A Note on a Conjecture concerning Symmetric Resilient Functions

K. Gopalakrishnan*
Department of Computer Science and Engineering
University of Nebraska - Lincoln
Lincoln, NE - 68588

D. G. Hoffman
Department of Discrete and Statistical Sciences
Auburn University
Auburn, AL - 36849

D. R. Stinson*
Department of Computer Science and Engineering and
Center for Communication and Information Sciences
University of Nebraska - Lincoln
Lincoln, NE - 68588

January 16, 1997

Abstract

In 1985, Chor *et al* [2] conjectured that the only 1-resilient symmetric functions are the exclusive-or of all n variables and its negation. In this note the existence of symmetric resilient functions is shown to be equivalent to the existence of a solution to a simultaneous subset sum problem. Then, using arithmetic properties of certain binomial coefficients, an infinite class of counterexamples to the conjecture is obtained.

*Supported by NSF grant CCR-9121051.

1 Introduction

The concept of resilient functions was introduced and studied in the papers Chor *et al* [2], Bennett *et al* [1] and Stinson [5]. Here is the definition. Let $n \geq m \geq 1$ be integers and suppose

$$f : \{0,1\}^n \longrightarrow \{0,1\}^m.$$

We will think of f as being a function that accepts n input bits and produces m output bits. Let $t \leq n$ be an integer. Suppose $(x_1, \ldots, x_n) \in \{0,1\}^n$, where the values of t arbitary inputs are fixed by an opponent, and the remaining $n-t$ input bits are chosen independently at random. Then f is said to be *t-resilient* provided that every possible output m-tuple is equally likely to occur. More formally, the property can be stated as follows: For every t-subset $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$, for every choice of $z_j \in \{0,1\}(1 \leq j \leq t)$, and for every $(y_1, \ldots, y_m) \in \{0,1\}^m$, we have

$$Pr(f(x_1, \ldots, x_n) = (y_1, \ldots, y_m) | x_{i_j} = z_j, 1 \leq j \leq t) = \frac{1}{2^m}.$$

We will refer to such a function f as an (n, m, t) - resilient function. Many interesting results on resilient functions can be found in [1], [2], [3] and [5].

Two possible applications of resilient functions are mentioned in [1] and [2]. The first application concerns the generation of shared random strings in the presence of faulty processors. The second involves renewing a partially leaked cryptographic key. They also are used in stream ciphers as combining functions for running-key generators that are resistant to a correlation attack (see, for example, Rueppel [4]).

A function

$$f : \{0,1\}^n \longrightarrow \{0,1\}^m$$

is called *symmetric* if for every permutation $\pi : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$, we have

$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}).$$

In 1985, Chor *et al* [2] conjectured that the only $(n, 1, 1)$-resilient symmetric functions are the exclusive-or of all n variables and its negation. In what follows, we will investigate the structure of symmetric resilient functions and disprove the conjecture.

2 Formulation as a subset sum problem

Let

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

be a symmetric function. Then it is clear that there exists a function

$$g : \{0, 1, \ldots, n\} \longrightarrow \{0,1\}$$

such that $f(x) = g(w(x))$ where $w(x)$ denotes the Hamming weight of the n-tuple x. This is because any two n-tuples with the same Hamming weight are permutations of each other.

Let $S = g^{-1}(0)$ and $T = g^{-1}(1)$. Any 1-resilient function is balanced in the first place (i.e., both the outputs 0 and 1 are equally likely). Hence we get the following equation.

$$\sum_{i \in S} \binom{n}{i} = \sum_{i \in T} \binom{n}{i} \tag{1}$$

The number of n-tuples x such that $x_1 = 0$ and $f(x) = 0$ should be the same as the number of n-tuples x such that $x_1 = 0$ and $f(x) = 1$, as f is an 1-resilient function. This yields the following equation, where binomial coefficients which do not make sense must be treated as zeroes.

$$\sum_{i \in S} \binom{n-1}{i} = \sum_{i \in T} \binom{n-1}{i} \tag{2}$$

Similarly, setting $x_1 = 1$ gives rise to the following equation.

$$\sum_{i \in S} \binom{n-1}{i-1} = \sum_{i \in T} \binom{n-1}{i-1}$$

However this equation could be inferred from equations (1) and (2), using Pascal's identity. Considering other variables apart from x_1 also do not yield any additional equations, as the function is symmetric. Thus it is clear that equations (1) and (2) are sufficient to ensure that the symmetric function f is a 1-resilient function.

As $S \cup T = \{0, 1, \ldots, n\}$ and

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n,$$

we can rewrite the above two equations as

$$\sum_{i=0}^{n} \binom{n}{i} \times g(i) = 2^{n-1} \tag{3}$$

and

$$\sum_{i=0}^{n} \binom{n-1}{i} \times g(i) = 2^{n-2}. \tag{4}$$

We could also think of g as a binary vector of size $n+1$. The above observations lead to the following lemma which shows that the existence problem of $(n, 1, 1)$-resilient functions (which is of combinatorial nature) reduces to a pure number theoretic problem in the symmetric case.

Lemma 2.1 *A binary vector g of size $n+1$ that simultaneously satisfies both equations (3) and (4) exists if and only if an $(n, 1, 1)$-resilient symmetric function exists.*

Let B_{n-j}, $0 \leq j \leq n-1$ be an integer vector of length $n+1$ defined as

$$B_{n-j} = \left(\binom{n-j}{0}, \binom{n-j}{1}, \binom{n-j}{2}, \ldots, \binom{n-j}{n} \right)$$

where binomial coefficients which do not make sense must be treated as zeroes. A simple extension of the previous lemma yields the following theorem.

Theorem 2.2 *A symmetric function f is t-resilient if and only if the induced vector g satisfies the equation*

$$B_{n-j} \circ g = 2^{n-j-1}$$

for all j, $0 \leq j \leq t$. In the above equation, g is to be treated as an integer vector rather than a binary vector and $\circ$ is the usual dot product over the ring of integers.

3 An infinite class of counterexamples

If f is the exclusive-or of all n variables then $g(0) = 0$, and zeroes and ones appear alternately in the g vector. If f is the negation of the exclusive-or of all n variables then $g(0) = 1$, and zeroes and ones appear alternately in the g vector. Hence the conjecture of Chor *et al* can be phrased as follows: *The only vectors g that satisfy both the equations (3) and (4) simultanously are the two alternating 0-1 vectors.* Actually there is an infinite class of counterexamples that violates the conjecture and in this section we will construct this infinite class.

Let n be an even integer. Let $g = (0, 1, 0, 1, \ldots, 0)$ be a vector of length $n+1$. Since g corresponds to the exclusive or of all n variables, g satisfies the equations (3) and (4).

Define a binary vector h of length $n+1$ as follows.

$$h(i) = \begin{cases} 0 & \text{if } i = k, k+1, n-k \text{ or } n-k+1 \text{ and } g(i) = 1 \\ 1 & \text{if } i = k, k+1, n-k \text{ or } n-k+1 \text{ and } g(i) = 0 \\ g(i) & \text{otherwise,} \end{cases} \tag{5}$$

where k is yet to be determined. Note that k and $n-k$ are of the same parity as n is even. Similarly $k+1$ and $n-k+1$ are of the same parity. Hence we have

$$\sum_{i=0}^{n} \binom{n}{i} \times h(i) = 2^{n-1} \pm \left[\binom{n}{k+1} - \binom{n}{k} + \binom{n}{n-k+1} - \binom{n}{n-k} \right]$$

and

$$\sum_{i=0}^{n} \binom{n-1}{i} \times h(i) = 2^{n-2} \pm \left[\binom{n-1}{k+1} - \binom{n-1}{k} + \binom{n-1}{n-k+1} - \binom{n-1}{n-k} \right].$$

Suppose

$$\binom{n}{k+1} - \binom{n}{k} + \binom{n}{n-k+1} - \binom{n}{n-k} = 0.$$

Then, using Pascal's identity and the symmetry of binomial coefficients, we get

$$\begin{aligned}
0 &= \binom{n-1}{k+1} + \binom{n-1}{k} - \binom{n-1}{k} - \binom{n-1}{k-1} + \\
&\quad \binom{n-1}{n-k+1} + \binom{n-1}{n-k} - \binom{n-1}{n-k} - \binom{n-1}{n-k-1} \\
&= \binom{n-1}{k+1} - \binom{n-1}{k-1} + \binom{n-1}{n-k+1} - \binom{n-1}{n-k-1} \\
&= \binom{n-1}{k+1} - \binom{n-1}{k} + \binom{n-1}{n-k+1} - \binom{n-1}{n-k}
\end{aligned}$$

Thus if h satisfies equation (3), then it automatically satisfies equation (4) also. But h satisfies equation (3) only if

$$\binom{n}{k+1} - \binom{n}{k} = \binom{n}{n-k} - \binom{n}{n-k+1}.$$

Dividing by $\binom{n}{k}$ throughout, we get

$$\frac{n-k}{k+1} - 1 = 1 - \frac{k}{n-k+1}.$$

Elementary arithmetic yields the following diophantine equation:

$$(n-2k)^2 = n+2$$

Let $r = n - 2k$. Then we have

$$\begin{aligned}
n &= r^2 - 2 \\
k &= \frac{1}{2}(r-2)(r+1).
\end{aligned}$$

Note that r has to be an even integer to ensure that n is even, and r must be greater than 2 to ensure that $k, k+1, n-k, n-k+1$ are distinct. Setting r to be any even integer determines values for n and k for which the h vector simultaneously satisfies both equations (3) and (4). Clearly h is not an alternating 0-1 vector and hence it provides a counterexample to the conjecture. Since there are infinitely many possible values for r, we get an infinite class of counterexamples. The smallest possible value of r is 4 and this implies $n = 14$ and $k = 5$. The corresponding counterexample is the vector $g = (0,1,0,1,0,0,1,1,0,0,1,1,0,1,0)$.

One might modify the conjecture to the following: *The only $(n,1,2)$-resilient symmetric functions are the exclusive-or of all n variables and its negation.* However this statement is not true either. In fact, all the members of the abovementioned infinite class are counterexamples of the modified conjecture also. This can be seen to be true by observing that the equation

$$\binom{n+1}{k+1} - \binom{n+1}{k} + \binom{n+1}{n-k+1} - \binom{n+1}{n-k} = 0$$

is an identity. We summarize the above discussion as the following theorem.

Theorem 3.1 *Let r be an even integer greater than 2. Let $n = r^2 - 2$ and $k = (r-2)(r+1)/2$. Then the h vector defined by equation (5) corresponds to an $(n, 1, 2)$-resilient symmetric function.*

4 Concluding Remarks

In this note the structure of t-resilient symmetric functions is investigated and the existence of an $(n, 1, t)$-resilient symmetric function is shown to be equivalent to the existence of a solution to a simultaneous subset sum problem. The conjecture [2] that the only 1-resilient symmetric functions are the exclusive-or of all n variables and its negation is disproved. Further, the conjecture is shown to be false even if we weaken it to 2-resilient symmetric functions.

Initially we found the counterexample to the original conjecture when $n = 14$ by trial and error. We observed that the counterexample is 2-resilient as well. The structure was then analyzed and extended to the infinite class of counterexamples given in section 3. However, the infinite class of counterexamples does not seem to extend any further in an obvious way. We also determined by an exhaustive computer search that these are the only counterexamples to the original conjecture up to $n = 30$.

These observations suggest the following open problems related to symmetric resilient functions:

1. Find the smallest *constant* t such that the following statement holds, or prove that the statement is false for any constant t.

   The only $(n, 1, t)$-resilient symmetric functions are the exclusive-or of all n variables and its negation.

   In this regard, we mention that Chor *et al* [2] have proved the exclusive-or of all n variables and its negation are the only $2n/3$-resilient symmetric functions.

2. Other than the exclusive-or of all n variables, its negation and those corresponding to the infinite class presented in this note, are there any symmetric functions f that are 1-resilient or 2-resilient?

References

[1] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Computing* **17** (1988), 210-229.

[2] Benny Chor, Oded Goldreich, Johan Hastad, Joel Friedman, Steven Rudich, and Roman Smolensky. The bit extraction problem or t-resilient functions. *Proc. 26th IEEE Symposium on Foundations of Computer Science* (1985), 396-407.

[3] J. Friedman. On the bit extraction problem. *Proc. 33rd IEEE Symposium on Foundations of Computer Science* (1992), 314-319.

[4] Rainer A. Rueppel. *Analysis and Design of Stream Ciphers*. Springer-Verlag, 1986.

[5] D. R. Stinson. Resilient functions and large sets of orthogonal arrays. To appear in *Congressus Numer.*, 1993.