1-1-2012

Some constructions of mutually orthogonal latin squares and superimposed codes

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Dongvu Tonien
Australian National University, dong@uow.edu.au

Some constructions of mutually orthogonal latin squares and superimposed codes

Abstract

Superimposed codes is a special combinatorial structure that has many applications in information theory, data communication and cryptography. On the other hand, mutually orthogonal latin squares is a beautiful combinatorial object that has deep connection with design theory. In this paper, we draw a connection between these two structures. We give explicit construction of mutually orthogonal latin squares and we show a method of generating new larger superimposed codes from an existing one by using mutually orthogonal latin squares. If n denotes the number of codewords in the existing code then the new code contains n2 codewords. Recursively, using this method, we can construct a very large superimposed code from a small simple code. Well-known constructions of superimposed codes are based on algebraic Reed-Solomon codes and our new construction gives a combinatorial alternative approach.

Keywords

mutually, codes, superimposed, latin, squares, constructions, orthogonal

Disciplines

Engineering | Science and Technology Studies

Publication Details

Seberry, J. & Tonien, D. (2012). Some constructions of mutually orthogonal latin squares and superimposed codes. Discrete Mathematics, Algorithms and Applications, 4 (3), 1250022-1-1250022-8.

Discrete Mathematics, Algorithms and Applications
Vol. 4, No. 3 (2012) 1250022 (8 pages)

DOI: 10.1142/S179383091250022X

World Scientific
www.worldscientific.com

SOME CONSTRUCTIONS OF MUTUALLY ORTHOGONAL LATIN SQUARES AND SUPERIMPOSED CODES

JENNIFER SEBERRY*,‡ and DONGVU TONIEN†,§

*School of Computer Science and Software Engineering
University of Wollongong, Australia

†Mathematical Sciences Institute
Australian National University, Australia

‡jennie@uow.edu.au

§dongvu.tonien@gmail.com

Received 26 January 2011
Published 1 August 2012

Superimposed codes is a special combinatorial structure that has many applications in information theory, data communication and cryptography. On the other hand, mutually orthogonal latin squares is a beautiful combinatorial object that has deep connection with design theory. In this paper, we draw a connection between these two structures. We give explicit construction of mutually orthogonal latin squares and we show a method of generating new larger superimposed codes from an existing one by using mutually orthogonal latin squares. If n denotes the number of codewords in the existing code then the new code contains n^2 codewords. Recursively, using this method, we can construct a very large superimposed code from a small simple code. Well-known constructions of superimposed codes are based on algebraic Reed–Solomon codes and our new construction gives a combinatorial alternative approach.

Keywords: Superimposed codes; difference function family; recursive construction.

1. Introduction

The two equivalent concept, superimposed codes and cover-free families, were introduced by Kautz and Singleton [8]. Since then, these combinatorial structures have been studied extensively and appeared to have many applications in information theory, molecular biology [5] and cryptography including information retrieval, data communication, magnetic memories [8], group testing [1, 2], key distribution [7, 9, 10], DNA library screening [3, 4], tracing pirate media [12] and conflict resolution in multiple access channels [1]. In these applications, it is desirable to construct superimposed codes that have large number of codewords of relatively small length.

Well-known constructions of superimposed codes are based on algebraic Reed–Solomon codes [4, 8]. In this paper, we present a new class of superimposed codes

recursively constructed by combinatorial method. We link superimposed codes to another beautiful structure – the mutually orthogonal latin squares. We show that it is possible to combine a collection of mutually orthogonal latin squares with a superimposed code to generate a larger superimposed code. We give some explicit construction of mutually orthogonal latin squares and show that by using these mutually orthogonal latin squares we can generate explicitly large superimposed codes with small length. Compared to the number of codewords, the length of our superimposed codes is of logarithmic order.

The paper is organized as follows. In Sec. 2, we give definitions of latin squares, mutually orthogonal latin squares and superimposed codes. We give some explicit constructions of mutually orthogonal latin squares in Sec. 3. In Sec. 4, we present our method of combining a superimposed code with a collection of mutually orthogonal latin squares. Main theorems will be stated in Sec. 5. We will show that our combination of a superimposed code with a collection of mutually orthogonal latin squares indeed can generate a larger superimposed code and this construction can be used recursively to construction of a very large and efficient superimposed codes. Proofs of main theorems will be provided in Sec. 6.

2. Definitions

In this section, we give definitions of mutually orthogonal latin squares and superimposed codes. Throughout the paper, for a matrix M of size $n \times m$, we use the notation $M_{r,c}$ to denote the matrix entry at row r and column c, where $1 \leq r \leq n$ and $1 \leq c \leq m$.

2.1. *Mutually orthogonal latin squares*

Definition 2.1. A square matrix L of size $n \times n$ is called a *latin square* if any row of L and any column of L contains a permutation of the numbers $1, \ldots, n$.

Example: The following matrix is a latin square. Each row and each column of the matrix contains a permutation of the numbers 1, 2, 3, 4, 5.

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

Definition 2.2. Let $L^{(1)}, \ldots, L^{(m)}$ be square matrices of the same size $n \times n$. Then the collection $\mathcal{L} = \{L^{(1)}, \ldots, L^{(m)}\}$ is called a *mutually orthogonal latin squares* if the following two conditions are satisfied:

(1) each matrix $L^{(i)}$ is a latin square; and

(2) for any two matrices $L^{(i)}$ and $L^{(j)}$, n^2 order pairs $(L^{(i)}_{r,c}, L^{(j)}_{r,c})$ obtained from the matrix entries of $L^{(i)}$ and $L^{(j)}$ are all distinct.

We will say that $\mathcal{L}$ is a (n, m)-MOLS.

Example: The following two matrices are two mutually orthogonal latin squares. Apart from being latin squares, these two matrices are orthogonal. To verify that, we look at the entries of matrix A that contain number 1: these are (row 1, column 5), (row 2, column 1), (row 3, column 2), (row 4, column 3), and (row 5, column 4). In these entries, matrix B contains numbers 3, 5, 2, 4, 1, respectively. Similarly, the entries of matrix A that contain number 2 are: (row 1, column 1), (row 2, column 2), (row 3, column 3), (row 4, column 4), and (row 5, column 5). The corresponding entries on matrix B contain numbers 1, 3, 5, 2, 4.

$$A = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 4 & 2 & 5 & 3 \\ 5 & 3 & 1 & 4 & 2 \\ 4 & 2 & 5 & 3 & 1 \\ 3 & 1 & 4 & 2 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}.$$

2.2. *Superimposed codes*

A binary code Γ of size n and length ℓ is a subset of $\{0,1\}^\ell$ containing n elements called codewords. Each $\alpha \in \{0,1\}^\ell$ is written as $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ where $\alpha_i \in \{0,1\}$ is called the ith component of α.

If all codewords of Γ have the same weight, then Γ is called a *constant-weight* code.

The code Γ can be represented as a binary matrix of size $n \times \ell$ where n rows of the matrix represents n codewords. From now on, we abuse the language by using the same notation Γ to denote the code and its matrix. So for $1 \leq i \leq n$ and $1 \leq j \leq \ell$, the matrix entry $\Gamma_{i,j}$ is equal to the jth component of the ith codeword of the code Γ.

Definition 2.3. Let Γ be a binary code containing n codewords of length ℓ. Let t be a positive integer. Γ is called a t-superimposed code if for any $t+1$ rows $r_1, r_2, \ldots, r_t$ and r of the matrix Γ, such that $r \notin \{r_1, r_2, \ldots, r_t\}$, then there exists a column c such that

$$\Gamma_{r_1,c} = \Gamma_{r_2,c} = \cdots = \Gamma_{r_t,c} = 0, \quad \text{and} \quad \Gamma_{r,c} = 1.$$

Note that in the above definition, the t rows $r_1, r_2, \ldots, r_t$ do not require to be distinct.

3. Construction of Mutually Orthogonal Latin Squares

Theorem 3.1. *Let n, m, ρ be positive integers such that $m > 1$ and $\gcd(n, \rho) = \gcd(n, m!) = 1$; let $\eta_1, \ldots, \eta_m$ be arbitrary integers; and let $\pi_1, \ldots, \pi_n$ be a*

permutation of $1, 2, \ldots, n$. *Define*

$$1 \le L_{r,c}^{(i)} \le n, \quad L_{r,c}^{(i)} = \rho ic + \pi_r + \eta_i \pmod{n}.$$

Then $L^{(1)}, \ldots, L^{(m)}$ *is a collection of mutually orthogonal latin squares of size* $n \times n$.

Proof. If $L_{r,c_1}^{(i)} = L_{r,c_2}^{(i)}$ then $\rho ic_1 = \rho ic_2 \pmod{n}$. Since $\gcd(n, \rho) = \gcd(n, m!) = 1$, it follows that $c_1 = c_2$. Similarly, if $L_{r_1,c}^{(i)} = L_{r_2,c}^{(i)}$ then $\pi_{r_1} = \pi_{r_2}$ and thus $r_1 = r_2$. This shows that $L^{(i)}$ is a latin square.

To show that they are mutually orthogonal, we fix two values i and j. Suppose that $L_{r_1,c_1}^{(i)} = L_{r_2,c_2}^{(i)}$ and $L_{r_1,c_1}^{(j)} = L_{r_2,c_2}^{(j)}$. Then $\rho ic_1 + \pi_{r_1} = \rho ic_2 + \pi_{r_2}$ and $\rho jc_1 + \pi_{r_1} = \rho jc_2 + \pi_{r_2}$. So $\pi_{r_1} - \pi_{r_2} = \rho i(c_2 - c_1) = \rho j(c_2 - c_1) \pmod{n}$. It follows that $\rho(i-j)(c_2 - c_1) = 0 \pmod{n}$. This shows that $c_1 = c_2$ and $r_1 = r_2$. So the matrices are mutually orthogonal. □

Using Theorem 3.1 with $n = 5$, $m = 4$, $\rho = 2$, $\eta_1 = 1$, $\eta_2 = 0$, $\eta_3 = 4$, $\eta_4 = 1$, $\pi_1 = 2$, $\pi_2 = 1$, $\pi_3 = 5$, $\pi_4 = 4$, $\pi_5 = 3$, we have the following four mutually orthogonal latin squares

$$L^{(1)} = \begin{pmatrix} 5 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 5 & 2 \\ 3 & 5 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}, \quad L^{(2)} = \begin{pmatrix} 1 & 5 & 4 & 3 & 2 \\ 5 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 5 \\ 3 & 2 & 1 & 5 & 4 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix},$$

$$L^{(3)} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \quad L^{(4)} = \begin{pmatrix} 1 & 4 & 2 & 5 & 3 \\ 5 & 3 & 1 & 4 & 2 \\ 4 & 2 & 5 & 3 & 1 \\ 3 & 1 & 4 & 2 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}.$$

Similar to Theorem 3.1, we have the following construction.

Theorem 3.2. *Let* n, m, ρ *be positive integers such that* $m > 1$ *and* $\gcd(n, \rho) = \gcd(n, m!) = 1$; *let* $\eta_1, \ldots, \eta_m$ *be arbitrary integers*; *and let* $\pi_1, \ldots, \pi_n$ *be a permutation of* $1, 2, \ldots, n$. *Define*

$$1 \le L_{r,c}^{(i)} \le n, \quad L_{r,c}^{(i)} = \rho ir + \pi_c + \eta_i \pmod{n}.$$

Then $L^{(1)}, \ldots, L^{(m)}$ *is a collection of mutually orthogonal latin squares of size* $n \times n$.

Corollary 3.3. *Let* p *be a prime number and* $m < p$. *Then there exists a collection of* m *mutually orthogonal latin squares of size* $p \times p$. *These mutually orthogonal latin squares can be constructed as follows*

- $1 \le L_{r,c}^{(i)} \le p$, $L_{r,c}^{(i)} = ir + c \pmod{p}$; *or*
- $1 \le L_{r,c}^{(i)} \le p$, $L_{r,c}^{(i)} = ic + r \pmod{p}$.

4. Recursive Construction of Superimposed Codes

In this section, we present a recursive construction of superimposed codes by using a collection of mutually orthogonal latin squares. The plan is as follows. First, we show that given a binary code Γ that contains n codewords of length ℓ, by using a (n, m)-MOLS $\mathcal{L}$, we can construct a new binary code $\mathcal{L}\Gamma$ that contains n^2 codewords of length ℓm. Next, we show that by choosing the right parameters, our construction preserves the superimposed property. Our main theorem shows that if $m = t + 1$ then from a t-superimposed code Γ our construction gives rise another t-superimposed code $\mathcal{L}\Gamma$.

4.1. *Combining MOLS and superimposed codes*

In this section, we describe in details how to combine a MOLS $\mathcal{L}$ with a binary code Γ to produce a new binary code $\mathcal{L}\Gamma$. In order to combine, the two objects, MOLS and code, need to agree on the parameters. Here Γ is a code that contains n codewords and $\mathcal{L}$ is a (n, m)-MOLS — that is a collection of m latin matrices $L^{(1)}, \ldots, L^{(m)}$ of size $n \times n$.

Construct the binary matrix $\mathcal{L}\Gamma$ as follows.

$$\mathcal{L}\Gamma = \begin{pmatrix}
\Gamma_{L^{(1)}_{1,1}} & \Gamma_{L^{(2)}_{1,1}} & \cdots & \Gamma_{L^{(m)}_{1,1}} \\
\Gamma_{L^{(1)}_{1,2}} & \Gamma_{L^{(2)}_{1,2}} & \cdots & \Gamma_{L^{(m)}_{1,2}} \\
\vdots & \vdots & & \vdots \\
\Gamma_{L^{(1)}_{1,n}} & \Gamma_{L^{(2)}_{1,n}} & \cdots & \Gamma_{L^{(m)}_{1,n}} \\
\Gamma_{L^{(1)}_{2,1}} & \Gamma_{L^{(2)}_{2,1}} & \cdots & \Gamma_{L^{(m)}_{2,1}} \\
\Gamma_{L^{(1)}_{2,2}} & \Gamma_{L^{(2)}_{2,2}} & \cdots & \Gamma_{L^{(m)}_{2,2}} \\
\vdots & \vdots & & \vdots \\
\Gamma_{L^{(1)}_{2,n}} & \Gamma_{L^{(2)}_{2,n}} & \cdots & \Gamma_{L^{(m)}_{2,n}} \\
\vdots & \vdots & & \vdots \\
\Gamma_{L^{(1)}_{n,1}} & \Gamma_{L^{(2)}_{n,1}} & \cdots & \Gamma_{L^{(m)}_{n,1}} \\
\Gamma_{L^{(1)}_{n,2}} & \Gamma_{L^{(2)}_{n,2}} & \cdots & \Gamma_{L^{(m)}_{n,2}} \\
\vdots & \vdots & & \vdots \\
\Gamma_{L^{(1)}_{n,n}} & \Gamma_{L^{(2)}_{n,n}} & \cdots & \Gamma_{L^{(m)}_{n,n}}
\end{pmatrix}.$$

We recall that $L^{(i)}_{r,c}$ is the entry of the latin matrix $L^{(i)}$ at the row r and column c — which is a number among $1, 2, \ldots, n$. Γ_j is the jth codeword of Γ. So $\Gamma_{L^{(i)}_{r,c}}$ does make sense. If codewords Γ_j have length ℓ then the new matrix $\mathcal{L}\Gamma$ is a matrix

of size $n^2 \times m\ell$. This matrix gives rise to a new binary code $\mathcal{L}\Gamma$ which contains n^2 codewords of length $m\ell$.

If Γ is a constant-weight code then clearly the new code $\mathcal{L}\Gamma$ is also a constant-weight code. If each codeword of Γ has weight w then each codeword of $\mathcal{L}\Gamma$ has weight mw. In the next section, we state our main theorem which asserts that if we choose $m = t + 1$ then given an existing t-superimposed code Γ, the new code $\mathcal{L}\Gamma$ generated by our construction is also t-superimposed.

5. Main Theorems

We are now ready to state our new theorems. The first theorem assert the correctness of our construction, that is the construction preserves the superimposedness property.

Theorem 5.1. *Let Γ be a t-superimposed code containing n codewords of length ℓ, and $\mathcal{L}$ be a $(n, t+1)$-MOLS. Then the binary code $\mathcal{L}\Gamma$ containing n^2 codewords of length $\ell(t+1)$ is also a t-superimposed code. Moreover, if Γ is a constant-weight code then $\mathcal{L}\Gamma$ is also a constant-weight code. In this case, if the codewords of Γ have weight w then the codewords of $\mathcal{L}\Gamma$ have weight $w(t+1)$.*

The next three theorems show that we can apply the above theorem to generate practical t-superimposed codes — codes that have many codewords and relatively short length.

Theorem 5.2. *For any prime p, and for any natural number z, there exists a binary $(p-2)$-superimposed constant-weight code containing p^{2^z} codewords of length p^{z+1} and weight p^z.*

Theorem 5.3. *Let t be a positive number and p be the smallest prime that is greater than $t+1$. Then for any natural number z, it is possible to construct a binary t-superimposed constant-weight code containing p^{2^z} codewords of length $p(t+1)^z$ and weight $(t+1)^z$.*

Theorem 5.4. *Let n, t, z be positive integers. If $\gcd(n, (t+1)!) = 1$ then from a binary t-superimposed code containing n codewords of length ℓ, it is possible to construct a new binary t-superimposed code containing n^{2^z} codewords of length $\ell(t+1)^z$. Moreover, if the original code is a constant-weight code then the new code is also a constant-weight code. In this case, if the codewords of the original code have weight w, then the codewords of the new code have weight $w(t+1)^z$.*

6. Proofs of Theorems

Proof of Theorem 5.1. Observe that the matrix $\mathcal{L}\Gamma$ contains n^2 rows divided into n blocks, each block contains n rows. For $1 \le b \le n$, $1 \le r \le n$, let $\langle b, r\rangle$

denote the index of the rth row in the bth block of $\mathcal{L}\Gamma$, e.g., $\langle b, r\rangle = r + (b-1)n$. The $\langle b, r\rangle$th codeword of $\mathcal{L}\Gamma$, $\mathcal{L}\Gamma_{\langle b,r\rangle}$, consists of $t+1$ rows of Γ as follows

$$\mathcal{L}\Gamma_{\langle b,r\rangle} = \Gamma_{L_{b,r}^{(1)}}\Gamma_{L_{b,r}^{(2)}}\cdots\Gamma_{L_{b,r}^{(t+1)}}.$$

Now we prove that $\mathcal{L}\Gamma$ is a t-superimposed code. Take $t+1$ rows of $\mathcal{L}\Gamma$, $\langle b_1, r_1\rangle, \ldots, \langle b_t, r_t\rangle, \langle b, r\rangle$, such that $\langle b, r\rangle \notin \{\langle b_1, r_1\rangle, \ldots, \langle b_t, r_t\rangle\}$,

$$\begin{array}{rcccc}
\mathcal{L}\Gamma_{\langle b_1,r_1\rangle} & = & \Gamma_{L_{b_1,r_1}^{(1)}} & \Gamma_{L_{b_1,r_1}^{(2)}} & \cdots \quad \Gamma_{L_{b_1,r_1}^{(t+1)}} \\
\mathcal{L}\Gamma_{\langle b_2,r_2\rangle} & = & \Gamma_{L_{b_2,r_2}^{(1)}} & \Gamma_{L_{b_2,r_2}^{(2)}} & \cdots \quad \Gamma_{L_{b_2,r_2}^{(t+1)}} \\
\vdots & & \vdots & \vdots & \qquad\quad \vdots \\
\mathcal{L}\Gamma_{\langle b_t,r_t\rangle} & = & \Gamma_{L_{b_t,r_t}^{(1)}} & \Gamma_{L_{b_t,r_t}^{(2)}} & \cdots \quad \Gamma_{L_{b_t,r_t}^{(t+1)}} \\
\hline
\mathcal{L}\Gamma_{\langle b,r\rangle} & = & \Gamma_{L_{b,r}^{(1)}} & \Gamma_{L_{b,r}^{(2)}} & \cdots \quad \Gamma_{L_{b,r}^{(t+1)}}.
\end{array}$$

Now suppose that for any $1 \le k \le t+1$, we have

$$L_{b,r}^{(k)} \in \{L_{b_1,r_1}^{(k)}, L_{b_2,r_2}^{(k)}, \ldots, L_{b_t,r_t}^{(k)}\}.$$

Let S_k denote the set of all indices u such that $1 \le u \le t$ and $L_{b,r}^{(k)} = L_{b_u,r_u}^{(k)}$, then S_k is not an empty set. From Pigeon Hole Principle, there must exist an index $1 \le u \le t$ that belongs to at least two sets, say S_{k_1} and S_{k_2} with $k_1 \ne k_2$. We have

$$L_{b,r}^{(k_1)} = L_{b_u,r_u}^{(k_1)} \quad \text{and} \quad L_{b,r}^{(k_2)} = L_{b_u,r_u}^{(k_2)}.$$

Since $L^{(k_1)}$ and $L^{(k_2)}$ are orthogonal, it follows that $b_u = b$ and $r_u = r$. Hence $\langle b, r\rangle = \langle b_u, r_u\rangle$, a contradition. Therefore, there must exist $1 \le k \le t+1$ such that

$$L_{b,r}^{(k)} \notin \{L_{b_1,r_1}^{(k)}, L_{b_2,r_2}^{(k)}, \ldots, L_{b_t,r_t}^{(k)}\},$$

then since Γ is t-superimposed, there exists column $1 \le c \le \ell$ such that

$$\Gamma_{L_{b,r}^{(k)},c} = 1 \quad \text{and} \quad \Gamma_{L_{b_1,r_1}^{(k)},c} = \Gamma_{L_{b_2,r_2}^{(k)},c} = \cdots = \Gamma_{L_{b_t,r_t}^{(k)},c}.$$

This shows that the new code $\mathcal{L}\Gamma$ is t-superimposed. □

Proof of Theorem 5.4. Suppose we have a binary t-superimposed code Γ containing n codewords of length ℓ. Since $\gcd(n, (t+1)!) = 1$, using Theorem 3.1 or Theorem 3.2 to construct a collection of $t+1$ mutually orthogonal latin squares of size $n \times n$. Using Theorem 5.1 to construct a t-superimposed code containing n^2 codewords of length $\ell(t+1)$. Since $\gcd(n^2, (t+1)!) = 1$, using Theorem 3.1 or Theorem 3.2 again to construct a collection of $t+1$ mutually orthogonal latin squares of size $n^2 \times n^2$. Again, using Theorem 5.1 to construct a t-superimposed code containing n^4 codewords of length $\ell(t+1)^2$. Eventually, after z times of doing this, we have a t-superimposed code containing n^{2^z} codewords of length $\ell(t+1)^z$. □

Proof of Theorem 5.3. Let I_p be the identity matrix of size $p \times p$. Then the corresponding code I_p is trivially a t-superimposed constant-weight code which contains p codewords of length p and weight 1. Since $p > t + 1$ and p is prime, we have $\gcd(p, (t + 1)!) = 1$. Therefore, by Theorem 5.4, for each natural number z, we can construct a binary t-superimposed constant-weight code containing p^{2^z} codewords of length $p(t + 1)^z$ and weight $(t + 1)^z$. □

Proof of Theorem 5.2. Theorem 5.2 is a direct consequence of Theorem 5.3. □

References

[1] A. D. Bonis and U. Vaccaro, Constructions of generalized superimposed codes with applications to group testing and conflict resolution in multiple access channels, *Theor. Comput. Sci.* **306** (2003) 223–243.

[2] K. A. Bush, W. T. Federer, H. Pesotan and D. Raghavarao, New combinatorial designs and their application to group testing, *J. Stat. Plann. Infer.* **10** (1984) 335–343.

[3] A. G. Dyachkov, A. J. Macula and V. V. Rykov, On optimal parameters of a class of superimposed codes and designs, *1998 IEEE Int. Symp. Information Theory* (1998), p. 363.

[4] A. G. Dyachkov, A. J. Macula and V. V. Rykov, New constructions of superimposed codes, *IEEE Trans. Inf. Theory* **46** (2000) 284–290.

[5] A. G. Dyachkov, A. J. Macula and V. V. Rykov, New applications and results of superimposed code theory arising from the potentialities of molecular biology, in *Numbers, Information and Complexity* (Kluwer Academic Publishers, 2000), pp. 265–282.

[6] A. G. Dyachkov, A. J. Macula, D. C. Torney, P. A. Vilenkin and S. M. Yekhanin, New results in the theory of superimposed codes, in *Proc. ACCT-7* (Bansko, Bulgaria, 2000), pp. 126–136.

[7] M. Dyer, T. Fenner, A. Frieze and A. Thomason, On key storage in secure networks, *J. Cryptol.* **8** (1995) 189–200.

[8] W. H. Kautz and R. C. Singleton, Nonrandom binary superimposed codes, *IEEE Trans. Inf. Theory* **10** (1964) 363–377.

[9] C. J. Mitchell and F. C. Piper, Key storage in secure networks, *Discrete Appl. Math.* **21** (1988) 215–228.

[10] K. A. S. Quinn, Bounds for key distribution patterns, *J. Cryptol.* **12** (1999) 227–239.

[11] D. Tonien and R. Safavi-Naini, Recursive constructions of secure codes and hash families using difference function families, *J. Combin. Theor. A* **113**(4) (2006) 664–674.

[12] D. Tonien and R. Safavi-Naini, An efficient single-key pirates tracing scheme using cover-free families, in *Proc. 4th Int. Conf. Applied Cryptography and Network Security (ACNS'06)*, Lecture Notes in Computer Science, Vol. 3989 (2006), pp. 82–97.