$$p := \|v\| : \mathbb{F}_2^n \to \mathbb{Z}, \quad p = \sum_{i=1}^{n} |v_i| \tag{26}$$

This definition is equivalent to the definition of the L^1-norm [5] of a vector $\|x\|_1$. The value of the norm is an element of the set $\{0, 1, \ldots, n\} \subset \mathbb{Z}$. Obviously this norm satisfies the axioms of a norm:

Subadditivity / Triangle inequality

$p(x + y) \leq p(x) + p(y) \ \ \forall x, y \in \mathbb{F}_2^n$,

Absolute homogeneity

$p(s \cdot x) = s \cdot p(x) \ \ \forall s \in \mathbb{F}_2, x \in \mathbb{F}_2^n$,

Positive definiteness

$p(x) = 0 \Rightarrow x = \mathbb{0}$.

Please note the norm of the unit vectors $\|e_i\| = 1, \forall i \in \{1, \ldots n\}$.

Scalar product

We define the scalar product, dot product [1, 7] or inner product of two vectors as given in equation (27):

$$<,>: \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{Z}, < x, y >= z, \|x\&y\| = \sum_i^n |x_i \cdot y_i| = z, \tag{27}$$

We can easily verify by computation the properties of the scalar product:

Distributivity

$< x \oplus x', y >=< x, y > + < x', y >,$
$< x, y \oplus y' >=< x, y > + < x, y' >,$
$< \lambda x, y >= \lambda < x, y >,$
$< x, \lambda y >= \lambda < x, y >,$

Commutativity

$< x, y >=< y, x >,$

Positive definiteness

$< x, x > \ \geq 0,$ with $< x, x >= 0$ only if $x = \mathbb{0}$,

Orthogonality

$< x, y >= 0,$ we say the two vectors are orthogonal.

Orthonormal Basis

With the properties of the norm and the scalar product it follows $\mathbb{E}$ is an orthonormal basis, and this is the only orthonormal basis of $\mathbb{F}_2^n$.

References

[1] Gerd Fischer and Boris Springborn. *Lineare Algebra: Eine Einführung für Studienanfänger*. de. 19th ed. Wiesbaden, Germany: Springer Spektrum, 2020.

[2] Donald E. Knuth. *The Art of Computer Programming, Vol 4, Fasc 0. Introduction to Combinatorical Algorithms and Boolean Functions*. Vol. 4 Fascicle 0. Addison-Wesley, 2008. URL: https://www-cs-faculty.stanford.edu/~knuth/fasc0a.ps.gz (visited on 01/17/2018).

[3] Donald E. Knuth. *The Art of Computer Programming, Vol 4, Fasc 1. Bitwise Tricks and Techniques*. Vol. 4 Fascicle 1. Addison-Wesley, 2008. URL: https://www-cs-faculty.stanford.edu/~knuth/fasc1a.ps.gz (visited on 10/08/2025).

[4] Ralf Poeppel. *Go package documentation gf2vs*. https://pkg.go.dev/github.com/rpoe/gf2vs. [Online; accessed 10-January-2026]. Jan. 6, 2026.

[5] Eric W. Weisstein. *L^1 – Norm From MathWorld–A Wolfram Resource*. https://mathworld.wolfram.com/L1-Norm.html. [Online; accessed 09-October-2025]. July 27, 2025.

[6] Wikipedia contributors. *Distributive property — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Distributive_property&oldid=1329322251. [Online; accessed 28-January-2026]. 2025.

[7] Wikipedia contributors. *Dot product — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Dot_product&oldid=1328631745. [Online; accessed 2-February-2026]. 2025.

[8] Wikipedia contributors. *Exclusive or — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Exclusive_or&oldid=1316886803. [Online; accessed 12-January-2026]. 2025.

[9] Wikipedia contributors. *Finite field — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Finite_field&oldid=1330855394. [Online; accessed 12-January-2026]. 2026.

[10] Wikipedia contributors. *Group (mathematics) — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Group_(mathematics)&oldid=1330839314. [Online; accessed 12-January-2026]. 2026.

[11] Wikipedia contributors. *Hamming weight — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Hamming_weight&oldid=1306107874. [Online; accessed 13-January-2026]. 2025.

[12] Wikipedia contributors. *Logical conjunction — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Logical_conjunction&oldid=1324909528. [Online; accessed 12-January-2026]. 2025.

[13] Wikipedia contributors. *Logical disjunction — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Logical_disjunction&oldid=1317551960. [Online; accessed 12-January-2026]. 2025.

[14] Wikipedia contributors. *Norm (mathematics) — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Norm_(mathematics)&oldid=1326013131. [Online; accessed 14-January-2026]. 2025.

[15] Wikipedia contributors. *Vector space — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Vector_space&oldid=1326882436. [Online; accessed 12-January-2026]. 2025.