Journal of Southeast University (English Edition) Vol. 22, No. 2, pp. 153 – 158 June 2006 ISSN 1003—7985

Mathematical demonstration of correlation of optical prime code

Li Chuanqi[1] Zhang Mingde[2] Sun Xiaohan[2]

([1]Department of Physics, Nanjing University of Information Science and Technology, Nanjing 210044, China)

([2]Department of Electronic Engineering, Southeast University, Nanjing 210096, China)

Abstract: Starting from the configuration of the optical prime code, a kind of key signature code for the optical code-division multiple access (OCDMA) system, based on the linear congruence theory in the finite Galois field, the correlation properties of the basic prime code, the extended prime code and the modified prime code are mathematically analyzed, the distribution of cross-correlation values is given and the overlap area of "1"s in the case of periodically circularly shifting is indicated. It is mathematically demonstrated that the maximum cross-correlation of the basic prime code is 2, and that of the extended prime code and the modified prime code is 1. The integrated correlation analysis process is proposed. The signal-interfere ratio (SIR) and the BER performance of the systems employing different signature codes are calculated, respectively, and the performances of OCDMA systems employing different signature codes mode are compared.

Key words: fiber-optic communication; optical code-division multiple access; optical prime code; correlation

The optical code-division multiple access (OCDMA) system has many advantages, such as information security, anti-jamming ability, permission of users to add/drop randomly, coding in the optical domain, so it is thought to be the most hopeful multiplexing technology in establishing all-optical networks. As a result, it has received much attention and research in recent years[1-2]. To be practically applied in the network, the OCDMA system needs a signature code with better performance, which directly depends on the correlation between the codewords. The optical prime code (OPC), a kind of key signature code, was firstly brought forward by Sharr et al. [3], and from then on, the construction schemes of the extended prime code[4-5], the modified prime code[6-7] and the 2^n prime code[8-9] have been set up. Although one knows that the maximum cross-correlation of the basic prime code is 2, and that of the extended prime code and the modified prime code is 1, this has not been mathematically demonstrated. Considering this, this paper will start from the linear congruence theory in the finite Galois field, and mathematically analyze the correlation properties of the basic prime code, the extended prime code and the modified prime code to give an integrated analysis process of prime code correlation. And then, the performances of OCDMA systems employing different signature code modes are compared under the same transmitting speed and the same code-length.

1 Typical Configurations of Prime Code

1.1 Basic prime code (BPC)

According to the linear congruence theory in the Galois field, the basic prime code can simply be acquired. In the Galois field GF(p), where p is a prime larger than 2, take $S_i(j) = \{i \times j\}(\mathrm{mod}p)$, $i \in \mathrm{GF}(p)$, $j \in \mathrm{GF}(p)$, we get the prime sequence $S_i = \{S_{i0}, S_{i1}, \ldots, S_{ij}, \ldots, S_{i(p-1)}\}$[1], which can be used to construct the basic prime code, whose code function $C_i = \{C_{i0}, C_{i1}, \ldots, C_{i(N-1)}\}$ $(i = 0, 1, \ldots, p-1)$,

$$\left.\begin{aligned} C_i(k) &= 1 \qquad \forall : k = S_{ij} + jp \\ C_i(k) &= 0 \qquad \forall : k \neq S_{ij} + jp \end{aligned}\right\} \tag{1}$$

where $j = 0, 1, \ldots, p-1$.

The above expressions are employed to determine the locations of "1"s in the (0, 1) sequence of the prime code, the value of $C_i(k)$ denotes the position of the k-th "1". And then we acquire p basic prime codes whose length $L = p^2$, weight $w = p$, the maximum autocorrelation (AC in concision) side-lobe and crosscorrelation (CC in concision) are $p-1$ and 2, respectively.

1.2 Extended prime code (EPC)

Because the maximum CC value of the BPC, 2, is not helpful to the performance of the system, Maric et al. [5] proposed a new prime code model by increasing the code-length, i. e., adding some "0"s in the (0, 1) sequence of the code, in order to improve the CC[3]. The code function they employed is

$$C_i(k) = (ik)(\mathrm{mod}p) + k(2p-1)$$
$$k \in \mathrm{GF}(p), \quad i \in \mathrm{GF}(p) \tag{2}$$

Eq. (2) means that $p-1$ "0"s are added to each sub-sequence of the BPC, which will make the "1"s

Received 2005-12-05.

Foundation item: The Natural Science Foundation of Jiangsu Higher Education Institutions (No. 04KJB510057).

Biography: Li Chuangqi (1964—), male, doctor, associate professor, leecq@ seu. edu. cn.

more sparse in the whole (0, 1) sequence, and, therefore, the chance that two “1”s have the same location is cut down greatly, and CC is reduced. To code from Eq. (2), the length $L = p(2p-1)$, weight $w = p$, the maximum AC sidelobe is also $p-1$, but the maximum CC value is decreased from 2 to 1. Obviously, the improvement in the CC in the EPC bears a penalty of a decrease in bit rate because of the longer code-length.

1.3 Modified prime code

Another disadvantage of the BPC is that the maximum number of users it can support is just the same as the prime p. If we want to contain a large number of simultaneous users, the p must be large enough, which leads to the AC peak (proportioning to p^2) being much higher than is needed. For better power efficiency, we can remove some “1”s in the (0, 1) sequence to lower the AC peak. The code function of MPC[4] is

$$C_i(j) = (ib_j)(\bmod p) + b_j p$$
$$j \in \{0, 1, \ldots, w-1\},\ b_j \in \mathrm{GF}(p),\ i \in \mathrm{GF}(p) \qquad (3)$$

Eq. (3) is equivalent to drawing out $p-w$ “1”s in the (0, 1) sequence of the basic prime code.

2 Correlation Analysis for Prime Codes

To optical signature code with length L, weight w, the AC sidelobe between a code and its periodically cyclical shifting satisfies (4a), and the CC between different codes satisfies (4b), where λ_a and λ_c are the maximum AC sidelobe and the maximum CC value, respectively.

$$\sum_{i=0}^{L-1} x_i x_{i\oplus\tau} \leqslant \lambda_a \qquad \forall x \in C, \tau \neq 0 \qquad (4a)$$

$$\sum_{i=0}^{L-1} x_i y_{i\oplus\tau} \leqslant \lambda_c \qquad \forall x, y \in C, x \neq y \qquad (4b)$$

where $\oplus$ denotes module L addition. If the code is denoted by vector, the above two constraints can be expressed as

$$\max\{\boldsymbol{C}_i \cdot \boldsymbol{C}_i^{\tau} \mid \tau \in \{1, 2, \ldots, L-1\},\ i \in \mathrm{GF}(p)\} \leqslant \lambda_a \qquad (4c)$$

$$\max\{\boldsymbol{C}_i \cdot \boldsymbol{C}_j^{\tau} \mid \tau \in \{0, 1, \ldots, L-1\},\ i \neq j\} \leqslant \lambda_c \qquad (4d)$$

where $\boldsymbol{C}_i \cdot \boldsymbol{C}_j^{\tau}$ means the scalar product of vectors $\boldsymbol{C}_i$ and $\boldsymbol{C}_j^{\tau}$, and $\boldsymbol{C}_j^{\tau}$ denotes the τ-cyclical shifting of code $\boldsymbol{C}_j$.

In the asynchronous OCDMA system, the AC sidelobe comes from the interference between different chips of the same code, and CC comes from different codes (users). At the OCDMA transmitter and receiver, CC is the main source of the system BER. If the maximum CC value, λ_c, is used to calculate the system BER, the result will not be accurate, because the maximum CC value appears at only a few τ-shiftings, not all the shiftings. Meanwhile, the apparent probability of the maximum CC value is far less than that of other correlation values. For example, as for the basic prime code, the maximum CC is 2, the apparent probability of which is much less than that of CC, 1 or CC, 0. This will be identified in the following section.

2.1 Basic model for code correlation

From (1), we know that the (0, 1) sequence of the code can be evenly divided into p subsequences (sub in concision), each of which has just one “1”. To the i-th code, C_i, of the code family, the location scope of all p chips of the k-th $(0 \leqslant k \leqslant p-1)$ sub are from kp to $(k+1)p-1$. Meanwhile, we know the location of the only “1” of this sub $(ik)(\bmod p) + kp$, $k \in \mathrm{GF}(p)$, $i \in \mathrm{GF}(p)$, which means the “1” locates at the $(ik)(\bmod p)$-th in the k-th sub relatively. For another code, $C_j (0 \leqslant j \leqslant p-1,\ j \neq i)$, chips between $kp - \tau$ and $(k+1)p - 1 - \tau$ will move to the k-th sub after τ-cyclical shifting, as shown in Fig. 1. Let $\tau = ap + b (0 \leqslant b \leqslant p-1)$, the chips' location is from $(k-a-1)p + (p-b)$ to $(k-a)p + (p-b-1)$ before shifting, shown as the shadowed area. If there are “1”s in the k-th sub, they must locate in the shadowed area before shifting. If the “1” originally locates in the $(k-a-1)$-th sub, its relative position, $(j(k-a-1))(\bmod p)$ must satisfy

$$(j(k-a-1))(\bmod p) \geqslant p - b \qquad (5)$$

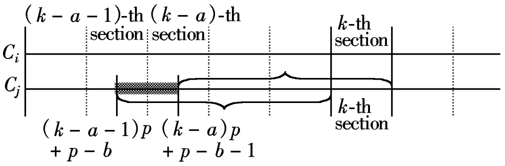

Fig. 1 Schematic of code periodically cyclical shifting

After $\tau = ap + b$ cyclical shifting, its relative position in the k-th sub is

$$(j(k-a-1))(\bmod p) + (k-a-1)p + (ap+b) - kp =$$
$$(j(k-a-1))(\bmod p) + b - p \qquad (6)$$

On the other hand, if the “1” comes from $(k-a)$-th sub, its relative position $(j(k-a))(\bmod p)$ must satisfy

$$(j(k-a))(\bmod p) \leqslant p - b - 1 \qquad (7)$$

After $\tau = ap + b$ cyclical shifting, its relative position in the k-th sub is

$$(j(k-a))(\bmod p) + (k-a)p + (ap+b) - kp =$$
$$(j(k-a))(\bmod p) + b \qquad (8)$$

According to the definition of (1), the CC between codes C_j and C_i means that some “1”s of the two codes have the same position after cyclical shifting, i.e., the following equation must be satisfied

$$(j(k-a-1))(\bmod p) + b - p = (ik)(\bmod p) \qquad (9)$$

or

$$(j(k-a))(\bmod p) + b = (ik)(\bmod p) \qquad (10)$$

Eqs. (9) and (10) are the linear congruence equations in the Galois field, whose solutions are

$$k = \frac{j(a+1) - b + \xi p}{j - i} \tag{11}$$

$$k = \frac{ja - b + \zeta p}{j - i} \tag{12}$$

where ξ, ζ are integers. The values of k decided by (11) and (12) must satisfy the conditions of (5) and (7), respectively; otherwise, the solution is invalid. Obviously, if a, b make both (11) and (12) have no integer solution, the CC between codes C_j and C_i is zero at such a shifting $\tau = ap + b$. Similarly, if only one of the equations has an integer solution, CC is 1, and if both equations have integer solutions, CC is 2.

Tab. 1 gives the variation of the CC between codes C_3 and C_5 in GF(7) versus shifting $\tau = ap + b$. Tab. 2 shows the subsequences k in which the "1"s of the two codes have the same location.

Tab. 1 CC of C_3 and C_5 vs. shifting $\tau = ap + b$

a	b						
	0	1	2	3	4	5	6
0	1	1	2	1	0	1	1
1	1	1	0	2	2	1	0
2	1	2	1	0	0	1	2
3	1	0	1	2	2	0	1
4	1	1	1	0	1	2	1
5	1	1	2	2	0	0	1
6	1	1	0	0	2	2	1

Tab. 2 Overlapping area of "1"s, k vs. shifting $\tau = ap + b$

a	b						
	0	1	2	3	4	5	6
0	0	3	5,6	2	—	0	3
1	6	2	—	0,1	3,4	6	—
2	5	0,1	4	—	—	5	1,2
3	4	—	3	5,6	1,2	—	0
4	3	6	2	—	0	3,4	6
5	2	5	0,1	3,4	—	—	5
6	1	4	—	—	5,6	1,2	4

From Tabs. 1 and 2, we can see that CC varies with different shiftings τ; meanwhile, different CC values have different appearing probabilities.

2.2 Correlation property of basic prime code

$\lambda = 2$ means that there are just 2 "hit"s that happened between two codes at some cyclical shifting τ. In this case, the distance between the two "1"s in one code equals the distance between two "1"s in another code, here "distance" means the position difference. From definition (1), the distance between two adjacent "1"s in code C_i is

$$d = ((i(k+1))(\mathrm{mod}p) + (k+1)p) - ((ik)(\mathrm{mod}p) + kp) \tag{13}$$

According to the characteristics of the finite congruence equation, we consider the distance in three cases:

① When $i(k+1) < mp$, we have $d = p + i$;

② When $ik < mp \leqslant i(k+1)$, we get $d = p + i - p = i$;

③ When $ik \geqslant mp$, we have $d = p + i$.

Thus, the distance of adjacent "1"s in C_i is either $p + i$ or i. Considering the periodically cyclical shifting, the distance $p + i$ appears $p - i$ times, and i, i times. As a result, we obtain the distances between any two "1"s in the code C_i.

$$d^i_{m,n} = m(p+i) + ni \qquad 0 \leqslant m \leqslant p - i, 0 \leqslant n \leqslant i \tag{14}$$

where m and n are integers, cannot be zero, cannot be the maximum simultaneously. Otherwise, the distance will be zero or L. When the CC value between codes C_i and C_j is 2, there are m, n, m', n' satisfying $d^j_{m,n} = d^i_{m',n'}$, i. e.,

$$(m'(p+j) + n'j)(\mathrm{mod}L) = (m(p+i) + ni)(\mathrm{mod}L) \tag{15}$$

$$m' - m = \frac{(m+n)i - (m'+n')j}{p} = \frac{li - l'j}{p}$$

$$0 < l = m + n < p, \ 0 < l' = m' + n' < p \tag{16}$$

When $i = 0$ or $j = 0$, both $l'j$ and li are aliquant by p, therefore, no m, n, m', n' can satisfy (15). In such a case, CC is 1. When $i \neq j \neq 0$, because $\min(l'j) = 1$, we know $\max(li) = (p-1)^2$. From Eq. (16), we have

$$\max(m' - m) = \frac{(p-1)^2 - 1}{p} = p - 2 \tag{17}$$

In the above case, there must be m, n, m', n' satisfying (15), which means the CC value between C_i and C_j is 2 in some τ-shiftings.

The maximum CC value of the basic prime code family is 2, i. e., in (4), $\lambda_c = 2$. However, the probability of $\lambda = \lambda_c$ is far less than that of $\lambda = 1$ or $\lambda = 0$. Tab. 3 shows the appearing times of $\lambda = 2$ in the whole shifting process $(0 \leqslant \tau \leqslant 48)$ of the prime code family acquired in GF(7).

Tab. 3 Appearing times of $\lambda = 2$ between any two prime codes in GF(7)

i	j						$\sum_{j=1,j\neq i}^{p-1} C_iC_j$
	1	2	3	4	5	6	
1	—	10	10	6	12	12	50
2	10	—	6	12	6	12	46
3	10	6	—	10	12	6	44
4	6	12	10	—	6	10	44
5	12	6	12	6	—	10	46
6	12	12	6	10	10	—	50
$\sum_{i=1}^{p-1}\sum_{j=1,j\neq i}^{p-1} C_iC_j$							280

2.3 Correlation property of extended prime code

According to Eq. (2), we have the distance between adjacent "1"s in the (0,1) sequence of the extended prime code,

$$d = ((i(k+1))(\mathrm{mod}p) + (k+1)(2p-1)) - (ik)(\mathrm{mod}p) + k(2p-1) \tag{18}$$

There are three cases as follows:

① When $i(k+1) < mp$, we have $d = 2p - 1 + i$;

② When $ik < mp \leqslant i(k+1)$, we get $d = 2p - 1 + i - p = p - 1 + i$;

③ When $ik \geqslant mp$, we have $d = 2p - 1 + i$.

Thus, the distance of adjacent "1"s in C_i is either $2p - 1 + i$ or $p - 1 + i$. Considering the periodically cyclical shifting, the distance $2p - 1 + i$ appears $p - i$ times, and $p - 1 + i$, i times. As a result, we obtain the distances between any two "1"s in the code C_i

$$d^i_{m,n} = m(2p - 1 + i) + n(p - 1 + i)$$
$$0 \leqslant m \leqslant p - i,\ 0 \leqslant n \leqslant i \tag{19}$$

where m and n are integers, cannot be zero and cannot be the maximum simultaneously. Otherwise, the distance will be zero or L. When the CC value between codes C_i and C_j is 2, then there are m, n, m', n' satisfying $d^j_{m,n} = d^i_{m',n'}$, i. e.,

$$(m'(2p - 1 + j) + n'(p - 1 + j))(\mathrm{mod}L) = (m(2p - 1 + i) + n(p - 1 + i))(\mathrm{mod}L) \tag{20}$$

$$(2m' + n') - (2m + n) = \frac{l(i-1) - l'(j-1)}{p}$$
$$0 < l = m + n < p,\ 0 < l' = m' + n' < p \tag{21}$$

When $i = 1$ or $j = 1$, both $l'(j-1)$ and $l(i-1)$ are aliquant by p, therefore, no m, n, m', n' can satisfy (20). In such a case, CC is 1. When $i \neq j \neq 1$, $\max(l(i-1) - l'(j-1)) = (p-1)(p-2) - 1 = p^2 - 3p + 1$, i. e.,

$$\max((2m' + n') - (2m + n)) = \frac{p^2 - 3p + 1}{p} \tag{22}$$

In the above case, there are no m, n, m', n' satisfying (22), which means the CC value between C_i and C_j is at most 1 in any τ-shifting.

According to the analysis of sections 2. 2 and 2. 3, we know that the CC property of the extended prime code is better than that of the basic prime code, but the length of the extended code is longer than that of the basic prime code.

As for the modified prime code defined by (3), $w < p$, $L = p^2$, which can be acquired by taking out $p - w$ "1"s from the basic prime code. The positions of the left "1"s have not been changed. Therefore, the CC property of the modified prime code is the same as that of the basic prime code. However, the AC property of the former is better than that of the latter.

3 Calculation of BER from Code Correlation

To analyze the system BER induced from multiple user interference, we should first analyze the distribution of the different CC values. That is to say that the influence of different CC values ($\lambda_m \in \{0, 1, \ldots, \lambda_c\}$) to system BER is different. Let q_m denote the appearing probabilities of λ_m, we obtain the average CC value

$$\bar{\lambda} = q_0 \cdot 0 + q_1 \cdot 1 + q_2 \cdot 2 + \ldots q_{\lambda c}\lambda_c = \sum_{m=0}^{\lambda_c} q_m \lambda_m \tag{23}$$

where $\bar{\lambda}$ denotes the average probability that a "1" in a code "hits" a "1" in another code. To the codes with length L and weight w, each code has w "1"s uniformly. Thus, the probability of a certain "1" in the first code "hits" the "1"s in the second code is w/L. If the system employs the on-off key modulation mode, both data bits 0 and 1 are transmitted with equal probability, 1/2. When a user transmits data 0, there will be no "hit" happening. Therefore, the practical "hit" probability is $w/2L$. Considering these, the "hit" probability that the w "1"s in the first code "hit" w "1"s in the second code is $\bar{\lambda} = w^2/2L$.

From the prime code, we can easily know $\bar{\lambda}$. The values of q_0, q_1, and q_2 can be derived from Ref. [10]. Then we have the distribution variance of correlation values, $\sigma^2 = 5/12 - 1/(6p) - 1/(3p^2)$ for the basic prime code and $\sigma^2 = 3/16 + 1/(8(2p-1)) - 1/(16(2p-1)^2)$ for the extended prime code. Supposing that there are total K simultaneous users, a special user received the interference from other $K - 1$ users is $(K-1)\sigma^2$, the signal-interference ratios $R_{\mathrm{SIR,B}}$ of the basic prime code and $R_{\mathrm{SIR,E}}$ of the extended prime code, are respectively:

$$R_{\mathrm{SIR,B}} = \frac{w^2}{2(K-1)\sigma^2} = \frac{p^2}{2(K-1)(5/12 - 1/(6p) - 1/(3p^2))} \tag{24}$$

$$R_{\mathrm{SIR,E}} = \frac{p^2}{2(K-1)}\left(\frac{3}{16} + \frac{1}{8(2p-1)} - \frac{1}{16(2p-1)^2}\right) \tag{25}$$

In the DS-OCDMA system, in order to satisfy the BER requirement, the p used in code designing is much larger than 1(normally 37 or 41). In this case, we have

$$R_{\mathrm{SIR,B}} = \frac{12p^2}{10(K-1)} = \frac{1.2p^2}{K-1} \tag{26}$$

$$R_{\mathrm{SIR,E}} = \frac{8p^2}{3(K-1)} = \frac{2.67p^2}{K-1} \tag{27}$$

Therefore, we obtain the system BER induced by cross-correlation between codes as

$$B_{\mathrm{BER,B}} = \Phi\left(-\sqrt{\frac{R_{\mathrm{SIR,B}}}{2}}\right) = 0.5 + 0.5\mathrm{erf}\left(-\frac{\sqrt{R_{\mathrm{SIR,B}}}}{2}\right) =$$

$$0.5+0.5\mathrm{erf}\left(-0.548\frac{p}{\sqrt{K-1}}\right) \qquad (28)$$

$$B_{\mathrm{BER,E}}=\Phi\left(-\sqrt{\frac{R_{\mathrm{SIR,E}}}{2}}\right)=0.5+0.5\mathrm{erf}\left(-\frac{\sqrt{R_{\mathrm{SIR,E}}}}{2}\right)=$$
$$0.5+0.5\mathrm{erf}\left(-0.817\frac{p}{\sqrt{K-1}}\right) \qquad (29)$$

where the variation function

$$\mathrm{erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x \exp\left(-\frac{t^2}{2}\right)\mathrm{d}t$$

Fig. 2 to Fig. 5 give $R_{\mathrm{SIR,B}}$, $B_{\mathrm{BER,B}}$, $R_{\mathrm{SIR,E}}$ and $R_{\mathrm{BER,E}}$ vs. the number of simultaneous users of the OCDMA system with the basic prime code or with the extended prime code, respectively. According to Fig. 2 to Fig. 5, we can see that when the prime number p increases, the system SIR increases soon and BER decreases fast, which indicates that the greater p is, the better the system performance. But the greater p will increase the code-length, which will depress the bit rate. So, for properly choosing p, we should make overall plans and take all factors into consideration.

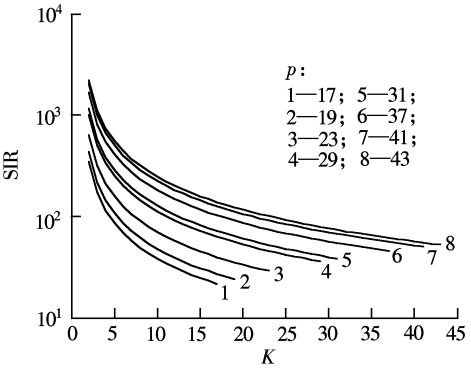

Fig. 2 SIR performance of prime code

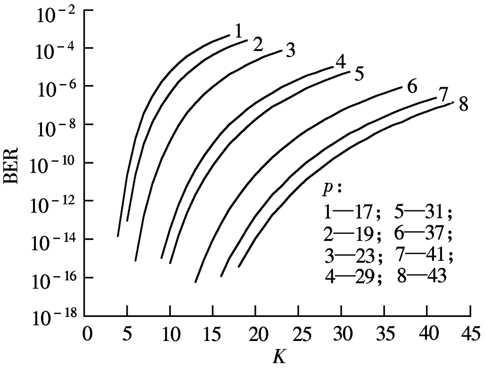

Fig. 3 BER performance of prime code

According to Figs. 2 to 5, as for the same prime code p, we can directly conclude that the SIR and the BER performance of the extended code $(p(2p-1), p, p-1, 1)$ are far better than those of the basic prime code $(p^2, p, p-1, 2)$. However, the code-length of the former is about twice that of the latter, which indicates that the improvement in performance is under the penalty of a decrease in bit rate.

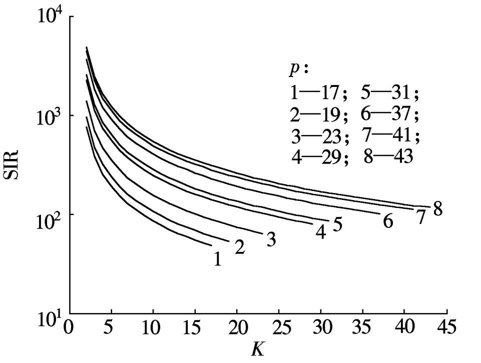

Fig. 4 SIR performance of extended prime code

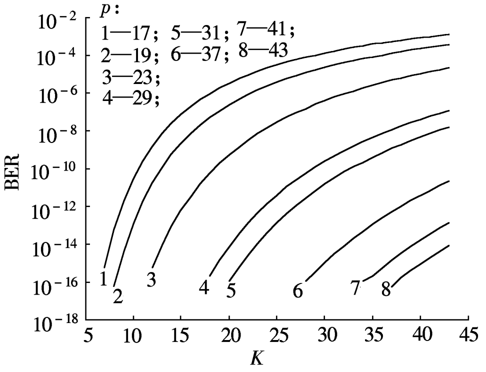

Fig. 5 BER performance of extended prime code

With the same code-length, the code weight of EPC is about 0.707 time of that of BPC. We can get the comparison of SIR and BER between the EPC and BPC, according to Eqs. (26) to (29). The comparison results are shown in Fig. 6 and Fig. 7.

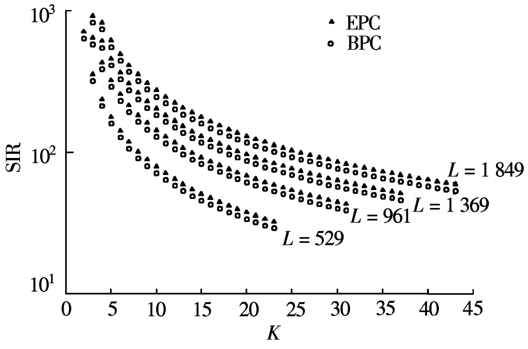

Fig. 6 SIR comparison between EPC and BPC

From Fig. 7, we find that the BER of the OCDMA system with the extended prime code is improved by one order compared to the BPC; therefore, we can say that the extended prime code has a better performance than the basic prime code.

Finally, it should be pointed out that one disadvantage of both the EPC and the BPC is that they have a high autocorrelation value, which leads to the quite

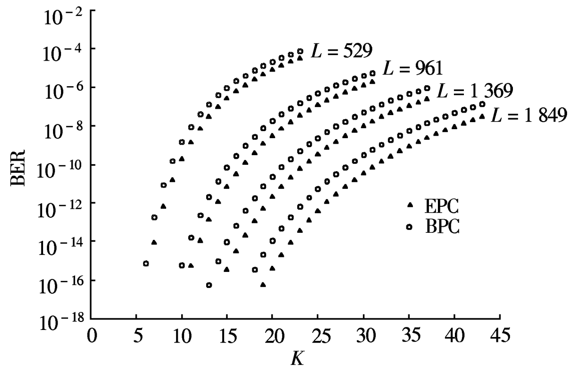

Fig. 7 BER comparison between EPC and BPC

low weight-autocorrelation ratio $w/\lambda_a = p/(p-1)$.

4 Conclusion

The performance of the optical code family depends on the BER induced by multiple access interference, which is mainly based on the cross-correlation between signature codes. The optical prime code is one kind of basic signature code, and the correlation property of its code function directly determines the code performance. Starting from the linear congruence theory in the finite Galois field, this paper mathematically analyzes the correlation properties of the basic prime code, the extended prime code and the modified prime code, and then calculates the system SIR and BER induced by multiple access interference according to the distribution of the correlation values. The performance of OCDMA systems with the basic or extended prime codes are compared. The result indicates that the system performance with the EPC is better than that with the BPC under the same transmitting data rate.

References

[1] Shalaby T H M. Performance analysis of an optical CDMA random access protocol[J]. *J of Light Tech*, 2004, **22**(5): 1233 - 1241.

[2] Miyazawa T, Sasase T. Enhancement of tolerance to MAIs by the synergistic effect between M-ary PAM and the chip-level receiver for optical CDMA systems [J]. *J of Light Tech*, 2006, **24**(2): 658 - 666.

[3] Shaar A A, Davis P A. Prime sequence: quasi-optimal sequences for channel code division multiplexing [J]. *Electronics Letters*, 1983, **19**(21): 888 - 890.

[4] Kwong W C, Perrier P A, Prucnal P R. Performance comparisons of asynchronous and synchronous code-division multiple-access techniques for fiber-optic local area network [J]. *IEEE Trans Communications*, 1991, **39** (11): 1625 - 1634.

[5] Maric S. New family of algebraically designed optical code for use in CDMA fibre-optic networks [J]. *Electronics Letters*, 1993, **29**(6): 538 - 539.

[6] Zhang J G. Effective design of optical code-division multiple access networks by using the modified prime code[J]. *Electronics Letters*, 1997, **33**(3): 229 - 230.

[7] Zhang J G, Kwong W C, Sharma A B. Effective design of optical fiber code-division multiple access networks using the modified prime codes and optical processing[A]. In: *WCC-ICCT*2000[C]. Beijing, 2000, **1**: 392 - 397.

[8] Kwong W C, Yang G C. Construction of 2^n prime-sequence codes for optical code division multiple access[J]. *IEE Proceedings Communications*, 1995, **142** (3): 141 - 150.

[9] Zhang J G, Kwong W C, Yang G C. 2^n modified prime codes for use in fiber optic CDMA networks[J]. *Electronics Letters*, 1997, **33**(22): 1840 - 1841.

[10] Yang G C, Kwong W C. Performance analysis of optical CDMA with prime codes[J]. *Electronics Letters*, 1995, **31**(7): 569 - 570.

光素数地址码互相关特性数学分析

李传起[1] 张明德[2] 孙小菡[2]

([1] 南京信息工程大学物理系,南京 210044)

([2]东南大学电子工程系,南京 210096)

摘要:围绕 OCDMA 系统的重要地址码类型——光素数地址码的结构模型,根据有限 Galois 域上的线性全等理论,系统分析了基本素数码、扩展素数码、修正素数码的互相关特性,指出码字中“1”位的重叠区域. 具体给出基本素数码最大互相关为 2、扩展素数码和修正素数码最大互相关为 1 的数学证明,并给出完整的的素数码相关性分析过程. 在此基础上,计算基本素数码和扩展素数码的信号干扰比以及多址干扰误码率,并比较基于不同素数码的 OCDMA 系统的误码性能,给出定量比较结果.

关键词:光纤通信;光码分多址(OCDMA);光素数地址码(OPC);相关性

中图分类号:TN29