Branch Number Formalization

Ben Breen

October 30, 2025

Introduction

This blueprint formalizes Theorem 1 from *A New Algorithm for Computing Branch Number of Non-Singular Matrices over Finite Fields*. We provide a verified proof that the branch number of an invertible matrix can be computed using an alternate, but equivalent definition. The branch number measures how well a linear transformation spreads information, which is essential for designing secure cryptographic systems.

Preliminaries

Let $\mathbb{F}_q$ denote a finite field of order q, where $q = p^m$ for some prime p and positive integer m. We denote by $\mathbb{F}_q^n$ the set of vectors of length n with entries from $\mathbb{F}_q$.

Definition 1 (Hamming Weight)**.** *The Hamming weight of a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, denoted by $w_h(x)$, is the total number of non-zero components in x:*

$$w_h(x) = |\{i \in \{1, 2, \ldots, n\} : x_i \neq 0\}|.$$

Definition 2 (Branch Function)**.** *For a matrix M of order n over $\mathbb{F}_q$ and a vector $x \in \mathbb{F}_q^n$, we define*

$$h(M, x) = w_h(x) + w_h(Mx).$$

Definition 3 (Differential Branch Number)**.** *The differential branch number $\mathcal{B}_d(M)$ of a matrix M of order n over the finite field $\mathbb{F}_q$ is defined as*

$$\mathcal{B}_d(M) = \min_{x \neq 0}\{w_h(x) + w_h(Mx)\}.$$

For simplicity, we refer to the differential branch number as the branch number and denote it by $\mathcal{B}(M)$.

Branch Number Theorem

Theorem 1 (Branch Number of Invertible Matrix)**.** *Let $M \in M_n(\mathbb{F}_q)$ be an invertible matrix. Then the branch number of M is given by*

$$\mathcal{B}(M) = \min\left\{\min\{h(M, x), h(M^{-1}, x)\} \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}.$$

We establish this theorem through a series of intermediate steps.

Recall that for an invertible matrix M in $M_n(\mathbb{F}_q)$, where $n > 1$, the branch number $\mathcal{B}(M)$ is given as

$$\mathcal{B}(M) = \min\{h(M, x) \mid x \in \mathbb{F}_q^n, x \neq 0\}.$$

Since $x \neq 0 \Rightarrow w_h(x) \neq 0$, we may write

$$\mathcal{B}(M) = \min\{h(M, x) \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq n\}.$$

Step 1 (Weight Partition)**.** For an invertible matrix $M \in M_n(\mathbb{F}_q)$, the branch number can be partitioned by vector weight:

$$\begin{aligned}\mathcal{B}(M) = \min\Bigg\{ &\min\left\{h(M, x) \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \\ &\min\left\{h(M, x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n\right\}\Bigg\}.\end{aligned} \tag{1}$$

Proof. We partition the set $\{1, \ldots, n\}$ into two parts: $\{1, \ldots, \lfloor (n+1)/2 \rfloor\}$ and $\{\lfloor (n+1)/2 \rfloor + 1, \ldots, n\}$, to compute $\mathcal{B}(M)$ as in (1). □

Step 2 (Partition High Weight by Image)**.** The high-weight term in (1) can be further partitioned by the weight of the image:

$$\begin{aligned}
&\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n\right\} \\
=&\min\left\{ \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n, w_h(Mx) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \right. \\
&\left. \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n, w_h(Mx) > \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \right\}.
\end{aligned} \tag{2}$$

Proof. We divide the second term on the right-hand side of (1) into cases where $w_h(Mx) \leq \lfloor (n+1)/2 \rfloor$ and $w_h(Mx) > \lfloor (n+1)/2 \rfloor$, which gives us (2) directly. □

Step 3 (High Weights Excluded)**.** Vectors with both high input weight and high output weight do not contribute to the branch number. Specifically,

$$\begin{aligned}
\mathcal{B}(M) =&\min\left\{ \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \right. \\
&\left. \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n, w_h(Mx) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \right\}.
\end{aligned} \tag{3}$$

Proof. From (1) and (2), we have:

$$\begin{aligned}
\mathcal{B}(M) = \min&\left\{ \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \right. \\
&\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n, w_h(Mx) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \\
&\left. \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n, w_h(Mx) > \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \right\}.
\end{aligned}$$

For the third term, when $w_h(x) > \lfloor (n+1)/2 \rfloor$ and $w_h(Mx) > \lfloor (n+1)/2 \rfloor$:

$$h(M,x) = w_h(x) + w_h(Mx) > 2\left\lfloor \frac{n+1}{2} \right\rfloor + 1 \geq n+1.$$

However, we know that the upper bound for $\mathcal{B}(M)$ is $n+1$. Thus, this term will not contribute to the computation of the branch number, giving us (3). □

Step 4 (Adding Extra Term)**.** We can add an extra term without affecting the branch number:

$$\begin{aligned}
\mathcal{B}(M) =&\min\left\{ \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \right. \\
&\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \leq w_h(x) \leq \left\lfloor \frac{n+1}{2} \right\rfloor, w_h(Mx) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \\
&\left. \min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \leq n, w_h(Mx) \leq \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \right\}.
\end{aligned} \tag{4}$$

Proof. We note that

$$\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor, w_h(Mx) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \subseteq$$
$$\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}.$$

Therefore,

$$\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \le$$
$$\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor, w_h(Mx) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}.$$

Since the right-hand side is always greater than or equal to the left-hand side, if we include this extra term in (3), it will not affect the minimum value, giving us (4). □

Step 5 (Matrix Inverse Substitution)**.** By merging the last two terms in (4) and substituting $y = Mx$, we can express the branch number using M^{-1}:

$$\begin{aligned}\mathcal{B}(M) = \min\Bigg\{ &\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \\ &\min\left\{h(M^{-1},y) \mid y \in \mathbb{F}_q^n, 1 \le w_h(y) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}\Bigg\}.\end{aligned} \tag{5}$$

Proof. By merging the second and third terms on the right-hand side of (4), we obtain:

$$\begin{aligned}\mathcal{B}(M) = \min\Bigg\{ &\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \\ &\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le n, w_h(Mx) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}\Bigg\}.\end{aligned}$$

Let $Mx = y$, then $x = M^{-1}y$ and $x \neq 0 \iff y \neq 0 \iff w_h(y) \ge 1$. Then $h(M,x) = h(M^{-1},y)$ and

$$\begin{aligned}\mathcal{B}(M) = \min\Bigg\{ &\min\left\{h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}, \\ &\min\left\{h(M^{-1},y) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le n, 1 \le w_h(y) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}\Bigg\}.\end{aligned}$$

We may drop the condition $1 \le w_h(x) \le n$ as this is a trivial condition for $x \neq 0$. Note that the term $x \in \mathbb{F}_q^n$ may be replaced by $y \in \mathbb{F}_q^n$ as the correspondence $x \to y$ is one-to-one, giving us (5). □

Step 6 (Efficient Formula)**.** The branch number of M can be computed efficiently as:

$$\mathcal{B}(M) = \min\left\{\min\{h(M,x), h(M^{-1},x)\} \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor\right\}. \tag{6}$$

Proof. From (5), we may rename y to x to obtain:

$$\mathcal{B}(M) = \min\left\{ \min\left\{ h(M,x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor \right\}, \right.$$
$$\left. \min\left\{ h(M^{-1},x) \mid x \in \mathbb{F}_q^n, 1 \le w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor \right\} \right\}.$$

Or, equivalently, we obtain (6). □

This completes the proof of Theorem 1.

Verification

In Step 2, the proof takes the minimum over a set of vectors. In order to take the minimum, we need to know that the set is nonempty. In this case, the set

$$\left\{ x \in \mathbb{F}_q^n \mid \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \le n, w_h(Mx) \le \left\lfloor \frac{n+1}{2} \right\rfloor \right\}$$

can be empty. Specifically, for $M = I$, the second condition becomes $w_h(Mx) = w_h(Ix) = w_h(x)$. In this case, the set becomes

$$\left\{ x \in \mathbb{F}_q^n \mid \left\lfloor \frac{n+1}{2} \right\rfloor < w_h(x) \le n, w_h(x) \le \left\lfloor \frac{n+1}{2} \right\rfloor \right\} = \emptyset$$

which is empty due to the contradictory conditions $w_h(x) \le \lfloor \frac{n+1}{2} \rfloor < w_h(x)$. This error is represented by the `sorry` on line 1606 in .