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

Ralf Poeppel
mailto:ralf@poeppel-familie.de

2026-01-14

Abstract

This article is a supplementary documentation to the Go package `gf2vs` [1]. 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 $GF(2)$ [4]. We use $GF(2)$ to model binary values, or bits, and consider the properties of the vector space of bit vectors.

Field $\mathbb{F}_2$

The finite field of order 2 has two elements $\mathbb{F}_2 = \{0, 1\}$ and the operations addition $+$ and multiplication $\cdot$. For the definition see equation (1).

$$\begin{array}{rllll} + : & 0+0=0, & 0+1=1, & 1+0=1, & 1+1=0, \\ \cdot : & 0\cdot 0=0, & 0\cdot 1=0, & 1\cdot 0=0, & 1\cdot 1=1. \end{array} \tag{1}$$

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

Each of the two operations of the field $\mathbb{F}_2$ satisfies the group axioms [5] for the groups $G_+ := (\mathbb{F}_2, +)$ and $G_\cdot := (\mathbb{F}_2, \cdot)$. In addition, both operations are commutative. For reference the group axioms are repeated here. We use the symbol $\circ$ to denote the binary operations $+$ or $\cdot$.

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

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

Inverse element a^{-1}
$\forall a \in G \;\; \exists b \in G : a \circ b = e$ and $b \circ a = e$, e identity element, b is unique for each a, notation $b = a^{-1}$.

Commutativity
$a \circ b = b \circ a$.

We can look at the field from an algebraic point of view or from a logical point of view. In logic the field can be seen as the Boolean values $F = 0$ and $T = 1$. The Boolean operations are disjunction $\vee$ [8], exclusive or (contravalence) $\oplus$ [3] and conjunction $\wedge$ [7]. The definitions are repeated in equation (2).

$$
\begin{array}{lllll}
\vee: & 0 \vee 0 = 0, & 0 \vee 1 = 1, & 1 \vee 0 = 1, & 1 \vee 1 = 1, \\
\oplus: & 0 \oplus 0 = 0, & 0 \oplus 1 = 1, & 1 \oplus 0 = 1, & 1 \oplus 1 = 0, \\
\wedge: & 0 \wedge 0 = 0, & 0 \wedge 1 = 0, & 1 \wedge 0 = 0, & 1 \wedge 1 = 1.
\end{array} \tag{2}
$$

Please note that the operations $\oplus$ and $\wedge$ are identically defined as $+$ and $\cdot$ and hence satisfy the group axioms.

The operation $\vee$ does not satisfy the group axioms; there is no inverse element. In the remaining chapters we will use the notation $+, \cdot, \vee$ for the operations only.

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 (3).

$$
u + v = w, \;\; u, v, w \in V, \quad a \cdot v = w, \;\; a \in \mathbb{F}_2, \;\; v, w \in V. \tag{3}
$$

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

This definition is similar to the one in [10].

We use the notation $v := (v_i)$ for the vector v with components v_i.

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 [10]:

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

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

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

Inverse elements of vector addition
: $\forall v \in \mathbb{F}_2^n \;\; \exists - v \in \mathbb{F}_2^n : v + (-v) = \mathbb{0}$, 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
: $a(u + v) = au + av, \;\; a \in \mathbb{F}_2, \;\; u, v \in \mathbb{F}_2^n$.

Distributivity of scalar multiplication with respect to field addition

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

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

$\overline{v} = \mathbb{1} - v = \mathbb{1} + v$, swap all bits.

Disjunction, Or

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

Exclusive or, Xor

$u \oplus v = u + v = (u_i) + (v_i) = (u_i + v_i)$, 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.

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

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:

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

Thus the subset $\mathbb{E}$ spans $\mathbb{F}_2^n$. In this vector space it is the only such 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 the one and only 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 $|v|$ of a vector $v \in \mathbb{F}_2^n$ to be its Hamming weight [6], i.e. the number of ones in the vector. This definition is equivalent to the definition of the L^1-norm of a vector $|x|_1$ [2] sometimes called absolute-value norm [9]. 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 $\mathbb{C}$.

Inner product

We define the inner product of two vectors to be the norm of their product:

$$\langle u, v \rangle := |u \cdot v|.$$

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.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.