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

Ralf Poeppel

mailto:ralf@poeppel-familie.de

2026-01-28

Abstract

This article is a supplementary documentation to the Go package `gf2vs` [3]. The package implements data types and functions modeling the vector space $\mathbb{F}_2^n$.

The vector space $\mathbb{F}_2^n$ of dimension n is based on the finite field of order 2, the Galois field $GF(2)$. We use $GF(2)$ to model binary values, or bits, and provide the properties of the vector space of bit vectors.

1 Field $\mathbb{F}_2$

1.1 Supporting Set

The supporting set of $GF(2) = \mathbb{F}_2$ is $S = \{0, 1\}$. This set equivalent 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].

1.2 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 [7][1], both operations are commutative.

1.2.1 Negation

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

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

1.2.2 Value

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

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

[1] We cite Wikipedia for reused wordings.

1.2.3 Addition

The addition is named exclusive disjunction in logic and XOR [2, 6] in computer science. The definition of addition is given in equation 3 obeying $(1 + 1) \mod 2 = 0$.

$$+ : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2, \quad 0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0, \tag{3}$$

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.

1.2.4 Multiplication

The multiplication is named conjunction in logic and AND [2, 9] in computer science. The multiplication is identically defined as in $\mathbb{Z}$.

$$\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2, \quad 0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1. \tag{4}$$

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.

1.2.5 Disjunction

In boolean logic we have the operation disjunction, named OR in computer science [2, 10].

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

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

1.3 Field axioms

The set $K := \mathbb{F}_2$ with the operations addition and multiplication satisfies the field axioms [1] ch. 2.3.3.

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 [5] is satisfied $\forall a, b, c \in K$

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c, \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned} \tag{6}$$

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

We define the vector space $\mathbb{F}_2^n$ over the field $\mathbb{F}_2$ as the set V of vectors v with n elements of the field, together with the binary operation of vector addition and the binary function of scalar multiplication, see (7). This definition is similar to the one in [12]. We use the notation $v := (v_i)$ for the vector v with components v_i.

$$u \oplus v = w, \;\; u, v, w \in V, \quad a \cdot v = w, \;\; a \in \mathbb{F}_2, \;\; v, w \in V. \tag{7}$$

We apply the addition element-wise and we multiply the scalar with each element of the vector.

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

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

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

The axioms of a vector space are satisfied [12]:

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
$a(bv) = (ab)v, \;\; a, b \in \mathbb{F}_2, \;\; v \in \mathbb{F}_2^n.$

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
$a(u \oplus v) = au \oplus av, \;\; a \in \mathbb{F}_2, \;\; u, v \in \mathbb{F}_2^n.$

Distributivity of scalar multiplication with respect to field addition
$(a \oplus b)v = av \oplus bv, \;\; a, b \in \mathbb{F}_2, \; v \in \mathbb{F}_2^n.$

In this vector space we are not limited to the operations vector addition and scalar multiplication. We can use the Boolean operations as well.

Complement, Not
$\overline{v} = \mathbb{1} - v = \mathbb{1} \oplus v$, 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.

We use some more definitions to cover further properties of the vector space:

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.

$$e_i = (x_k),$$
$$x_k = \begin{cases} 1, & k = i, \\ 0, & k \neq i, \end{cases} \qquad x_k \in \mathbb{F}_2, \;\; e_i \in \mathbb{F}_2^n.$$

Please note the e_i are linearly independent.

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:

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

For the summation, we can use either the algebraic addition + or the modulo 2 $\oplus$ addition.

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 $\mathbb{F}_2^n$.

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

Norm
We define the norm as a function p of a vector $v \in \mathbb{F}_2^n$ to be its Hamming weight [8], see Equation 8, i.e. the number of ones in the vector. In some programming languages like C the function is named popcount().

$$p := \parallel v \parallel : \mathbb{F}_2^n \rightarrow \mathbb{R}, \;\; p = \sum_{i=1}^{n} v_i \tag{8}$$

This definition is equivalent to the definition of the L^1-norm [4] of a vector $\| x \|_1$ sometimes called absolute-value norm [11]. The value of the norm is an element of the set $\{0, 1, \ldots, n\} \subset \mathbb{R}$. This definition is in accordance with the definition of the norm of the vector space over $\mathbb{C}$. 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 $\| e_i \| = 1, \forall i \in \{1, \ldots n\}$.

Inner product

We define the inner product or scalar product of two vectors as given in equation (9):

$$\langle u, v \rangle := \begin{cases} 0, & u \cdot v = \mathbb{0}, \\ 1, & else. \end{cases} \tag{9}$$

Orthogonality

If $\langle u, v \rangle = 0$, we say the two vectors are orthogonal. Note that the inner product of any vector with $\mathbb{0}$ is 0.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.