The Gate Complexity of Syndrome Decoding of Hamming Codes

J. Carmelo Interlando, Eimear Byrne, and Joachim Rosenthal

Abstract. Let $A = (a_{ij})_{k\times n}$ be a matrix with entries in the Galois field $GF(2)$, and let $x = (x_1, x_2, \ldots, x_n)^t$ be a vector of variables assuming values in $GF(2)$. The *gate complexity* of A, denoted by $\mathcal{C}(A)$, is the minimum number of XOR gates necessary to compute the matrix-vector product Ax. In this paper it is shown that $\mathcal{C}(\mathcal{H}_k) = 2^{k+1} - 2k - 2$, where $\mathcal{H}_k$ is the parity-check matrix of the $[2^k - 1, 2^k - k - 1]$ Hamming code. As a consequence, upper bounds on $\mathcal{C}(A)$ for any matrix $A = (a_{ij})_{k\times n}$, one for fixed k and another one for fixed n, are derived. As a interesting application of these results, we give a simple proof that the upper bound on the gate complexity of an $n \times n$ matrix is $2n^2/\log_2 n$.

1. Introduction

The number of operations required to compute a Boolean function is of extreme interest in complexity theory and consequently, in cryptography, in connection with one-way functions [**2, 5**]. The complexity of computing a Boolean function can be formalized by the notion of circuit size, that is, the number of gates a circuit possesses, see [**1, 7, 8**].

This work focuses exclusively on Boolean functions in $LB_{n,k}$, the set of all linear transformations from $GF(2^n)$ to $GF(2^k)$, and their complexity. Elements of the field $GF(2^m)$, $m \geq 1$, are represented by m-tuples of elements in $GF(2) = \{0, 1\}$. All gates are assumed to be XOR gates, having fan-in equal to 2 and unrestricted fan-out. The reason we concentrate on binary fields is due to their extensive use in engineering applications, such as error-correcting codes [**4**] and cryptography [**3, 6**].

The gate complexity of a Boolean function $f \in LB_{n,k}$, given by $f(x) = Ax$, is denoted by $\mathcal{C}(A)$. Here, $A = (a_{ij})_{k\times n}$ is a matrix with entries in $GF(2)$ and $x = (x_1, \ldots, x_n)^t$ is a vector of variables in $GF(2)$. $\mathcal{C}(A)$ is then defined as the minimum number of XOR gates needed to realize f. This number is also referred to as the (gate) complexity of A. For positive integers n and k we denote by $\mathcal{C}(n, k)$

J. Carmelo Interlando and Joachim Rosenthal are with the Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556-4618, USA (e-mail: {jinterla,rosen}@nd.edu). Eimear Byrne is with the Department of Mathematics, University College, Dublin Belfield, Dublin 4, Ireland (e-mail: ebyrne@maths.ucd.ie).

the value

$$\mathcal{C}(n,k) = \max\{\mathcal{C}(A) : A \in LB_{n,k}\},$$

the maximum complexity of any $k \times n$ matrix. We say that a $k \times n$ matrix A is *optimal* if $\mathcal{C}(A) = \mathcal{C}(n,k)$.

One of the objectives of the present work is to compute $\mathcal{C}(\mathcal{H}_k)$, where $\mathcal{H}_k$ is the parity-check matrix of the $[2^k - 1, 2^k - k - 1]$ Hamming code. Although an interesting result, the main reason for knowing the complexity of $\mathcal{H}_k$ is that it allows one to compute general upper bounds on the gate complexity of functions in $LB_{n,k}$, for fixed k, and also for fixed n. A general upper bound on the complexity of functions in $LB_{n,n}$ is derived as well. It can be derived from the complexity of the transpose of $\mathcal{H}_k$.

The paper is organized as follows. In Section 2 we present the basic results concerning the complexity of functions in $LB_{n,k}$; in Section 3 we derive the complexity of syndrome computation of Hamming codes; in Section 4, we derive the upper bounds on the complexity of a $k \times n$ matrix; and finally in Section 5 we draw our conclusion.

2. Preliminaries

Consider a function $f : GF(2^n) \to GF(2^k)$ given by $f(x) = Ax$, where $A = (a_{ij})_{k\times n}$ has entries in $GF(2)$. Note that f can be written as

$$f(x) = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n,$$

where a_i is the ith column of A, $1 \leq i \leq n$. We only consider matrices with no all-zero rows or columns. The following result is trivial, but it will be invoked frequently.

PROPOSITION 1. *Let A be a $k \times n$ matrix. Then $\mathcal{C}(A) = \mathcal{C}(AP)$, where P is a permutation matrix.*

In view of Proposition 1, we can now suppose that A is a matrix whose first $m \leq n$ columns are pairwise distinct. When two (rows) columns are equal, we will refer to them as (rows) columns of the same type. Thus we can rewrite f as

$$f(x) = a_1z_1 \oplus a_2z_2 \oplus \ldots \oplus a_mz_m,$$

where $\{a_1, \ldots, a_m\}$ is a subset of the set of columns of the parity-check matrix of the $[2^k - 1, 2^k - k - 1]$ Hamming code, and $z_\ell = \bigoplus_{i\in S_\ell} x_i$, with S_ℓ being the set of indices of the columns of the same type as a_ℓ, $1 \leq \ell \leq m$.

DEFINITION 1. *Let A be a $k \times n$ matrix, and let $R \subset \{1, \ldots, n\}$. We denote by A^R the matrix obtained from A by deleting the columns indexed by R.*

Clearly $\mathcal{C}(A^R) \leq \mathcal{C}(A)$ for any $k \times n$ matrix A and $R \subset \{1, \ldots, n\}$.

LEMMA 1. *Let A be a $k \times n$ matrix such that the ith row of A has Hamming weight at least 2 for some i, and $A = [A'|a]$, where column a has a 1 in the ith position and 0s elsewhere. Then $\mathcal{C}(A') = \mathcal{C}(A) - 1$.*

LEMMA 2. *Let $A = [a_1, \ldots, a_n]$ be a $k \times n$ matrix and let $A_i = [A|a_i]$, for some $i \in \{1, \ldots, n\}$. Then $\mathcal{C}(A_i) = \mathcal{C}(A) + 1$.*

PROOF. It is clear that $\mathcal{C}(A_i) \geq \mathcal{C}(A)+1$, as a new coordinate has been added to the system. Since $A[x_1, \ldots, x_n, x_{n+1}]^t = x_1a_1 \oplus x_2a_2 \oplus \ldots \oplus (x_i \oplus x_{n+1})a_i \oplus \ldots \oplus x_na_n$, we get the reverse inequality $\mathcal{C}(A_i) \leq \mathcal{C}(A) + 1$. □

As an immediate consequence of Lemma 2, we have the following

COROLLARY 1. *Let A be a $k \times n$ matrix and let $R = \{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$. If the columns indexed by R are all of the same type, then $\mathcal{C}(A) = \mathcal{C}(A^{R-\{i_1\}}) + r - 1$.*

A matrix is said to be projective if its columns are distinct pairwise. Given a $k \times n$ projective matrix $A = [a_1, \ldots, a_n]$, we denote by $A(i_1, i_2, \ldots, i_n)$ any $k \times \sum_{j=1}^{n} i_j$ matrix which has i_j columns a_j for each j. From Lemma 2, it follows immediately that

COROLLARY 2. *If A is a $k \times n$ matrix and $B = A(i_1, i_2, \ldots, i_n)$ is a $k \times N$ matrix, then $\mathcal{C}(B) = \mathcal{C}(A) + \sum_{j=1}^{n} i_j - N$.*

In particular, the gate complexity of any matrix can be expressed in terms of its corresponding projective matrix, together with the multiplicities of its columns. For this reason, we are mainly interested in computing the complexity of projective matrices.

Similarly, if a $k \times n$ matrix A has any repeated rows, then $\mathcal{C}(A) = \mathcal{C}(A')$, where A' a $k' \times n$ matrix ($k' \leq k$) containing all the rows of A of different type. Therefore we can assume that no row appears twice in a matrix.

3. Gate Complexity of $\mathcal{H}_k$

Note that any $k \times n$ projective matrix is obtained by deleting columns, or *puncturing* the parity check matrix of the $[2^k - 1, 2^k - k - 1]$ binary Hamming code, which is simply the matrix obtained by selecting as columns all the distinct nonzero binary vectors of length k. We denote this matrix by $\mathcal{H}_k$. Then if $n \geq 2^k - 1$, any $k \times n$ matrix A has complexity which can be expressed in terms of $\mathcal{C}(\mathcal{H}_k)$, and if $n \leq 2^k - 1$, then $A = \mathcal{H}_k^R$ for some set R such that $2^k - 1 = |R| + n$. In light of these connections, it is useful to determine $\mathcal{C}(\mathcal{H}_k)$.

LEMMA 3. *Let $A = [a_1, \ldots, a_n]$ be a $k \times n$ matrix and let $j \in \{1, \ldots, n\}$. Then the matrix*

$$B = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 & 1 \\ a_1 & a_2 & \cdots & a_n & 0 & a_j \end{bmatrix}$$

has gate complexity $\mathcal{C}(A) + 2$.

PROOF. It is clear that $\mathcal{C}(A) + 1 \leq \mathcal{B} \leq \mathcal{C}(A) + 2$. If $\mathcal{B} = \mathcal{C}(A) + 1$ then the $(k-1) \times (n+2)$ matrix formed by deleting the first row of B must have complexity $\mathcal{C}(B) - 1 = \mathcal{C}(A)$, contradicting Lemma 2. The result follows. □

The next result is an immediate consequence of Lemma 3, and gives an exact value for the complexity of $(\mathcal{H}_k)$.

THEOREM 1. *For all $k \geq 2$, $\mathcal{C}(\mathcal{H}_k) = \mathcal{C}(\mathcal{H}_{k-1}) + 2^k - 2$, starting with $\mathcal{C}(\mathcal{H}_1) = 0$. Moreover, this implies that $\mathcal{C}(\mathcal{H}_k) = 2^{k+1} - 2k - 2$. In particular,*

k	$\mathcal{C}(\mathcal{H}_k)$
3	8
4	22
5	52

4. Upper Bounds

We can now obtain some upper bounds on $\mathcal{C}(n,k)$. Note that deleting any t of the k columns of weight 1 from $\mathcal{H}_k$ results in a matrix of complexity $2^{k+1}-2k-2-t$ (each columns contributes exactly 1 to the complexity of the matrix). Let $\hat{\mathcal{H}}_k$ denote the matrix found by deleting all k columns of weight 1 from $\mathcal{H}_k$, which is sometimes more convenient to use. Then $\mathcal{C}(\hat{\mathcal{H}}_k) = 2^{k+1} - 3k - 2$.

COROLLARY 3. *Let n and k be positive integers satisfying $n \geq 2^k - k - 1$. Then $\mathcal{C}(n,k) = n - (2^k - k - 1) + \mathcal{C}(\hat{\mathcal{H}}_k)$, which implies that $\mathcal{C}(n,k) = n + 2^k - 2k - 1$.*

PROOF. Let A be a $k \times n$ matrix formed by appending some $n - 2^k + k + 1$ columns to $\hat{\mathcal{H}}_k$. Then every new column is either of weight 1, or has appeared already as a column of $\hat{\mathcal{H}}_k$, so $\mathcal{C}(A) \leq n - (2^k - k - 1) + \mathcal{C}(\hat{\mathcal{H}}_k)$. On the other hand, each new column requires at least one new gate, so $\mathcal{C}(A) \geq n - (2^k - k - 1) + \mathcal{C}(\hat{\mathcal{H}}_k)$. The result follows. □

The following table gives some initial values for $\mathcal{C}(n,k)$, for $n \geq 2^k - k + 1$. Clearly $\mathcal{C}(n,k) \leq 2n$, for such n, k.

k	$\mathcal{C}(n,k) \leq$
2	$n-1$
3	$n+1$
4	$n+7$
5	$n+21$

Corollary 3 essentially gives an upper bound on $\mathcal{C}(n,k)$, where k is fixed, and we allow n to grow with respect to k. Similarly, we derive an upper bound on $\mathcal{C}(n,k)$ where we fix n, and allow k to grow.

PROPOSITION 2. *Let n be a positive integer. Then $\mathcal{C}(n,k) \leq 2^n - n - 1$, and the least integer k such that $\mathcal{C}(n,k) = 2^n - n - 1$ is given by $k = 2^n - n - 1$.*

PROOF. Let H be the matrix formed by deleting all rows of weight 1 from $\mathcal{H}_k^t$. H has $2^n - n - 1$ rows, and there is a one-to-one correspondence between the supports of all rows and the collection of all subsets of $\{1, \ldots, n\}$ of size at least 2. Since no pair of rows of H are identical, for every row of H the circuit requires at least one Boolean gate, so $\mathcal{C}(H) \geq 2^n - n - 1$. On the other hand, it's easy to see that $\mathcal{C}(H) \leq 2^n - n - 1$, by computing a Boolean circuit as follows. First construct each pair by $x_i \oplus x_j$ for every $i, j \in \{1, \ldots, n\}$. Now every sum of the form $x_i \oplus x_j \oplus x_t$ can be constructed by adding exactly one gate to the system, for each row of weight 3. Continuing in this manner, each sum $\sum_{i \in \mathcal{I}} \oplus x_i$ can constructed by adding exactly one gate to $\sum_{i \in \mathcal{I}'} \oplus x_i$, where $\mathcal{I}' \subset \mathcal{I} \subset \{1, \ldots, n\}$ and $|\mathcal{I}'| = |\mathcal{I}| - 1$. In particular, the entire circuit has exactly one gate for each row of H.

It is clear that adding any further rows to H does not increase the complexity of the new matrix. On the other hand, deleting any row of H must result in a matrix of complexity equal to $\mathcal{C}(H) - 1$. To see this, suppose we delete the row corresponding to the sum $s = x_{i_1} \oplus \cdots \oplus x_{i_t}$. Then any sum $s_1 = s \oplus x_{i_{t+1}}$ can still be constructed by adding some x_{i_j} to any of the t remaining sums, so the complexity is reduced by exactly 1. □

With regard to the Hamming code, the gate complexity of syndrome decoding is simply the value of $\mathcal{C}(\mathcal{H}_k)$. An interesting application of this result is the following, which gives the upper bound on the complexity of an arbitrary $n \times n$ matrix.

THEOREM 2. *Let A be an $n \times n$ matrix for some positive integer n. Then*

$$\mathcal{C}(A) \leq \frac{2n^2}{\log n}.$$

PROOF. Let k be the greatest integer such that $2^k - k - 1 \leq n$. Partition the n coordinates as $\lfloor \frac{n}{k} \rfloor$ sets of size k and a set of size r, where $n = \lfloor \frac{n}{k} \rfloor k + r$. Each set of the partition corresponds to a submatrix of A, whose columns are indexed by it. We estimate the complexity of A by computing the complexity of each such matrix, and then add the cost of summing the $\lfloor \frac{n}{k} \rfloor + 1$ blocks of equations together. Then

$$\begin{aligned}
\mathcal{C}(A) &\leq \mathcal{C}(\mathcal{H}_k^t)\lfloor \frac{n}{k} \rfloor + n\lfloor \frac{n}{k} \rfloor + \mathcal{C}(\mathcal{H}_r^t) \\
&= (2^k - k - 1)\lfloor \frac{n}{k} \rfloor + n\lfloor \frac{n}{k} \rfloor + 2^r - r - 1 \\
&\leq 2n\lfloor \frac{n}{k} \rfloor + 2^r - r - 1 \\
&\leq \frac{2n^2}{\log n}.
\end{aligned}$$

□

5. Conclusion

The XOR gate complexity of computing the matrix-vector product $\mathcal{H}_k x$, where $\mathcal{H}_k$ is the parity-check matrix of the $[2^k - 1, 2^k - k - 1]$ Hamming code has been determined. This further allowed us to derive upper bounds on the XOR gate complexity of the product Ax, where $A = (a_{ij})_{k \times n}$ is a matrix with entries in $GF(2)$, one for fixed k and another one for fixed n. It would be interesting to derive other formulas for the complexity of syndrome decoding of Hamming codes, now using other types of gates, such as $\neg$, AND, and OR.

Acknowledgment

The authors would like to thank Professor Michele Elia (Dipartimento di Elettronica, Politecnico di Torino, Torino, Italy) for several helpful comments and discussions during the course of this work.

References

[1] P. Bürgisser, M. Clausen, and M. A. Shokrollahi: *Algebraic Complexity Theory*. Springer-Verlag: Berlin Heildelberg, 1997.
[2] A. P. L. Hiltgen, *Cryptographically Relevant Contributions to Combinational Complexity Theory*, (ETH-Zürich Dissertation). Konstanz: Hartung-Gorre Verlag, 1994.
[3] N. Koblitz, *Algebraic Aspects of Cryptography*. Springer-Verlag: Berlin Heildelberg, 1998.
[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland: New York, NY, 1977.
[5] J. L. Massey, "The difficulty with difficulty," *Advances in Cryptology - Eurocrypt '96 Proceedings*.
[6] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*. Kluwer Academic Publihers: Boston, 1993.
[7] J. E. Savage, *The Complexity of Computing*. Wiley: New York, 1976.
[8] I. Wegener, *The Complexity of Boolean Functions*. Wiley (Stuttgart: Teubner): New York, 1987.