An infinite class of counterexamples to a conjecture concerning non-linear resilient functions

D. R. Stinson
Computer Science and Engineering Department
and Center for Communication and Information Science
University of Nebraska
Lincoln, NE 68588-0115, U.S.A.

J. L. Massey
Signal and Information Processing Laboratory
Swiss Federal Institute of Technology
CH-8092 Zürich, Switzerland

January 7, 1994

Abstract

The main construction for resilient functions uses linear error-correcting codes; a resilient function constructed in this way is said to be linear. It has been conjectured that if there exists a resilient function, then there exists a linear function with the same parameters. In this note, we construct infinite classes of non-linear resilient functions from the Kerdock and Preparata codes. We also show that there do not exist linear resilient functions having the same parameters as the functions that we construct from the Kerdock codes. Thus, the aforementioned conjecture is disproved.

1 Introduction

The concept of resilient functions was introduced independently in the two papers Chor et al [4] and Bennett, Brassard and Robert [1]. Applications to cryptography are also given in [1] and [4]. Here is the definition: Let $n \geq k \geq 1$ be integers and suppose

$$f : \{0,1\}^n \rightarrow \{0,1\}^k.$$ 

We will think of $f$ as being a function that accepts $n$ input bits and produces $k$ output bits. Let $t \leq n$ be an integer. Suppose $(x_1, \ldots, x_n) \in \{0,1\}^n$, where the values of $t$ arbitrary input bits 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 $k$–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 $(y_1, \ldots, y_k) \in \{0,1\}^k$, we have

$$p(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \mid x_{i_j} = z_j, 1 \leq j \leq t) = \frac{1}{2^k}.$$
We will refer to such a function $f$ as an $(n,k,t)$-resilient function, or $(n,k,t)$-RF.

Many interesting results on resilient functions can be found in [1] and [4]. The basic problem is to maximize $t$ given $k$ and $n$; or equivalently, to maximize $k$ given $n$ and $t$. Here are some examples from [4] (all addition is modulo 2):

(1) $k = 1$, $t = n - 1$. Define $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n$.

(2) $k = n - 1$, $t = 1$. Define $f(x_1, \ldots, x_n) = (x_1 + x_2, x_2 + x_3, \ldots, x_{n-1} + x_n)$.

(3) $k = 2$, $n = 3h$, $t = 2h - 1$. Define $f(x_1, \ldots, x_{3h}) = (x_1 + \ldots + x_{2h}, x_{2h+1} + \ldots + x_{3h})$.

In fact, the $t$-resilient functions in all three of these examples are optimal. It is easy to see that $n \geq k + t$, so the first two examples are optimal. The result that $t < \left\lceil \frac{3n}{k+1} \right\rceil$ if $k = 2$ is more difficult and is proved in [4].

An $(n,k,t)$-RF, $f$, is said to be linear if $f(x) = xM$ for some $n \times k$ binary matrix $M$. The most important construction method for (linear) resilient functions uses (linear) binary codes. (We will be using several standard results from coding theory without proof; see MacWilliams and Sloane [9] for background information on error-correcting codes.) An $[n,k,d]$ code is a $k$-dimensional subspace $C$ of $(\mathbb{Z}_2)^n$ such that any two distinct vectors (or codewords) in $C$ have Hamming distance at least $d$. If $M$ is a $k \times n$ matrix whose rows form a basis for $C$, then $M$ is called a generating matrix for $C$.

The use of linear codes to form resilient functions relies on the following simple fact.

**Lemma 1** A $k \times n$ matrix $M$ of rank $k$ is the generating matrix of an $[n,k,d]$ code if and only if $d$ is the smallest number of columns that can be deleted from $M$ to give a matrix of rank less than $k$.

**Proof.** Let $d$ be the minimum distance of the code generated by $M$. Because the minimum distance of a linear code coincides with the minimum Hamming weight of its non-zero codewords, there exists a non-zero $k$-tuple $x$ such that $xM$ has weight $d$. Deleting the $d$ non-zero components of $xM$ gives the $(n-d)$-tuple $x\tilde{M} = (0, \ldots, 0)$ where $\tilde{M}$ is formed by deleting the corresponding $d$ columns of $M$. Hence $\tilde{M}$ has rank less than $k$. Conversely, if deleting $t$ columns of $M$ gives a matrix $\tilde{M}$ of rank less than $k$, then there is a non-zero $k$-tuple $x$ such that the $(n-t)$-tuple $x\tilde{M} = (0, \ldots, 0)$ and hence such that the non-zero codeword $xM$ has weight at most $t$. Thus $t \geq d$. \[\Box\]

The following theorem shows that linear resilient functions are equivalent to linear binary codes [1, 4]. The proof given in [1, 4] uses a result known as the “x-or lemma”; here we give a slightly more direct proof that uses Lemma 1.

**Theorem 1** The existence of an $[n,k,d]$ code is equivalent to the existence of a linear $(n,k,d-1)$-RF.

**Proof.** Let $M$ be a generating matrix for an $[n,k,d]$ code. Define the function $f : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^k$ by the rule $f(x) = xM^T$. We show that $f$ is an $(n,k,d-1)$-RF. Suppose an opponent fixes $t$ components of $x$, where $t < d$. Let $\bar{x}$ and $\tilde{M}$ be the $(n-t)$-tuple and matrix formed by deleting these $t$ components and the corresponding $t$ columns from $x$ and $M$, respectively. Then $f(x) = \bar{x}\tilde{M}^T + b$, where $b$ is some fixed $k$-tuple. By Lemma 1, $\tilde{M}^T$ has rank $k$, so the mapping $g : (\mathbb{Z}_2)^{n-t} \to (\mathbb{Z}_2)^k$, defined by the equation $g(\bar{x}) = \bar{x}\tilde{M}^T$,
is surjective. If \( \tilde{x} \) is chosen uniformly at random, then \( f(x) = g(\tilde{x}) + b \) is also uniformly random because the linearity of \( g \) guarantees that, for any value of \( f(x) - b \), the number of solutions \( \tilde{x} \) to \( g(\tilde{x}) = f(x) - b \) is equal to the cardinality of the kernel of \( g \). Hence \( f \) is indeed an \((n, k, d - 1)\)-RF.

Conversely, suppose \( f(x) = zM^T \) is a linear \((n, k, d - 1)\)-RF (where \( M \) is a \( k \times n \) binary matrix). Let \( C \) be the code with generating matrix \( M \). We need to show that \( C \) has distance at least \( d \). Suppose not; then by Lemma 1, it is possible to delete at most \( d - 1 \) columns from \( M \) to produce a matrix \( \tilde{M} \) having rank less than \( k \). Now if the opponent sets the components of \( x \) corresponding to the deleted columns of \( M \) to be zero, then the function \( f(x) = zM^T \) is not surjective and hence cannot be resilient.

It was posed as an open problem in [4], and explicitly conjectured in [1], that if there exists an \((n, k, t)\)-RF, then there exists a linear \((n, k, t)\)-RF. In the remainder of this note, we will disprove the conjecture by exhibiting an infinite class of counterexamples derived from the non-linear Kerdock codes.

2 Resilient functions, codes, and orthogonal arrays

Resilient functions turn out to be equivalent to certain “large sets” of orthogonal arrays, which we now define. An orthogonal array \( OA_{\lambda}(t, n, v) \) is a \( \lambda v^t \times n \) array of \( v \) symbols, such that in any \( t \) columns of the array every one of the possible \( v^t \) ordered pairs of symbols occurs in exactly \( \lambda \) rows. An orthogonal array is said to be simple if no two rows are identical. In this paper, we consider only simple orthogonal arrays and hence we will speak interchangeably of an orthogonal array and the set of \( n \)-tuples that forms its rows.

A large set of orthogonal arrays \( OA_{\lambda}(t, n, v) \) is defined to be a set of \( v^{n-t}/\lambda \) simple arrays \( OA_{\lambda}(t, n, v) \) such that every possible \( n \)-tuple of symbols occurs in exactly one of the OA’s in the set. (Equivalently, the union of the OA’s forms a (trivial) \( OA_{\lambda}(n, n, v) \).)

The following result was proved in [12].

**Theorem 2** An \((n, k, t)\)-RF is equivalent to a large set of \( OA_{2n-k-t}(t, n, 2) \)’s.

The correspondence between resilient functions and orthogonal arrays is this: for any \( k \)-tuple \((y_1, \ldots, y_k)\), the inverse image \( f^{-1}(y_1, \ldots, y_k) \) of an \((n, k, t)\)-RF, \( f \), is an orthogonal array \( OA_{2n-k-t}(t, n, 2) \); and the 2\( k \) OA’s thus obtained comprise a large set.

Suppose \( C \) is an \([n, k, d] \) code. Let \( C^\perp \) denote the dual code; \( C^{\perp} \) is an \([n, n-k, d'] \) linear code for some integer \( d' \). Suppose we write the codewords of \( C \) as the rows of a \( 2^k \times n \) array \( A \). It is well-known that \( A \) is an orthogonal array \( OA_{2^k-d'+1}(d' - 1, n, 2) \) (see for example [9, p. 139]). In fact, this is obvious since any \( d' - 1 \) columns of the generating matrix for \( C^\perp \) (= the parity check matrix for \( C \)) are linearly independent. (Further, any additive coset of \( C \) yields an \( OA_{2^{d'+1}}(d' - 1, n, 2) \), and these \( 2^{n-d} \) OA’s form a large set equivalent to an \((n, n-k, d'-1)\)-RF.)

Delsarte [5] generalized these ideas to non-linear codes. This generalization will be the basis of our method of constructing non-linear resilient functions. We will use the notation \((n, K, d) \) code to denote a binary code \( C \) (not necessarily linear), where \( C \subseteq \{0, 1\}^n \), \( |C| = K \), and any two codewords have Hamming distance at least \( d \). (Thus, an \([n, k, d] \) code is also an \((n, 2^k, d) \) code.) Delsarte observed that an \([n, k, d] \) code gives rise to an orthogonal array \( OA_{\lambda}(t, n, 2) \) where \( t \) is one less than the distance of the dual code. If an \((n, K, d) \) code is non-linear, then there is no such thing as the dual code, but nevertheless it is possible
to compute a dual distance $d'$ such that the array of codewords is an orthogonal array $OA_{\lambda}(d' - 1, n, 2)$, where $\lambda 2^{d'-1} = K$. This computation involves the distance enumerator of $C$; for details see [5] or [9], for example. In the case where $C$ is linear, the value $d'$ is in fact the distance of the dual code $C^\perp$.

From any (linear or non-linear) code, we have seen that one obtains an orthogonal array. In order to construct a resilient function, however, we need a large set of orthogonal arrays. In the linear case, we get the large set “for free” as cosets of $C$. We give a construction, which is almost as easy, that will apply to many known classes of non-linear codes.

Suppose $C$ is an $(n, K, d)$ code in which there exist $k$ co-ordinates such that every possible $k-$tuple occurs in exactly one codeword within the $k$ specified co-ordinates (of course, this implies $K = 2^k$). Then $C$ is said to be systematic. These $k$ co-ordinates are called information bits and the remaining $n - k$ co-ordinates are called parity-check bits.

We will use the following easy result.

**Theorem 3** If there exists a systematic $(n, K, d)$ code, $C$, having dual distance $d'$, then there is an $(n, n-k, d' -1) - RF$, where $K = 2^k$.

**Proof.** As described above, if we write the codewords of $C$ as the rows of an $K \times n$ array, then we have an $OA_{2^k-d'+1}(d' -1, n, 2)$. Without loss of (essential) generality, let us suppose that the first $k$ co-ordinates are the information bits. For any $(n-k)$-tuple $z = (z_1, \ldots, z_{n-k}) \in (Z_2)^{n-k}$, let $C_z$ denote the array obtained from $C$ by adding the $n-$tuple $(0, \ldots, 0, z_1, \ldots, z_{n-k})$ to every row (modulo 2). The resulting set of arrays

$$\{C_z : z \in (Z_2)^{n-k}\}$$

is obviously a large set of $OA_{2^k-d'+1}(d' -1, n, 2)$’s. By Theorem 2, there exists an $(n, n-k, d' -1) - RF$. \qed

### 3 Resilient functions from the Kerdock and Preparata codes

The Preparata and Kerdock codes are interesting classes of non-linear codes. The Preparata codes were constructed in 1968 [11]; the Kerdock codes were discovered in 1972 [8]. The properties of these codes are also discussed in [9], where the following results are proved.

**Theorem 4** Let $r \geq 3$ be odd. The Preparata code $P(r + 1)$ is a non-linear, systematic $(2^{r+1}, 2^{2r+1-2r-2}, 6)$ code having dual distance $d' = 2^r - 2^{(r-1)/2}$. The Kerdock code $K(r+1)$ is a non-linear, systematic $(2^{r+1}, 2^{2r+2}, 2^r - 2^{(r-1)/2})$ code having dual distance $d' = 6$.

Applying Theorem 3, we obtain resilient functions from these codes as follows.

**Theorem 5** For any odd integer $r \geq 3$, there is a non-linear $(2^{r+1}, 2r + 2, 2^r - 2^{(r-1)/2} - 1) - RF$ and a non-linear $(2^{r+1}, 2^{r+1} - 2r - 2, 5) - RF$.

The code $P(4)$ is the same as $K(4)$, and it is also known as the Nordstrom-Robinson code. It is a $(16, 256, 6)$ code which yields a large set of $OA_{8}(5, 16, 2)$’s and a $(16, 8, 5) - RF$. A method for computing this resilient function is presented in the following example.
Example 1 We begin with an encoding algorithm for the Nordstrom-Robinson code that is presented in [2, p. 328]. The information bits are $z_1, \ldots, z_8$ and the parity-check bits are $z_9, \ldots, z_{16}$. The parity-check bits are computed as follows (all operations modulo 2):

$$
z_9 = z_1 + z_2 + z_4 + z_7 + z_8 + (z_1 + z_5)(z_2 + z_3 + z_4 + z_6) + (z_2 + z_3)(z_4 + z_6)\\
z_{10} = z_2 + z_3 + z_5 + z_1 + z_8 + (z_2 + z_6)(z_3 + z_4 + z_5 + z_7) + (z_3 + z_4)(z_5 + z_7)\\
z_{11} = z_3 + z_4 + z_6 + z_2 + z_8 + (z_3 + z_7)(z_4 + z_5 + z_6 + z_1) + (z_4 + z_5)(z_6 + z_1)\\
z_{12} = z_4 + z_5 + z_7 + z_3 + z_8 + (z_4 + z_1)(z_5 + z_6 + z_7 + z_2) + (z_5 + z_6)(z_7 + z_2)\\
z_{13} = z_5 + z_6 + z_1 + z_4 + z_8 + (z_5 + z_2)(z_6 + z_7 + z_1 + z_3) + (z_6 + z_7)(z_1 + z_3)\\
z_{14} = z_6 + z_7 + z_2 + z_5 + z_8 + (z_6 + z_3)(z_7 + z_1 + z_2 + z_4) + (z_7 + z_1)(z_2 + z_4)\\
z_{15} = z_7 + z_1 + z_3 + z_6 + z_8 + (z_7 + z_4)(z_1 + z_2 + z_3 + z_5) + (z_1 + z_2)(z_3 + z_5)\\
z_{16} = \sum_{i=1}^{15} z_i.
$$

Then the $(16,8,5)$-RF, $f : \{0,1\}^{16} \rightarrow \{0,1\}^8$, can be computed according to the following algorithm:

1. Given $x = (x_1, \ldots, x_{16})$, compute parity-check bits $z_9, \ldots, z_{16}$ for the information bits $x_1, \ldots, x_8$.

2. Define $f(x) = (z_9 - x_9, \ldots, x_{16} - z_{16}) \mod 2$.

It remains to consider the existence of linear resilient functions with the above parameters. Theorem 1 states that existence of these (hypothetical) functions are equivalent to existence of linear codes as follows:

$$
\begin{array}{|c|c|}
\hline
\text{linear } (2^{r+1},2r + 2,2^r - 2^{(r-1)/2} - 1) \text{-RF} & \leftrightarrow & [2^{r+1},2r + 2,2^r - 2^{(r-1)/2}] \text{ code} \\
\hline
\text{linear } (2^{r+1},2^{r+1} - 2r - 2,5) \text{-RF} & \leftrightarrow & [2^{r+1},2^{r+1} - 2r - 2,6] \text{ code} \\
\hline
\end{array}
$$

It was proved in [6, Theorem 6.2] that there does not exist a $[2^{r+1} - 1,2^{r+1} - 2r - 2,5]$ code for any odd integer $r \geq 3$ (see also [3] for a slightly stronger result). This immediately implies the nonexistence of a linear code with the parameters of a Preparata code, since puncturing a $[2^{r+1},2^{r+1} - 2r - 2,6]$ code would produce a $[2^{r+1} - 1,2^{r+1} - 2r - 2,5]$ code. Hence, there do not exist linear $(2^{r+1},2^{r+1} - 2r - 2,5)$-RF’s for these values of $r$ (note that these resilient functions are the ones derived from the Kerdock codes).

As well, it is known that a $[64,12,28]$ code does not exist; see for example [13]. Hence, there is no $(64,12,27)$-RF. We summarize this discussion as follows.

Theorem 6 (1) For any odd integer $r \geq 3$, a $(2^{r+1},2^{r+1} - 2r - 2,5)$-RF exists, but no linear resilient function with these parameters exists.

(2) A $(64,12,27)$-RF exists, but no linear resilient function with these parameters exists.
4 Comments

It is apparently an open question as to whether there exist linear codes with the same parameters as Kerdock codes (except that it is known that there do not exist linear codes with the same parameters as $K(4)$ or $K(6)$; see above). So, for odd $r \geq 7$, the question of existence of linear $(2^{r+1}, 2r + 2, 2^r - 2^{(r-1)/2} - 1)$-RF's is undetermined.

The approach we have used in this paper to construct non-linear resilient functions is similar to that used by Maurer and Massey in [10] to construct non-linear perfect local randomizers. The main difference is that a perfect local randomizer (or PLR) is equivalent to an orthogonal array, whereas we require a large set of orthogonal arrays to obtain a resilient function. Maurer and Massey also use Preparata and Kerdock codes (in a similar fashion as we have done) to construct non-linear perfect local randomizers. Finally, our Theorem 6 shows that there does not exist a linear $(2r + 2, 2^{r+1}, 5)$ PLR for any odd $r \geq 3$. Maurer and Massey constructed non-linear $(2r + 2, 2^{r+1}, 5)$ PLR's for all odd $r \geq 3$ using the Kerdock codes. Thus our results answer in the affirmative the question posed by Maurer and Massey as to whether there are infinitely many instances of these parameters for which no linear PLR exists.

Some results on resilient functions over non-binary alphabets can be found in Gopakrishnan and Stinson [7]. For simplicity, we have restricted ourselves here to the binary case. Virtually all of our results, including Theorem 3, hold also for codes defined over arbitrary finite alphabets (with an additive group structure imposed) and for the appropriate non-binary generalization of the notion of a resilient function.

Acknowledgements

D. R. Stinson's research is supported by NSF Grant CCR-9121051.

References


