RI 01003 May 11, 2001 Subject: Computer Science

IBM Research Report

A Linear Lower Bound for Gate Complexity of Transformation Matrices for Conversion between Isomorphic Galois Fields

Atri Rudra[†], Charanjit S. Jutla[*], and Vijay Kumar[†1]

[†]IBM India Research Lab,
Block I, Indian Institue of Technology,
Hauz Khas, New Delhi, 110016, India
email: {ratri,vijayk}@in.ibm.com

[*]IBM Thomas J. Watson Research Center,
P.O.Box 704,
Yorktown Heights, NY 10598, U.S.A.
email: csjutla@watson.ibm.com

IBM Research Division
Almaden - Austin - Beijing - Delhi - Haifa - T.J. Watson - Tokyo - Zurich

LIMITED DISTRIBUTION NOTICE: This report has been submitted for publication outside of IBM and will probably be copyrighted is accepted for publication. It has been issued as a Research Report for early dissemination of its contents. In view of the transfer of copyright to the outside publisher, its distribution outside of IBM prior to publication should be limited to peer communications and specific requests. After outside publication, requests should be filled only by reprints or legally obtained copies of the article (e.g., payment of royalties). Copies may be requested from IBM T.J. Watson Research Center, Publications, P.O. Box 218, Yorktown Heights, NY 10598 USA (email: reports@us.ibm.com). Some reports are available on the Internet at http://www.research.ibm.com/resources/paper_search.html

[1] As of April 2001, the author can be reached at Amazon.com, 605 5^{th} Ave South, Seattle, WA 98104, U.S.A.

A Linear Lower Bound for Gate Complexity of Transformation Matrices for Conversion between Isomorphic Galois Fields

Atri Rudra[1], Charanjit S. Jutla[2], and Vijay Kumar*[1]

[1] IBM India Research Lab,
Block I, Indian Institue of Technology,
Hauz Khas, New Delhi, 110016, India
{ratri,vijayk}@in.ibm.com
[2] IBM Thomas J. Watson Research Center,
P.O.Box 704,
Yorktown Heights, NY 10598, U.S.A.
csjutla@watson.ibm.com

(**Extended Abstract**)

This note uses counting arguments to give a $\Omega(k)$ bound for the operation $T.\mathbf{x}$ where T is any transformation matrix for converting $GF(2^k)$ elements to elements of *isomorphic* composite field $GF((...((2^{d_1})^{d_2})...)^{d_v})$, where $\prod_{j=1}^{j=v} d_j = k$.

A $k \times k$ binary matrix $M = [m_{ij}]$ is called a *(k,t)-row matrix* if $\exists r_1, r_2, \cdots, r_t \in \{1, .., k\}$ such that

$$\sum_{j=1}^{k} m_{lj} \quad \begin{cases} \geq 2 & \text{if } l \in \{r_1, r_2, \cdots, r_t\} \\ = 1 & \text{otherwise} \end{cases}$$

M is called a *(k,t)-column matrix* if M^T is a (k,t)-row matrix.

Consider a transformation matrix T that performs the isomorphic mapping from $GF(2^k)$ to some composite field. That is, $\boldsymbol{y} = T.\boldsymbol{x}$ is the element of the composite field corresponding to $\boldsymbol{x} \in GF(2^k)$. Such a matrix T is called a *(k,t)-row (column) tranform* if it is a (k,t)-row (column) matrix.

For any matrix T, we denote by $s(T)$ the smallest possible number of binary gates in any circuit that computes $T.\boldsymbol{x}$.

Lemma 1. *For any (k,t)-row transform M, $s(M) = \Omega(t)$.*

Proof. The hamming distance between any two rows in M is atleast one. Let $\mathcal{R}$ be the set of rows where the number of 1s is greater than 1. Let $\boldsymbol{y} = M \cdot \boldsymbol{x}$. For each $r_i \in \mathcal{R}$, the corresponding y_i is the output of some circuit gate. Each such y_i is the output of a distinct gate, since otherwise there will be fewer than 2^k distinct possible $\boldsymbol{y}$ values. ■

* As of April 2001, the author can be reached at Amazon.com, 605 5^{th} Ave South, Seattle, WA 98104, U.S.A.

Lemma 2. [1] *For any boolean matrix B, $s(B) = s(B^T)$.*

Lemma 1 and Lemma 2 together imply

Corollary 1. *For any (k,t)-column transform M, $s(M) = \Omega(t)$.* ■

Let $R(z)$ be the field polynomial of $GF(2^k)$, and β a root of $R(z)$. Let $\mathcal{B}$ denote $\{1, \beta, \beta^2, ..., \beta^{k-1}\}$, the standard basis for representing elements of $GF(2^k)$. Let $\mathcal{S}$ denote the set $\{1, \beta, \beta^2, ..., \beta^{k/2-1}\}$. Note that if $\gamma \in \mathcal{S}$, then $\gamma^2 \in \mathcal{B}$.

We first consider the special case where the composite field is $GF((2^n)^m)$ where $n \times m = k$.

Let the underlying field polynomials of $GF((2^n)^m)$ be $Q(y)$ and $P(x)$. Let α be a root of $P(x)$. Any $a \in GF((2^n)^m)$ can be written as $a = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + ... + a_1\alpha + a_0$ for some $a_i \in GF(2^n) \forall i$.

Consider a (k,t)-column transformation matrix T that maps elements of $GF(2^k)$ to the isomorphic composite $GF((2^n)^m)$. Let H denote the isomorphism, and $\mathcal{T}$ the set $\{\beta^{r_1}, \beta^{r_2}, \cdots, \beta^{r_t}\}$. Then, $\exists r_1, r_2, ..., r_t \in \{1, .., k\}$ such that

$$H(\beta^l) = \begin{cases} \Sigma_{i=0}^{m-1}\Sigma_{j=0}^{n-1} c_{ij}^l \alpha^i \omega^j, & \text{where alteast two } c_{ij}^l = 1, \\ & \text{if } \beta^l \in \mathcal{T} \\ \alpha^{i_l}\omega^{j_l}, & \text{for some unique tuple } (i,j) \text{ where } i_l < m \\ & \text{and } j_l < n, \\ & \text{if } \beta^l \in \mathcal{B} - \mathcal{T}. \end{cases}$$

Let $\sqrt{\mathcal{T}} \subseteq \mathcal{B}$ denote the set $\{\beta^j \mid \beta^{2j} \in \mathcal{T}\}$. Let $\mathcal{Z} = \sqrt{\mathcal{T}} \cup (\mathcal{T} \cap \mathcal{S})$. Note that $|\mathcal{Z}| \leq 2|\mathcal{T}| = 2t$. Further, for any set A, let $H(A) = \{H(x) | \ x \in A\}$.

Lemma 3. $|H(\mathcal{S} - \mathcal{Z}) - \{1\}| \leq k/4 - 1$.

Proof. Consider $\beta^s \in (\mathcal{S} - \mathcal{Z})$. Since $(\mathcal{S} - \mathcal{Z}) \subset (\mathcal{B} - \mathcal{T})$, $H(\beta^s)$ is of the form $\alpha^{i_s}\omega^{j_s}$. Since H is an isomorphism, $(H(\beta^s))^2 = H(\beta^{2s})$. That is,
$\alpha^{2i_s \ mod(2^m-1)}\omega^{2j_s \ mod(2^n-1)} = \alpha^{i_{2s}}\omega^{j_{2s}}$ for some i_{2s} and j_{2s}.

Note that $(2i_s) \leq 2(m-1)$, which is less than $2^m - 1$ for all $m > 1$. Thus, $2i_s \ mod(2^m - 1) = 2i_s$, and similarly $2j_s \ mod(2^n - 1) = 2j_s$.

Next, we argue that $2i_s < m$ and $2j_s < n$. Assume that such is not the case, and that $2i_s \geq m$. Then $\alpha^{2i_s} = \Sigma_{r=0}^{m-1} v_r \alpha^r$ where $v_r \in GF(2^n)$, and there are at least two values of r for which $v_r \neq 0$. Thus, $\alpha^{2i_s}\omega^{2j_s} = \Sigma_{r=0}^{m-1}\alpha^r(v_r\omega^{2j_s})$, where at least two terms in the summation have non-zero coefficients. But that is not possible since $\beta^s \in (\mathcal{S} - \mathcal{Z})$ implies that $\beta^{2s} \in (\mathcal{B} - \mathcal{T})$, which implies that $H(\beta^{2s})$ must be of the form $\alpha^i\omega^j$ for some $i < m$, $j < n$. It follows that $2i_s < m$. A similar argument shows that $2j_s < n$.

Thus, $i_s \in [0..(m/2 - 1)]$ and $j_s \in [0..(n/2 - 1)]$, which implies that the number of unique (i_s, j_s) tuples is $n/2 \times m/2 = k/4$. Since that is an upper bound on the total number of elements in $H(\mathcal{S} - \mathcal{Z})$), the lemma follows. ■

H is a one-to-one mapping, so $|\mathcal{S} - \mathcal{Z}| = |H(\mathcal{S} - \mathcal{Z})|$. Since, as noted above, $|\mathcal{Z}| \leq 2t$, Lemma 3 implies that $t \geq k/8$. In other words,

Corollary 2. *For any $t < k/8$ there cannot exist a (k,t)-column transform that performs an isomorphic mapping from $GF(2^k)$ to a composite field $GF((2^n)^m)$.* ■

For the general version of Corollary 2 we use the following notation — let $P_j(x)$ denote the field polynomial corresponding to d_j where $k = \prod_{j=1}^{v} d_j$. Also let $P_j(\alpha_j) = 0$.

Consider a (k,t)-column transformation matrix T' that maps elements of $GF(2^k)$ to the isomorphic composite $GF((...((2^{d_1})^{d_2})...)^{d_v})$. Let H' denote the isomorphism, and $\mathcal{T}'$ the set $\{\beta^{r'_1}, \beta^{r'_2}, \cdots, \beta^{r'_t}\}$. Then, $\exists r'_1, r'_2, ..., r'_t \in \{1, .., k\}$ such that

$$H(\beta^l) \begin{cases} \Sigma_{i_1=0}^{d_1-1} \Sigma_{i_2=0}^{d_2-1} \cdots \Sigma_{i_v=0}^{d_v-1} c^l_{i_1 i_2 \cdots i_v} \Pi_{p=0}^{v-1} (\alpha_p)^{i_p}, & \text{where alteast two } c^l_{i_1 i_2 \cdots i_v} = 1, \\ & \text{if } \beta^l \in \mathcal{T}' \\ \Pi_{p=0}^{v-1} (\alpha_p)^{i_{p,l}}, & \text{for some unique v-tuple } (i_{1,l}, i_{2,l}, \cdots, i_{v,l}) \\ & \text{where } \forall p \in [1..v]\ i_p < d_p, \\ & \text{if } \beta^l \in \mathcal{B} - \mathcal{T}'. \end{cases}$$

Let $\sqrt{\mathcal{T}'} \subseteq \mathcal{B}$ denote the set $\{\beta^j \mid \beta^{2j} \in \mathcal{T}'\}$. Let $\mathcal{Z}' = \sqrt{\mathcal{T}'} \cup (\mathcal{T}' \cap \mathcal{S})$. Note that $|\mathcal{Z}'| \leq 2|\mathcal{T}'| = 2t$. Further, for any set A, let $H'(A) = \{H'(x) |\ x \in A\}$.

Lemma 4. *For any $t < (2^{v-1} - 1)k/2^{v+1}$ there cannot exist a (k,t)-column transform that performs an isomorphic mapping from $GF(2^k)$ to a composite field $GF((...((2^{d_1})^{d_2})...)^{d_v})$, where $k = \prod_{j=1}^{j=v} d_j$.*

Proof. Consider $\beta^{s'} \in (\mathcal{S} - \mathcal{Z}')$, i.e. $H'(\beta^{s'})$ is of the form $\Pi_{p=0}^{v-1}(\alpha_p)^{i_{p,s'}}$. A proof along the same lines as the proof for Lemma 3 shows that $|H(\mathcal{S} - \mathcal{Z}') - \{1\}| \leq k/2^v - 1$ (as the number of unique $(i_{1,s'}, i_{2,s'}, ...i_{v,s'})$ v-tuples is $\prod_{j=1}^{j=v}(d_j/2) - 1 = k/2^v - 1$). The proof is complete by noting that H' is a one-to-one mapping and that $|\mathcal{S} - \mathcal{Z}' - \{1\}| \geq k/2 - 2t - 1$. ■

Corollary 1 and Lemma 4 together imply

Theorem 1. *For any binary matrix T such that $T\dot{\boldsymbol{x}}$ is isomorphic mapping from $GF(2^k)$ to some composite field, $s(T) = \Omega(k)$.*

■

References

1. N.Alon, M.Karchmer and A.Wigderson "Linear Circuits over GF(2)". In *SIAM J. of Comput.* Vol. 19, No. 6, pp. 1064-1067, December 1990