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

[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 $T.\boldsymbol{x}$ 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 denote by $\mathcal{O}(f)$ and $\mathcal{D}(f)$, the order and degree respectively of an irreducible polynomial $f(x)$. We have the following observation–

Observation 1 *For any irreducible polynimial f, $\mathcal{O}(f)$ is odd .*

Further, $f(x)$ is a *good* polynomial if $\mathcal{O}(f) > 2(\mathcal{D}(f) - 1)$.

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 $P(x)$, where $Q(y)$ generates $GF(2^n)$. Let α and ω be a root of $P(x)$ and $Q(y)$ respectively . 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 $a_i \in GF(2^n)$.

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 $\{\beta^{r_1}, \beta^{r_2}, \cdots, \beta^{r_t}\}$. Thus,

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

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 $H(A) = \{H(x) | \; x \in A\}$.

We proceed in the following manner – first we prove that if H is of a particular type, then we trivially have the liner lower bound (Claim 1). The main proof does case analysis on whether $P(x)$ and/or $Q(y)$ are *good*. In all the cases we prove the bound by using contradiction and counting arguments.

Claim. If $H(\beta) \neq \alpha^u\omega^v$ for some $u \in [0 \cdots (\mathcal{O}(P)-1)], v \in [0 \cdots (\mathcal{O}(Q)-1)]; u + v \neq 0$, then $s(T) = \Omega(k)$.

Proof. $H(\beta) \neq \alpha^u\omega^v$ implies that there does not exist an i such that

- $H(\beta^i) = \alpha^{u'}\omega^{v'}$ for some $u' \in [0 \cdots (\mathcal{O}(P) - 1)], v' \in [0 \cdots (\mathcal{O}(Q) - 1)]$; and
- $H(\beta^{i+1}) = \alpha^{u''}\omega^{v''}$ for some $u'' \in [0 \cdots (\mathcal{O}(P) - 1)], v'' \in [0 \cdots (\mathcal{O}(Q) - 1)]$.

This implies that T is a (k, t')–column transform, where $t' > k/2$. The claim follows from Corollary 1 ■

We consider three cases depending on whether $P(x)$ and $Q(y)$ are *good*.

Case 1 : Both $P(x)$ and $Q(y)$ are *good* polynomials.

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, $\alpha^{2i_s \bmod (\mathcal{O}(P))}\omega^{2j_s \bmod (\mathcal{O}(Q))} = \alpha^{i_{2s}}\omega^{j_{2s}}$ for some i_{2s} and j_{2s}.

Note that $(2i_s) \leq 2(m-1)$, which is less than $\mathcal{O}(P)$ for all $m > 1$. Thus, $2i_s \bmod (\mathcal{O}(P)) = 2i_s$, and similarly $2j_s \bmod (\mathcal{O}(Q)) = 2j_s$.

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, for case 1, the following holds –

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 $GF((2^n)^m)$.* ■

Case 2: Exactly one of $P(x)$ and $Q(y)$ is a *good* polynomial .

Without loss of generality let us assume that $P(x)$ is not a *good* polynomial.

Suppose $H(\beta) = \alpha^u\omega^v$. Now consider the set $H(\mathcal{B})$ and the powers of α and ω. We denote by $\mathcal{U}$ and $\mathcal{V}$ the sequences $\{u, 2u \bmod (\mathcal{O}(P)), \cdots, (k-1)u \bmod (\mathcal{O}(P))\}$ and $\{v, 2v \bmod (\mathcal{O}(Q)), \cdots, (k-1)v \bmod (\mathcal{O}(Q))\}$ respectively. Let η be the minimum value such that $\eta u = 0 \bmod (\mathcal{O}(P)$ and let ρ be the minimum number such that $\rho v = 0 \bmod (\mathcal{O}(Q))$.

Also we denote a special case of $\mathcal{U}$ as $\mathcal{U}^* = \{1, 2, \cdots, \mathcal{O}(P) - 1\}$. Further let $\mathcal{A}_\mathcal{U} = \{\alpha^u | u \in \mathcal{U}\}$.

Lemma 4. *If $\mathcal{U} = \mathcal{U}^*$ and $\mathcal{A}_{\mathcal{U}^*}$ has $r + m$ entries*[1]*, then $s(T) = O(rn)$.*

Proof. Each of $\alpha^m ... \alpha^{\mathcal{O}(P)-1}$ has at least two entries. Each of α^i , with $i \in [m \cdots \mathcal{O}(P) - 1]$ appears $k/\mathcal{O}(P)$ times, each time with a different ω power. Similarly, for each ω power, all of α^i, $i \in [m \cdots \mathcal{O}(P) - 1]$ appear once. Thus, for each ω^{j_l}, $l \in [1 \cdots k/\mathcal{O}(P)]$ the circuit for $\alpha^m ... \alpha^{\mathcal{O}(P)-1}$ has to be implemented independently. Thus, $O(rn)$ gates are required. ■

Lemma 5. $\{\alpha^m, \cdots, \alpha^{\mathcal{O}(P)-1}\}$ *has $\Omega(m)$ entries.*

Proof. Write $\alpha^{m+s} \bmod (P(x))$ as $\sum_{i=0}^{m-1} c(s,i)\alpha^i$; i.e. $c(0,i)$ are the coefficients in α^m and so on. Consider an i, j such that $c(0,i) = 1 = c(0,j)$, and all the inbetween coefficients are zero. Then $c(s, s+i) = 1$, for $0 \leq s \leq (j-i)$. This

[1] Note that m entries come from the m singleton elements α^i, $i \in [1 \cdots (m-1)]$.

is easily proved by induction. Base case is true. Let $c(s-1, s-1+i) = 1$, then $c(s, s+i) = c(s-1, s-1+i) \oplus c(0, s+i) * c(s-1, m-1)$. However, $c(0, s+i) = 0$, proving the inductive step. In other words, what has been shown is that for each t, $0 \leq t < m$, there exists an s, $s < \mathcal{O}(P) - m$, such that $c(s, t) = 1$.

Among all the is and the corresponding js, let i_G and j_G that pair of i and j such that $|i-j|$ is the maximum. The proof is complete by noting that $\mathcal{O}(P) - m \geq |i_G - j_G|$.[2] ∎

Lemma 6. *If the condition of Claim 1 does not hold and* $gcd(u, \mathcal{O}(P)) = 1$ *then* $s(T) = \Omega(k)$.

Proof. As $gcd(u, \mathcal{O}(P)) = 1$, $\mathcal{U} = \mathcal{U}^*$. The proof follows from Lemma 5 and Lemma 4. ∎

Lemma 7. *In Case 2,* $s(T) = \Omega(k)$.

Proof. If the condition of Claim 1 holds, then we are done. Thus, $H(\beta) = \alpha^u \omega^v$. There are $\min(k-1, \rho)$ distinct values in $\mathcal{V}$. If $\rho \geq 3n/2$, then we are done (as there are atmost n distinct is such that ω^i is a singleton and hence, T is a $(k, k/3)$-column transform).

Assume $\gcd(u, \mathcal{O}(P)) > 1$. $\mathcal{U}$ has has atmost η distinct values.By Observation 1, $\eta < \mathcal{O}(P)/3$. Thus, $|H(\beta)| < \rho\eta < (3n/2) \times (\mathcal{O}(P)/3) < k$ which is a contradiction. Lemma 6 completes the proof. ∎

Case 3: Both $P(x)$ and $Q(y)$ are not *good* polynomials .

Here also we have the following lemma –

Lemma 8. *In Case 3,* $s(T) = \Omega(k)$.

Proof. As in the proof of Lemma 7 assume that the condition of Claim 1 does not hold. Also let $\gcd(u, \mathcal{O}(P)) > 1$ and $\gcd(u, \mathcal{O}(Q)) > 1$. Here $\eta < \mathcal{O}(P)/3$ and $\rho < \mathcal{O}(Q)/3$ and thus $H(\beta) < 4k/9$ which is a contradiction. Without loss of generality, $\gcd(u, \mathcal{O}(P)) = 1$. Lemma 6 completes the proof. ∎

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

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

[2] $\alpha^{\mathcal{O}(P)} = 1$. So when shifting and adjustments are done $\mathcal{O}(P) - m$ times, the resulting polynomial should become 1. Since there is no 1 between i_G and j_G , the 1 which started at position i in α^m cannot get cancelled by any *xor* due to overflow adjustments. It can only get cancelled when it has moved to position j_G.

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 $H'(A) = \{H'(x)| \ x \in A\}$.

It can be seen that Claim 1 can be generalised to the following claim –

Claim. If $H(\beta) \neq \Pi_{j=0}^{v} \alpha_j^{u_j}$ for some $u_j \in [0 \cdots (\mathcal{O}(P_j) - 1)]$ and $\Sigma_{j=0}^{v} u_j \neq 0$, then $s(T) = \Omega(k)$.

If $H(\beta) = \Pi_{j=0}^{v} \alpha_j^{u_j}$, then $\mathcal{U}_j = \{u_j, 2u_j \bmod (\mathcal{O}(P_j)), \cdots, (k-1) \bmod (\mathcal{O}(P_j))\}$ and ρ_j is the minimum value such that $\rho_j u_j = 0 \bmod (\mathcal{O}(P_j))$.

Again we consider three cases.

Case G.1 : All the $P_j(x)$ are *good* polynomials .

Lemma 9. *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 $|\mathcal{S} - \mathcal{Z}' - \{1\}| \geq k/2 - 2t - 1$. ∎

Case G.2 : Exactly d out of v $P_j(x)$ are *good* polynomials .

Without loss of generality assume $P_1(x), \cdots, P_d(x)$ are *good*.

Lemma 10. *In Case G.2, $s(T) = \Omega(k)$.*

Proof. If the condition of Claim 1 holds, then we are done. Thus, $H(\beta) = \Pi_{j=0}^{v} \alpha_j^{u_j}$. There are $\min(k-1, \rho_l)$ distinct values in $\mathcal{U}_l$ for $l \in [1 \cdots d]$. If $\rho_l \geq (3/2)^{v/d-1} d_l$, then we are done (as there are atmost d_l distinct is such that α_l^i is a singleton and hence, T is a $(k, O(k))$-column transform).

For each $e \in [d+1 \cdots v]$, assume $\gcd(u_e, \mathcal{O}(P_e)) > 1$. $\mathcal{U}_e$ has atmost ρ_e distinct values. By Observation 1, $\rho_e < \mathcal{O}(P_e)/3$. Thus, $|H(\beta)| < \Pi_{j=1}^{v} \rho_j < k$ which is a contradiction. Without loss of generality $\gcd(u_v, \mathcal{O}(P_v)) = 1$. Lemma 6 completes the proof[3]. ∎

Case G.3 All the $P_j(x)$ are not *good* polynomials .

A simple generalisation of the proof of Lemma 8 gives the following lemma –

Lemma 11. *In Case G.3, $s(T) = \Omega(k)$.*

Thus, we have proved

Theorem 1. *For any binary matrix T such that $T\dot{x}$ 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

[3] In the proof of Lemma 6 substitute $P, \mathcal{U}$ and m by $P_v, \mathcal{U}_v$ and d_v respectively .