The Generalized XOR Lemma

Yuliang Zheng [a], Xian-Mo Zhang [b]

[a] *Department of Software & Information Systems*
The University of North Carolina at Charlotte
9201 University City Blvd, Charlotte
NC 28223-0001, USA
Email: yzheng@uncc.edu

[b] *Department of Computing*
Macquarie University
Sydney, NSW 2109, Australia
Email: xianmo@ics.mq.edu.au

Abstract

The XOR Lemma states that a mapping is regular or balanced if and only if all the linear combinations of the component functions of the mapping are balanced Boolean functions. The main contribution of this paper is to extend the XOR Lemma to more general cases where a mapping may not be necessarily regular. The extended XOR Lemma has applications in the design of substitution boxes or S-boxes used in secret key ciphers. It also has applications in the design of stream ciphers as well as one-way hash functions. Of independent interest is a new concept introduced in this paper that relates the regularity of a mapping to subspaces.

Key words: XOR Lemma, Hadamard Transformation, Cryptography

1 Introduction

Let $F(x_1, \ldots, x_k) = (f_1(x_1, \ldots, x_k), \ldots, f_m(x_1, \ldots, x_k))$ be a mapping from V_k to V_m, where each $x_j \in GF(2)$, each f_i is a function with n variables and V_k is the vector space of k tuples of elements from $GF(2)$. F is said to be *regular* if F goes through all vectors in V_m, each 2^{k-m} times, when x goes through all vectors in V_k once. Obviously $k \geq m$ must hold for a regular mapping F. The *XOR Lemma* states that F is regular if and only if every non-zero linear combination of $f_1, \ldots, f_m$ is balanced. The XOR Lemma is expressed in terms of independence of random variables in [3] and [2]. It also appears as Corollary 7.39 of [4]. Note that every permutation on V_k is regular. An application of the XOR Lemma is to determine the strict regularity of a given cryptographic mapping by examining whether the linear combinations of its component functions are biased.

In practice, however, there is a need to study more general cases when F is not necessarily regular. In this work, we introduce a concept that a mapping *is regular with respect to a subspace* and show that for any given mapping P from V_k to V_m there exists a subspace W such that P is regular with respect to W. This allows us to look beyond regular mappings by establishing a *Generalized XOR Lemma*. The Generalized XOR Lemma can handle not only regular mappings but also those that are not strictly regular.

A major application of the Generalized XOR Lemma is the design of the so-called substitution-box or S-boxes employed in a block cipher. In many ciphers, S-boxes are the only non-linear operation it employs. Therefore these mappings are the most critical component of the ciphers. In order to ensure that the ciphers are not vulnerable to attacks that exploit statistical imbalance within the ciphers, S-boxes used in the ciphers must be regular or very close to regular. But there are some cases where we cannot hope for the strict regularity. One typical example is S-boxes that have more output bits than input bits. Such "expanding" S-boxes are used, for example, in the Cast-128 cipher which is an Internet standard [1]. Clearly, such expanding S-boxes are *not* regular; therefore we need a way for discussing somewhat weaker regularity. This is where we can use our generalized regularity and Generalized XOR Lemma. Further applications of the Generalized XOR Lemma include the design and analysis of other security tools such as one-way hash functions and stream ciphers [5] both of which rely on good (regular or slightly biased) non-linear S-boxes for their security.

2 Generalized Regularity

We now define formally the notion of generalized regularity. We generalize the regularity notion by relaxing its condition, which allows us to consider mappings with more output bits than input bits, i.e., those mappings from V_k to V_m with $k < m$.

Let W be an l-dimensional linear subspace of V_m. From linear algebra, V_m can be partitioned into 2^{m-l} parts:

$$V_m = \Pi_0 \cup \Pi_1 \cup \cdots \cup \Pi_{2^{m-l}-1}, \quad \text{where } \Pi_0 = W, \tag{1}$$

such that for any $0 \leq j \leq 2^{m-l} - 1$, $\beta, \gamma \in \Pi_j$ if and only if $\beta \oplus \gamma \in W$. It is known that $\Pi_j = 2^l$, $j = 0, 1, \ldots, 2^{m-l}$. Each Π_j is called a *coset* of W. It should be noted that for a fixed W, the partition (1) is unique if the order of the cosets is ignored.

Next we introduce the concept of a mapping regular with respect to a subspace.

Definition 1 *Let P be a mapping from V_k to V_m, and W be an l-dimensional linear subspace of V_m $(0 \le l \le \min\{k, m\})$ and s_j be zero or a positive integer, $i = 0, 1, \ldots, 2^{m-l} - 1$, satisfying $s_0 + s_1 + \cdots + s_{2^{m-l}-1} = 2^{k-l}$. We say that P is* regular with respect to W and $(s_0, s_1, \ldots, s_{2^{m-l}-1})$ *if for each fixed j, $0 \le j \le 2^{m-l}-1$ and each vector $\gamma \in \Pi_j$ (defined in (1)), we have $\#\{\alpha | P(\alpha) = \gamma,\ \alpha \in V_k\} = s_j$. When the choice of $(s_0, s_1, \ldots, s_{2^{m-l}-1})$ is not important, we simply say that P is* regular with respect to W.

Though trivial, two extreme cases need to be mentioned here.

Lemma 2 *(i) Any regular mapping from V_k to V_m is a mapping regular with respect to $W = V_m$.*

(ii) For any given mapping P from V_k to V_m, there exists a subspace W of V_m such that P is regular with respect to W.

PROOF. (i) If we set $l = m$, i.e., $W = V_m$ in Definition 1, then any regular mapping from V_k to V_m is a mapping regular with respect to $W = V_m$ and $s_0 = 2^{k-m}$. Clearly we have $k \ge m$ in this case.

(ii) Let $l = 0$, i.e., $W = \{0\}$. Then P is regular with respect to $W = \{0\}$.

In general, from Definition 1, we know that P is unbiased for all the vectors in each fixed coset Π_j. We give an example to explain Definition 1. Let $m = k + 2$ and $l = k$ in Definition 1. Let P be a mapping from V_k to V_{k+2} such that $P(a_1, \ldots, a_k) = (1, 0, a_1, \ldots, a_k)$. Let W be a k-dimensional subspace such as $W = \{(0, 0, x_1, \ldots x_k)|$ each $x_j \in GF(2)\}$. Set $\Pi_0 = W$, $\Pi_1 = \{(0, 1, x_1, \ldots x_k)|$ each $x_j \in GF(2)\}$, $\Pi_2 = \{(1, 0, x_1, \ldots x_k)|$ each $x_j \in GF(2)\}$, $\Pi_3 = \{(1, 1, x_1, \ldots x_k)|$ each $x_j \in GF(2)\}$. Hence $V_{k+2} = \Pi_0 \cup \Pi_1 \cup \Pi_2 \cup \Pi_3$ where $\Pi_j \cap \Pi_i = \emptyset$, where $\emptyset$ denotes the empty set, if $j \ne i$. Note that $P(V_k) = \Pi_2$ where $P(V_k) = \{P(\alpha)|\ \alpha \in V_k\}$. Since P takes all vectors in Π_2 once, but not any vector in $\Pi_0 \cup \Pi_1 \cup \Pi_3$, P is a regular mapping with respect to W and (s_0, s_1, s_2, s_3) where $s_0 = 0$, $s_1 = 0$, $s_2 = 1$ and $s_3 = 0$. Obviously P is unbiased for all the vectors in any fixed Π_j.

The following theorem indicates the existence of a mappings from V_k to V_m, that is regular with respect to a given subspace W of V_m.

Theorem 3 *Let m and k be two positive integers, W be an l-dimensional linear subspace of V_m, and integers $s_0, s_1, \ldots, s_{2^{m-l}-1}$ satisfy $s_j \ge 0$, $j =$*

$0, 1, \ldots, 2^{m-l}-1$ *and* $s_0+s_1+\cdots+s_{2^{m-l}-1} = 2^{k-l}$. *Then there exists a mapping from* V_k *to* V_m*, that is regular with respect to* W *and* $(s_0, s_1, \ldots, s_{2^{m-l}-1})$.

PROOF. Let $R = \{j|s_j \neq 0, \ \ j = 0, 1, \ldots, 2^{m-l} - 1\}$ and write $R = \{j_1, \ldots, j_t\}$. Hence $s_{j_1} + \cdots + s_{j_t} = 2^{k-l}$. We choose $\mu_{j_1} \in \Pi_{j_1}$, …, $\mu_{j_t} \in \Pi_{j_t}$, where each Π_j has been defined in the partition (1). Divide V_k into t disjoint subsets: $V_k = S_1 \cup \cdots \cup S_t$ such that $S_j \cap S_i = \emptyset$ whenever $j \neq i$ and $\#S_1 = s_{j_1}2^l, \ldots, \#S_t = s_{j_t}2^l$. Divide each S_u into 2^l disjoint subsets: $S_u = S_u^{(1)} \cup \cdots \cup S_u^{(2^l)}$ such that $S_u^{(j)} \cap S_u^{(i)} = \emptyset$ whenever $j \neq i$ and $\#S_u^{(1)} = \#S_u^{(2)} = \cdots \#S_u^{(2^l)} = s_{j_u}$. Write $\Pi_{j_u} = \{\gamma_u^{(1)}, \ldots, \gamma_u^{(2^l)}\}$. Define a mapping P, from V_k to V_m, such that for each u, $1 \leq u \leq t$ and each i, $1 \leq i \leq 2^l$, $P(S_u^i) = \{\gamma_u^{(i)}\}$, where $P(X) = \{P(\alpha)|\alpha \in X\}$. Hence P is mapping from V_k to V_m, that is regular with respect to W and $(s_0, s_1, \ldots, s_{2^{m-l}-1})$.

A *function* is a mapping from V_k to $GF(2)$ (or simply a function on V_k). The *truth table* of a function f on V_k is a $(0,1)$-sequence defined by $(f(\alpha_0), f(\alpha_1)$, …, $f(\alpha_{2^k-1}))$, and the *sequence* of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}$, $(-1)^{f(\alpha_1)}$, …, $(-1)^{f(\alpha_{2^k-1})})$. Let $\tilde{a} = (a_1, \cdots, a_{2^k})$ and $\tilde{b} = (b_1, \cdots, b_{2^k})$ be the sequences of functions f and g on V_k respectively. The *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as $\langle \tilde{a}, \tilde{b} \rangle = a_1b_1 \oplus \cdots \oplus a_{2^k}b_{2^k}$, where the addition and multiplication are over the reals. An *affine* function f on V_k is a function that takes the form of $f(x_1, \ldots, x_k) = a_1x_1 \oplus \cdots \oplus a_kx_k \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, k$. Furthermore f is called a *linear* function if $c = 0$.

A $(1,-1)$-matrix N of order k is called a *Hadamard* matrix if $NN^T = kI_k$, where N^T is the transpose of N and I_k is the identity matrix of order k. A Sylvester-Hadamard matrix of order 2^k, denoted by H_k, is generated by the following recursive relation

$$H_0 = 1, \ H_k = \begin{bmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{bmatrix}, \ k = 1, \, 2, \ldots.$$

Let ℓ_i, $0 \leq i \leq 2^k - 1$, be the i row of H_k. It is known that ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_k according to the ascending alphabetical order. The *Hamming weight* of a $(0,1)$-sequence ξ, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_k, the *Hamming distance* $d(f, g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1, \ldots, x_k)$.

Let $P(y)$ be a mapping from V_k to V_m, where $y \in V_k$. Write $P(y) = (p_1(y), \ldots$

, $p_m(y))$, where each $p_j(y)$ is a function on V_k. We are concerned with all the linear combinations of $p_1(y), \ldots, p_m(y)$, denoted by $q_0(y), q_1(y), \ldots, q_{2^m-1}(y)$, where $q_j(y) = \bigoplus_{u=1}^{m} c_u p_u(y)$ and $(c_1, \ldots, c_m)$ is the binary representation of an integer j, $j = 0, 1 \ldots, 2^m - 1$.

Let R_i denote the sequence of $q_i(y)$, $i = 0, 1, \ldots, 2^m - 1$. Define a $2^m \times 2^k$ $(1, -1)$ matrix B^* as follows:

$$B^* = \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ R_{2^m-1} \end{bmatrix} = [h_0, h_1, \cdots, h_{2^k-1}]$$

where R_i is the ith row and h_j is the jth column of B^*. One can verify that each h_j is the sequence of a linear function on V_m, i.e., a column of H_m.

Let $L_0, L_1, \ldots, L_{2^m-1}$ be the row vectors, from the top to the bottom of H_m. Assume that L_j^T appears in matrix B^* k_j times as a column of B^*. Using the same argument as that in the Appendix of [7], we know that

$$(\langle R_0, R_0\rangle, \langle R_0, R_1\rangle, \ldots, \langle R_0, R_{2^m-1}\rangle) = (k_0, k_1, \ldots, k_{2^m-1})H_m \tag{2}$$

holds even for the case of $k \geq m$ or $k < m$. Note that L_j is the sequence of a linear function on V_m, $\psi_j(x) = \langle \gamma_j, x\rangle$, where γ_j is the binary representation of integer j, $j = 0, 1, \ldots, 2^m - 1$. Hence, from the definition of k_j, k_j is also the number of times that $P(y)$ goes through $\gamma_j \in V_m$. Since $q_0(y)$ is the zero function on V_k, R_0 is the all-one sequence. Hence $\langle R_0, R_i\rangle$ is equal to the sum of the components in R_i. As a result, we have $\langle R_0, R_i\rangle = 0$ if and only if q_j is balanced.

Let W be an l-dimensional linear subspace of V_m. From linear algebra, there exists an $(m - l)$-dimensional linear subspace of V_m, denoted by W^*, such that each $\gamma \in V_m$ can be uniquely expressed as $\gamma = \beta \oplus \mu$ where $\beta \in W$ and $\mu \in W^*$. W^* is called a *complementary subspace* of W in V_m. Furthermore let W^* be composed of $\mu_0 = 0, \mu_1, \ldots, \mu_{2^{m-l}-1}$ where each $\mu_j \in W^*$. Then

$$V_m = (\mu_0 \oplus W) \cup (\mu_1 \oplus W) \cup \cdots \cup (\mu_{2^{m-l}-1} \oplus W) \tag{3}$$

where $\mu \oplus W = \{\mu \oplus \gamma | \gamma \in W\}$, $(\mu_j \oplus W) \cap (\mu_i \oplus W) = \emptyset$ for all $j \neq i$. It should be noted that W^* is not unique except for the special cases where $W = V_n$ and $W = \{0\}$. However, since the partition (1) is unique, (3) is identical to (1) except for the order of the cosets.

The following Theorem is called *the Generalized XOR Lemma*.

Theorem 4 *Let $P(y) = (p_1(y), \ldots, p_m(y))$ be a mapping from V_k to V_m where each $p_j(y)$ is a function on V_k, W be an l-dimensional linear subspace of V_m, where $l \leq \min\{k, m\}$.*

(i) If $P(y)$ is regular with respect to W, then for any complementary W^* subset of W in V_m, and any $(b_1, \ldots, b_m) \in V_m$ with $(b_1, \ldots, b_m) \notin W^*$, $b_1p_1(y) \oplus \cdots \oplus b_mp_m(y)$ is balanced.
(ii) If there exists a complementary subset W^* of W in V_m, such that for any $(b_1, \ldots, b_m) \in V_m$ with $(b_1, \ldots, b_m) \notin W^*$, $b_1p_1(y) \oplus \cdots \oplus b_mp_m(y)$ is balanced, then $P(y)$ is regular with respect to W.

PROOF. First we consider the special case of $W = \{(0, \ldots, 0, c_1, \ldots, c_l) \mid (0, \ldots, 0, c_1, \ldots, c_l) \in V_m\}$ and $W^* = \{(d_1, \ldots, d_{m-l}, 0, \ldots, 0) \mid (d_1, \ldots, d_{m-l}, 0, \ldots, 0) \in V_m\}$. Note that each $\gamma \in V_m$ can be uniquely expressed as $\gamma = (d_1, \ldots, d_{m-l}, c_1, \ldots, c_l)$. Set

$$j = u2^l + v,\ 0 \leq j \leq 2^m - 1,\ 0 \leq u \leq 2^{m-l} - 1,\ 0 \leq v \leq 2^l - 1 \qquad (4)$$

Hence $(d_1, \ldots, d_{m-l})$ is the binary representation of u and $(c_1, \ldots, c_l)$ is the binary representation of v.

Since $H_m = H_{m-l} \times H_l$, where $\times$ is the *Kronecker Product* [6], the jth row L_j of H_m can be expressed as $L_j = e_u \times \ell_v$, i.e., $L_j = (a_0\ell_v, a_1\ell_v, \ldots, a_{2^{m-l}-1}\ell_v)$ where $e_u = (a_0, a_1, \ldots, a_{2^{m-l}-1})$ is the uth row of H_{m-l} and ℓ_v is the vth row of H_l.

Comparing the j terms in the two sides of equality (2), we obtain $\langle R_0, R_j\rangle = \langle K, L_j\rangle$ where $K = (k_0, k_1, \ldots, k_{2^m-1})$. Rewrite K as $K = (K_0, K_1, \ldots, K_{2^{m-l}-1})$ where $K_i = (k_{i\cdot 2^l}, k_{i\cdot 2^l+1}, \ldots, k_{i\cdot 2^l+2^l-1})$, $i = 0, 1, \ldots, 2^{m-l} - 1$. Hence

$$\langle R_0, R_j\rangle = \sum_{i=0}^{2^{m-l}-1} a_i\langle K_i, \ell_v\rangle, \text{ where } e_u = (a_0, a_1, \ldots, a_{2^{m-l}-1}) \qquad (5)$$

where u and v are defined in (4).

Suppose that $P(y)$ is regular with respect to W. Then there exist integers $s_0, s_1, \ldots, s_{2^{m-l}-1}$, such that $s_j \geq 0$, $i = 0, 1, \ldots, 2^{m-l} - 1$, $s_0 + s_1 + \cdots + s_{2^{m-l}-1} = 2^{k-l}$, and $P(y)$ is regular with respect to W and $(s_0, s_1, \ldots, s_{2^{m-l}-1})$. Hence $K_i = s_i(1, \ldots, 1)$, where $i = 0, 1, \ldots, 2^{m-l} - 1$.

Consider $\gamma_j = (d_1, \ldots, d_{m-l}, c_1, \ldots, c_l)$, where γ_j is the binary representation of integer j and $\gamma_j \notin W^*$. Note that $\gamma_j \notin W^*$ implies $(c_1, \ldots, c_l) \neq (0, \ldots, 0)$ and hence $v \neq 0$, where v is defined in (4). Hence ℓ_v is $(1, -1)$ balanced.

Since $K_i = s_i(1, \ldots, 1)$, $i = 0, 1, \ldots, 2^{m-1} - 1$, we have $\langle K_i, \ell_v \rangle = 0$ for $i = 0, 1, \ldots, 2^{m-1}-1$ and $v \neq 0$. From (5), $\langle R_0, R_j \rangle = 0$. This means q_j is balanced, where $q_j = d_1p_1(y) \oplus \cdots \oplus d_{m-l}p_{m-l}(y) \oplus c_1p_{m-l+1}(y) \oplus \cdots \oplus c_lp_m(y)$ with $(d_1, \ldots, d_{m-l}, c_1, \ldots, c_l) = \gamma_j \notin W^*$. By using a nonsingular linear transform on the variables, we can change the special case of W and W^* to any general case. This proves (i) of the theorem.

Conversely, let us assume that for every $\gamma_j = (d_1, \ldots, d_{m-l}, c_1, \ldots, c_l)$, where γ_j is the binary representation of an integer j and $\gamma_j \notin W^*$, q_j is balanced, where $q_j = d_1p_1(y) \oplus \cdots \oplus d_{m-l}p_{m-l}(y) \oplus c_1p_{m-l+1}(y) \oplus \cdots \oplus c_lp_m(y)$. Write $j = u2^l + v$ where j, u and v are defined in (4). Hence $(d_1, \ldots, d_{m-l})$ is the binary representation of u and $(c_1, \ldots, c_l)$ is the binary representation of v.

Note that $\gamma_j \notin W^*$, if and only if $(c_1, \ldots, c_l) \neq (0, \ldots, 0)$, and $v \neq 0$. The balance of q_j implies that $\langle R_0, R_j \rangle = 0$. Hence from (5) we have

$$\sum_{i=0}^{2^{m-l}-1} a_i \langle K_i, \ell_v \rangle = 0, \text{ where } e_u = (a_0, a_1, \ldots, a_{2^{m-l}-1}) \tag{6}$$

Since u (or e_u, a row of H_{m-l}), can be arbitrary whenever $0 \leq u \leq 2^{m-l} - 1$, from (6), we conclude $(\langle K_0, \ell_v \rangle, \langle K_1, \ell_v \rangle, \ldots, \langle K_{2^{m-l}-1}, \ell_v \rangle) H_{m-l} = (0, 0, \ldots, 0)$, $v = 1, \ldots, 2^l - 1$, from which we have $\langle K_i, \ell_v \rangle = 0$, where $v = 1, \ldots, 2^l - 1$, $i = 0, 1, \ldots, 2^{m-l} - 1$.

We fix i with $0 \leq i \leq 2^{m-l} - 1$. Note that both $\langle K_i, \ell_v \rangle = 0$ and $\langle \ell_0, \ell_v \rangle = 0$ hold for $v = 1, \ldots, 2^l - 1$. Recall H_l is a Hadamard matrix. Hence $K_i = s_i\ell_0$ must hold for an integer s_i with $s_i \geq 0$. Recall $\ell_0 = (1, \ldots, 1)$. Hence $K_i = s_i(1, \ldots, 1)$ and $s_0 + s_1 + \cdots + s_{2^{m-l}-1} = 2^{k-l}$. By using a nonsingular linear transform on the variables, one can show that Part (ii) of the theorem also hold more general W and W^*. This completes the proof for the theorem.

It should be noted that Theorem 4 will be trivial when P is regular with respect to $W = \{0\}$, as in this case we have $W^* = V_m$. Another fact is that the XOR Lemma is a special case of Theorem 4. In fact, by letting $k \geq m$ and $l = m$ in Theorem 4, we have $W = V_m$ and $W^* = \{0\}$ and Theorem 4 becomes the XOR Lemma.

Acknowledgement

The authors would like to thank reviewers for their comments and suggestions that helped improve the presentation of this paper.

References

[1] C. Adams. The cast-128 encryption algorithm. Request for Comments RFC 2144, IETF, 1997.

[2] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Computing*, 17:210–229, 1988.

[3] Benny Chor, Oded Goldreich, Johan Håstad, Joel Friedman, Steven Rudich, and Roman Smolensky. The bit extraction problem or t-resilient functions. *IEEE Symposium on Foundations of Computer Science*, 26:396–407, 1985.

[4] Rudoff Lidl and Harald Niederreiter. *Finite Fields, Encyclopedia of Mathematics and Its Applications.* Cambridge University Press, 1983.

[5] A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptology.* CRC Press, Inc., 1997.

[6] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.

[7] X. M. Zhang, Y. Zheng, and Hideki Imai. Relating differential distribution tables to other properties of substitution boxes. *Designs, Codes and Cryptography*, 19:45–63, 2000.