I.J. Wireless and Microwave Technologies, **2011, 5, 1-8**
Published Online October 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.05.01

Available online at http://www.mecs-press.net/ijwmt

Frameproof Codes Based on The Generalized Difference Function Families

Qingjun CAI, Yuli ZHANG

School of Mathematics and Information Science, Guangzhou university, Guangdong, China

Abstract

The frameproof codes are used in copyright protecting. Motivated by the method of constructing frameproof codes coined by D.Tonien etal, in this paper, we introduced a new combinatorial designs which in fact generalized the difference function family introduced by D.Tonien. The new designs can be constructed from difference matrix efficiently. By using the new designs we construct more larger number of frameproof codes .

Index Terms: Frameproof codest; difference function family ; difference matrix

1. Introduction

Frameproof codes with tracing baleful users property are often used for copyright and piracy tracing [1][2][3][4][5]. Safavi-Naini et al used a kind of function family satisfying some special properties to construct several kinds of anti-pirate codes. Frameproof code is a kind of anti-pirate code. Recently, D. Tonien and Safavi-Naini introduced the notion of difference function families in [5], and used these designs to give all kind of anti-pirate codes except secure codes. In this paper, we generalize the notion of difference function families, and introduce a new combinatorial designs, which is in fact the generalization of difference matrix, called generalized difference matrix. The new designs can be efficiently construct from any difference matrix, thus we can provide more frameproof codes. So the conclusion in [5] is the special case of our work.

* Corresponding author.
E-mail address: zyuli456@163.com

2. Basic Definitions

A. frameproof code

Let A be an alphabet of size m. An (l,n,m) code Γ of length l and size n over A is a collection of n elements(called codewords)of A^l. Each $\bar{x} \in A^l$ is written in the form $\bar{x} = (x_1, x_2, \cdots, x_l)$. The matrix form of Γ is an $n \times l$ matrix whose rows are codewords of Γ. For a subset $\Lambda \subset \Gamma$ and a position $1 \le i \le l$, we define the projection of Γ on the position i as $\pi_i(\Lambda) = \{x_i \mid \bar{x} \in \Lambda\}$, and the set of descendants of Λ as desc$(\Lambda) = \prod_{i=1}^{l} \pi_i(\Lambda)$. The set of descendants is a subset of A that can be constructed by a coalition of users who have the codewords in Γ. If $\bar{x}^* \in$ desc(Λ), then codewords in Λ are called parents of $\bar{x}^*$. Let w be a positive integer and desc$^w(\Gamma) = \bigcup_{\Lambda \subset \Gamma, |\Lambda| \le w}$ desc(Λ).

In the following context, we let Γ be an (l,n,m) code and w be a positive integer.

Definition1 Γ is called $w-$ **frameproof** if for any $\Lambda \subseteq \Gamma$ such that $0 < |\Lambda| \le w$, we have **desc**$(\Lambda) \cap \Gamma = \Lambda$ .Let $w - FP(l,n,m)$ denote above code, and sometimes $w - FP$ for short.

B. Generalized Difference Function Families

Let $[n] = \{1,2,\cdots,n\}$. Assume $|A| = m$. An $(l,n,m)-$ hash family H is a collection of l functions which map $[n]$ into A. The **Matrix form** of H is an $n \times l$ matrix whose columns represent functions of H ,that is, the matrix entry at row i and column j is $h(i)$ where $h(x)$ is the j th function of H.

Definition2 An $(n,k,t)-$ generalized difference matrix is a $k \times n$ integer matrix $D = (d_{i,j})$ such that for any two different column index i_1 and i_2 , there exit no row index $u_1, u_2, \cdots, u_t$ such that $d_{u_1,i_1} - d_{u_2,i_1} \equiv d_{u_1,i_2} - d_{u_2,i_2}$,

$\cdots, d_{u_{t-1},i_1} - d_{u_t,i_1} \equiv d_{u_{t-1},i_2} - d_{u_t,i_2} \pmod{n}$, but there exits row index $v_1, v_2, \cdots, v_{t-1}$, such that $d_{v_1,i_1} - d_{v_2,i_1} \equiv d_{v_1,i_2} - d_{v_2,i_2}$,

$\cdots, d_{v_{t-1},i_1} - d_{v_t,i_1} \equiv d_{v_{t-1},i_2} - d_{v_t,i_2} \pmod{n}$.

Remark1 In above theorem, the first condition is called R_t **property**, and the last condition called L_t **property** for short.

Definition3 Let n, s, I and J be positive integers such that $J > 1$ and $I \le n$. An $(n; I, J, s)-$ **generalized difference function family** is a function family $\Phi = (\varphi_{i,j}) \subseteq ([n]^{[n]})_{I \times J}$

of size which satisfies the following condition: for any s different indices $j_1,\cdots,j_s$, if $\varphi_{i_1,j_1}(x)=\varphi_{i_2,j_1}(y)$, $\cdots,\varphi_{i_1,j_s}(x)=\varphi_{i_2,j_s}(y)$, then $i_1=i_2$ and $x=y$.

Therorem1 Let $\Phi=(\varphi_{i,j})\subseteq([n]^{[n]})_{I\times J}$ be a rotating function family of size $n\times J$ with the rotating coefficient matrix $\Delta=(\delta_{i,j})$, then Φ is an $(n;n,J,t)-$ difference function family if and only if the transpose matrix of Δ (Δ^T for short) is an $(n,J,t)-$difference matrix.

Proof Suppose Φ is an $(n;n,J,t)-$ difference function family, we prove the Δ^T is $(n,J,t)-$difference matrix.

If there exist two different column indices i_1 and i_2 ,and row indices $u_1,\cdots,u_t$ in Φ that such that $\delta_{u_1,i_1}-\delta_{u_2,i_1}\equiv$

$\delta_{u_1,i_2}-\delta_{u_2,i_2}$, $\cdots,\delta_{u_{t-1},i_1}-\delta_{u_t,i_1}\equiv\delta_{u_{t-1},i_2}-\delta_{u_t,i_2}\pmod n$. Then in the Δ^T , we have $\delta_{i_1,u_1}-\delta_{i_1,u_2}\equiv$

$\delta_{i_2,u_1}-\delta_{i_2,u_2}$, $\cdots,\delta_{i_1,u_{t-1}}-\delta_{i_1,u_t}\equiv\delta_{i_2,u_{t-1}}-\delta_{i_2,u_t}\pmod n$, then $\delta_{i_1,u_1}-\delta_{i_2,u_1}=\delta_{i_1,u_t}-\delta_{i_2,u_t}=x-1\pmod n$, for $x\in[n]$. Hence $\varphi_{i_1,u_1}(x)=\varphi_{i_2,u_1}(1)$, $\cdots,\varphi_{i_1,u_t}(x)=\varphi_{i_2,u_t}(1)$,

then $i_1=i_2$, this contradict with i_1 is different from i_2. So Δ^T is $(n,J,t)-$difference matrix.

Conversely, suppose Δ^T is $(n,J,t)-$ generalized diff-erence matrix, we will prove Φ is an $(n;n,J,t)-$difference

function family. Assume there are t different column indices $1\le j_1,\cdots,j_t\le J$ and two row indices i_1 , i_2 in Δ^T that make $\varphi_{i_1,j_1}(x)=\varphi_{i_2,j_1}(y),\cdots,\varphi_{i_1,j_t}(x)=\varphi_{i_2,j_t}(y)$, we will prove $i_1=i_2$ and $x=y$.

Indeed, we have $\varphi_{i_1,j_1}(x)-\varphi_{i_1,j_2}(x)=\delta_{i_1,j_1}-\delta_{i_1,j_2}=$

$\varphi_{i_2,j_1}(y)-\varphi_{i_2,j_2}(y)=\delta_{i_2,j_1}-\delta_{i_2,j_2},\cdots,\ \varphi_{i_1,j_{t-1}}(x)-\varphi_{i_1,j_t}(x)=$

$\delta_{i_1,j_{t-1}}-\delta_{i_1,j_t}=\varphi_{i_2,j_{t-1}}(y)-\varphi_{i_2,j_t}(y)=\delta_{i_2,j_{t-1}}-\delta_{i_2,j_t}$, then in Δ^T , we have $\delta_{j_1,i_1}-\delta_{j_2,i_1}=\delta_{j_1,i_2}-\delta_{j_2,i_2},\cdots,$ $\delta_{j_{t-1},i_1}-\delta_{j_t,i_1}$

$=\delta_{j_{t-1},i_2}-\delta_{j_t,i_2}$ .As Δ^T is $(n,J,t)-$difference matrix, then there must be $i_1=i_2$ and thus $x=y$.■

From the definition of $(n,k)-$ difference matrix and the new notion of $(n,k,t)-$ generalized difference matrix, it is easy to know $(n,k)-$ difference matrix is $(n,k,2)-$ difference matrix. Similarly ,

$(n;n,J)$ – difference function family in [5] is $(n;n,J,2)$ – generalized difference function family. We can construct $(n;J,t+1)$ – generalized difference matrix from $(n;J,t)$ – generalized difference matrix.

Therorem2 Let $\Delta^{(t)}$ be a $(n;J,t)$ – generalized difference matrix, then we can get a $(n;J,t+1)$ – generalized difference matrix.

Proof If $\Delta^{(t)}$ be a $(n;J,t)$ – difference matrix, then there exit row index $v_1,\cdots,v_{t-1}$ and column index i_1,i_2 that make $\delta_{v_1,i_1}-\delta_{v_2,i_1}\equiv\delta_{v_1,i_2}-\delta_{v_2,i_2}$, $\cdots,\delta_{v_{t-2},i_1}-\delta_{v_{t-1},i_1}\equiv\delta_{v_{t-2},i_2}-\delta_{v_{t-1},i_2}\pmod n$, let $\delta^{(t+1)}_{v_{t-1}+1,i_2}$ be $-\delta^{(t)}_{v_{t-1},i_1}+\delta^{(t)}_{v_{t-1}+1,i_1}+\delta^{(t)}_{v_{t-1}+1,i_2}$.

Thus if $i\neq v_{t-1}+1,\ j\neq i_2$, then let the element $\delta^{(t+1)}_{i,j}=\delta^{(t)}_{i,j}$, if $i=v_{t-1}+1,\ j=i_2$, then let $\Delta^{(t+1)}$ be above value, i.e. $-\delta^{(t)}_{v_{t-1},i_1}+\delta^{(t)}_{v_{t-1}+1,i_1}+\delta^{(t)}_{v_{t-1}+1,i_2}$ .The matrix $\Delta^{(t+1)}$ is just the wanted $(n;J,t+1)$ – difference matrix.

In fact, from $\delta^{(t+1)}_{v_{t-1}+1,i_2}$, we can have $\delta^{(t+1)}_{v_{t-1},i_1}-\delta^{(t+1)}_{v_{t-1}+1,i_1}$.

$\equiv\delta^{(t+1)}_{v_{t-1},i_2}-\delta^{(t+1)}_{v_{t-1}+1,i_2}\pmod n$, so there are t row indece

$v_1,\cdots,v_{t-1},v_{t-1}+1$ that make $\Delta^{(t+1)}$ have R_{t+1} property .

Next we show $\Delta^{(t+1)}$ also has the L_{t+1} property. If

$\Delta^{(t+1)}$ has no L_{t+1} property, then from the relation of $\Delta^{(t+1)}$ and $\Delta^{(t)}$, it is easy to see there are $t+1$ row indices $v_1,\cdots,v_{t-1},v_{t-1}+1,v_s$ that violate L_{t+1} property. Thus

$$\delta^{(t+1)}_{v_{t-1},i_1}-\delta^{(t+1)}_{v_{t-1}+1,i_1}\equiv\delta^{(s+1)}_{v_{t-1},i_2}-\delta^{(s+1)}_{v_{t-1}+1,i_2}\pmod n \tag{1}$$

and

$$\delta^{(t+1)}_{v_{t-1}+1,i_1}-\delta^{(s+1)}_{v_s,i_1}.\equiv\delta^{(s+1)}_{v_{t-1}+1,i_2}-\delta^{(s+1)}_{v_s,i_2}\pmod n \tag{2}$$

then

$$\delta^{(t+1)}_{v_{t-1},i_1}-\delta^{(s+1)}_{v_s,i_1}.\equiv\delta^{(s+1)}_{v_{t-1},i_2}-\delta^{(s+1)}_{v_s,i_2}\pmod n \tag{3}$$

that is

$$\delta^{(t)}_{v_{t-1},i_1}-\delta^{(t)}_{v_s,i_1}.\equiv\delta^{(t)}_{v_{t-1},i_2}-\delta^{(t)}_{v_s,i_2}\pmod n \tag{4}$$

So Δ^T have no L_t property, but this contradict the fact that Δ^T have L_t property. ■

3. Construction of Generalized Difference Function Families

Therorem3 Let $n, J, t, s = 2a$ be positive integers such that $J > 1$ and $\gcd(n,t) = \gcd(n,(aJ-a)!) = 1$. Let η, ξ, μ be functions mapping $[n]$ into integer set Z, such that μ is one-to-one modulo n, $\Phi = \{\varphi_{i,j}\} \subset [n]^{[n]}$ be a function family of size $n \times J$ constructed as $\varphi_{i,j}(x) \equiv tjx + \mu(i) + \eta(j) + \xi(x) \pmod n$, then Φ is an $(n; n, J, s)$ generalized difference function family.

Proof Suppose $\varphi_{i_1,j_1}(x) = \varphi_{i_2,j_1}(y), \varphi_{i_1,j_2}(x) = \varphi_{i_2,j_2}(y),$

$\cdots, \varphi_{i_1,j_{2a}}(x) = \varphi_{i_2,j_{2a}}(y)$ for some $2a$ distinct index $\{j_1, \cdots, j_{2a}\}$, then $\sum_{u=0}^{a-1}(\varphi_{i_1,j_{2u+1}}(x) - \varphi_{i_2,j_{2u+1}}(y) +$

$\varphi_{i_2,j_{2u+2}}(y) - \varphi_{i_1,j_{2u+2}}(x)) \equiv t(\sum_{u=1}^{a}(-1)^{u+1} j_u)(x-y)$

$\equiv 0 \pmod n$. Since $1 \le x, y \le n$, $|\sum_{u=1}^{a}(-1)^{u+1} j_u| \le$

$aJ - a$ and n is coprime to t and $(aJ-a)!$, it follows that $x = y$. Thus $\varphi_{i_1,j_1}(x) - \varphi_{i_2,j_1}(y) \equiv \mu(i_1) - \mu(i_2)$

$\equiv 0 (\mathrm{mod}\, n)$, Since μ is one-to-one modulo n, we have $i_1 = i_2$. Therefore, Φ is an $(n; n, J, s) -$ generalized difference function family. ■

Similarly, we have

Theorem4 Let $n, J, t, s = 2a$ be positive integers such that $J > 1$ and $\gcd(n,t) = \gcd(n,(aJ-a)!) = 1$. Let η, ξ, μ be functions mapping $[n]$ into integer set Z, such that ξ is one-to-one modulo n, $\Phi^* = \{\varphi_{i,j}\} \subseteq [n]^{[n]}$ be a function family of size $n \times J$ constructed as $\varphi_{i,j}(x) \equiv tij + \mu(i) + \eta(j)$

$+ \xi(x) \pmod n$, then Φ^* is a bijective $(n; n, J, s) -$

generalized difference function family.

If s is odd, we only have following results now.

Theorem5 Let n be a prime, $J, t, s = 3$ be positive integers such that $J > 1$ and $\gcd(n,t) = \gcd(n,(J-1)!) = 1$. Let μ be functions mapping $[n]$ into integer set Z, such that μ is one-to-one modulo n, $\Phi = \{\varphi_{i,j}\} \subseteq [n]^{[n]}$ be a function family of size $n \times J$ constructed as $\varphi_{i,j}(x) \equiv tjx + \mu(i) + j^2 x \pmod n$, then Φ is an $(n; n, J, 3) -$ generalized difference function family.

Proof Suppose $\varphi_{i_1,j_1}(x) = \varphi_{i_2,j_1}(y), \varphi_{i_1,j_2}(x) = \varphi_{i_2,j_2}(y)$

and $\varphi_{i_1,j_3}(x)=\varphi_{i_2,j_3}(y)$, then

$$tj_1(x-y)+\mu(i_1)-\mu(i_2)+j_1^2(x-y)\equiv 0(\text{mod } n) \tag{5}$$

$$tj_2(x-y)+\mu(i_1)-\mu(i_2)+j_2^2(x-y)\equiv 0(\text{mod } n) \tag{6}$$

$$tj_3(x-y)+\mu(i_1)-\mu(i_2)+j_3^2(x-y)\equiv 0(\text{mod } n) \tag{7}$$

From (5) and (6), we have

$$[t(j_1-j_2)+j_1^2-j_2^2](x-y)\equiv 0(\text{mod } n) \tag{8}$$

As n is a prime, if $n\nmid x-y$, then $n\mid[t(j_1-j_2)+j_1^2-j_2^2]$, i.e. $n\mid(j_1+j_2+t)(j_1-j_2)$. As $1\le j_1\ne j_2\le J$ and

$\gcd(n,(J-1)!)=1$, then $n\mid j_1+j_2+t$. Similarly, From (6) and (7), we get $n\mid j_3+j_2+t$, thus $n\mid j_1-j_3$, it is impossible. So $n\mid(x-y)$. As $x,y\in[n]$, then $x=y$. Thus, $\varphi_{i_1,j_1}(x)-\varphi_{i_2,j_1}(y)\equiv\mu(i_1)-\mu(i_2)\equiv 0(\text{mod } n)$. Since μ is one-to-one modulo n, we have $i_1=i_2$. Therefore, Φ is an $(n;n,J,2)-$difference function family. ■

Theorem6[6]The multiplication table for the finite field F_q is a $(q;q,2)-$ generalized difference matrix modulo q.

From theorem 2 and 6 , for any q which is a power of some prime, we can get $(q;q,t)-$difference matrix $(2\le t\le q+1)$.

Corollary 1 There exists $(q;q,q,t)-$ generalized difference function family where q is a power of some prime $(2\le t\le q+1)$.

4. Construction of Frameproof Codes

Let $\varphi\in[n]^{[n]}$, the matrix $\varphi(\Gamma)$ is constructed as

$$\varphi(\Gamma)=\begin{pmatrix} a_{\varphi(1)} \\ a_{\varphi(2)} \\ \vdots \\ a_{\varphi(n)} \end{pmatrix}, \text{ where } \Gamma=\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Let Γ be an $(l,n,m)-$code(hash family), Φ be an $(n,n,s)-$difference function family. $\Phi(\Gamma)$ is a matrix of size $n^2\times ls$ defined as

$$\Phi(\Gamma)=\begin{pmatrix} \varphi_{1,1}(\Gamma) & \varphi_{1,2}(\Gamma) & \cdots & \varphi_{1,s}(\Gamma) \\ \varphi_{2,1}(\Gamma) & \varphi_{2,2}(\Gamma) & \cdots & \varphi_{2,s}(\Gamma) \\ \vdots & \vdots & \cdots & \vdots \\ \varphi_{n,1}(\Gamma) & \varphi_{n,2}(\Gamma) & \cdots & \varphi_{n,s}(\Gamma) \end{pmatrix}$$

From theorem 3,4 ,5 and corollary 1, we can get some difference function families, and thus can get frameproof codes.

Theorem7 Let $s=3,2a,\frac{n-1}{w}+1$, where $a\geq 1$,if Γ is a $w-FP(l,n,m)$ code,

(1)when $s=2a$ and $\gcd(n,(a[(s-1)w+1]-1)!=1$, then Φ is an $(n;n,(s-1)w+1,s)-$ generalized difference function family and $\Phi(\Gamma)$ is a $w-FP([(s-1)w+1]l,\ n^2,m)$ code.

(2)when $s=3$ and $\gcd(n,(2w)!=1$, then Φ is an $(n;\ n,2w+1,s)-$ generalized difference function family and $\Phi(\Gamma)$ is a $w-FP([(2w+1]l,\ n^2,m)$ code.

(3)when $s=\frac{n-1}{w}+1$, n is a power of prime and $\gcd(n,$ $(a[(s-1)w+1]-1)!)=1$, then Φ is an $(n;n,(s-1)w+1,s)-$ generalized difference function family and $\Phi(\Gamma)$ is a $w-FP([(s-1)w+1]l,\ n^2,m)$ code.

5. Conclusion

In this paper, we introduce $(n;n,J,t)-$ generalized difference function family and its dual, i.e. $(n,J,t)-$ generalized difference matrix. The new function family can be used to generate more frameproof codes which used widely in protection of digital intellectual property. The $(n;n,J,t)-$ generalized difference function family in fact take the $(n;n,J)-$ difference function family introduced in [5] as a special case. Our new function family include their conclusion. We find that $(n,J,t)-$ generalized difference matrix which is the generalized $(n;n,J,t)-$ generalized difference function family dual designs can construct efficiently from well-known difference matrix ([6]). The $(n,J,t)-$ generalized difference matrix can be used to construct new frameproof codes.

Acknowledgment

The authors would like to acknowledge the financial support of the Natural Sciences Foundation Council of China (NSFC)10971246，2009AA01Z420，and the XinMiao Project from Guangzhou University.

References

[1] B.Chor, A.Fiat, M.Naor and B.Pinkas, Tracing traitors ,IEEE , Transactions on Information Theory 46(2000),pp480-491.

[2] D.Boneh and J.Shaw ,Collusion secure fingerprinting for digital data, IEEE Transactions on Information Theory44(1998),pp1897-1905.

[3] D.R. Stinson, Tran van Trung and R.Wei, Secure frameproof codes ,key distribution patterns, group testing algorithms and related structures, Journal of Statistical Planning and Inference,86(2000),189-200.

[4] D.R.Stinson, R.Wei and L.Zhu, New constructions for perfect hash families and related structures using combinatorial designs and

codes, Journal of Combinatorial Designs,8(2000),189-200.

[5] D.Tonien and R.Safavi-Naini, Recursive constructions of Secure codes and Hash Families Using Difference Fuction Families, Journal of Combinatorial Theory A 113 (2006), 664-674.

[6] Colbourn C J, Dinitz J H. The CRC Handbook of Combinatorial Designs. Florida: CRC Press Inc Boca Raton, 1996.