A $\sqrt{N}$ Method for Generating Coteries

Kuo-Tsung Tseng
Chang-Biau Yang

Department of Computer Science and Engineering,
National Sun Yat-sen University, Kaohsiung, Taiwan.
E-mail:cbyang@cse.nsysu.edu.tw

Key words: quorum, coterie, finite projective plane

1 Introduction

In order to get more efficiency of those computers, using distributed systems is a good choice. Thus, the mutual exclusion problem in distributed systems is an important issue. One of the ways to solve the mutual exclusion problem is the *coterie protocol*, which was proposed by Garcia-Molina and Barbara [2]. A coterie under U (U is the collection set of all the nodes in the distributed system) consists of a set of *quorums* in which each quorum is a subset of U, and the intersection of any pair of quorums is nonempty. It is called the *intersection property*. The other property of quorums is *minimality* that no quorum contains another quorum. With these two properties, a coterie can be used to solve the mutual exclusion problem in a distributed system. Any node which wants to enter the critical section must have the permissions of all nodes in a quorum, and release the permissions when the node leaves the critical section. The permission can be given to at most one node in the distributed system at a time. Because of the intersection property, no node can enter the critical section if there is another node in the critical section at that time.

With a well designed coterie, we can have less communication cost and tolerate some nodes failure. Many researchers proposed some methods for constructing coteries or investigated the properties of coteries [3–7].

2 Previous Work

Maekawa proposed a $\sqrt{N}$ algorithm for mutual exclusion in decentralized systems [6]. It is actually a $\sqrt{N}$ coterie using the concept of *finite projective plane*. A finite projective plane of order p is formally defined as a set of $p(p+1)+1$ points with the following properties:

1. Any two points determine a line,

2. Any two lines determine a point,

3. Every point has $p+1$ lines on it, and

4. Every line contains $p+1$ points.

In a finite projective plane of order p, there are $p(p+1)+1$ lines. It is clear that a finite projective plane is a coterie if we take each line as a quorum. It has been proved if p is a power of a prime, there exists a finite projective plane of order p. If either $p-1$ or $p-2$ is divisible by 4 and p is not a sum of two integral squares ($p \neq a^2+b^2$), there exists no finite projective plane of order p [1].

Maekawa pointed out the relationship between a finite projective plane and a coterie, however, how to construct a finite projective plane or to generate a coterie is not very clear. Thus, in this paper, we shall propose a method for generating a coterie with quorum size $p+1$, where p is a prime.

3 A Generating Method

In this section, we shall propose a simple method to generate coteries. The method can be applied when the quorum size of the coterie is equal to $p+1$, where p is a prime number, and the number of members in the coterie is $n = p(p+1)+1$, and n is also the coterie size (number of quorums in a coterie). For example, if the quorum size is $p+1=6$, then $n = 5(5+1)+1 = 31$. We will use this example to explain how the method works (see Table 1).

We divide the coterie into $p+1$ quorum matrices, denoted as $M_1^{(p+1)\times(p+1)}$, $M_2^{p\times(p+1)}$, $M_3^{p\times(p+1)}$, $\cdots$, $M_{p+1}^{p\times(p+1)}$. Let $m_{i,j}^x$ denote an element in matrix M_x. The method for generating the quorum matrices is as follows:

$$m_{i,j}^1 = \begin{cases} 1 & \text{if } j=1, \\ (i-1)p+j & \text{if otherwise,} \end{cases}$$

where $1 \leq i,\ j \leq p+1$.

For other matrices $M_x, 2 \leq x \leq p+1$, the generating method is more complicated. We use some generating matrices $G_2^{p\times p}$, $G_3^{p\times p}$, $\cdots$, $G_{p+1}^{p\times p}$, to guide the construction of those matrices. Let $g_{i,j}^x$ denote an element in matrix G_x. The generating matrices are defined as follows:

$$g_{i,j}^x = [(x-2)(j-1)+(i-1)]\ mod\ p,$$

where $2 \leq x \leq p+1,\ 1 \leq i,\ j \leq p$.

Now, we define the other quorum matrices in our coterie as follows:

$$m_{i,j}^x = \begin{cases} x & \text{if } j=1, \\ m_{j,2}^1 + g_{i,j-1}^x & \text{if otherwise,} \end{cases}$$

where $2 \leq x \leq p+1,\ 1 \leq i \leq p,\ 1 \leq j \leq p+1$.

Lemma 1 *In each quorum matrix,* $m_{i_1,j_1}^x \neq m_{i_2,j_2}^x,\ 1 \leq x \leq p+1$, *if and only if* $(i_1,\ j_1) \neq (i_2,\ j_2)$, $2 \leq j_1,\ j_2 \leq p+1$.

Table 1: Our Coterie with $p = 5$

1	2	3	4	5	6
1	7	8	9	10	11
1	12	13	14	15	16
1	17	18	19	20	21
1	22	23	24	25	26
1	27	28	29	30	31

(a)$M_1^{6\times 6}$

2	7 (0)	12 (0)	17 (0)	22 (0)	27 (0)
2	8 (1)	13 (1)	18 (1)	23 (1)	28 (1)
2	9 (2)	14 (2)	19 (2)	24 (2)	29 (2)
2	10 (3)	15 (3)	20 (3)	25 (3)	30 (3)
2	11 (4)	16 (4)	21 (4)	26 (4)	31 (4)

(b)$M_2^{5\times 6}(G_2^{5\times 5})$

3	7 (0)	13 (1)	19 (2)	25 (3)	31 (4)
3	8 (1)	14 (2)	20 (3)	26 (4)	27 (0)
3	9 (2)	15 (3)	21 (4)	22 (0)	28 (1)
3	10 (3)	16 (4)	17 (0)	23 (1)	29 (2)
3	11 (4)	12 (0)	18 (1)	24 (2)	30 (3)

(c)$M_3^{5\times 6}(G_3^{5\times 5})$

4	7 (0)	14 (2)	21 (4)	23 (1)	30 (3)
4	8 (1)	15 (3)	17 (0)	24 (2)	31 (4)
4	9 (2)	16 (4)	18 (1)	25 (3)	27 (0)
4	10 (3)	12 (0)	19 (2)	26 (4)	28 (1)
4	11 (4)	13 (1)	20 (3)	22 (0)	29 (2)

(d)$M_4^{5\times 6}(G_4^{5\times 5})$

5	7 (0)	15 (3)	18 (1)	26 (4)	29 (2)
5	8 (1)	16 (4)	19 (2)	22 (0)	30 (3)
5	9 (2)	12 (0)	20 (3)	23 (1)	31 (4)
5	10 (3)	13 (1)	21 (4)	24 (2)	27 (0)
5	11 (4)	14 (2)	17 (0)	25 (3)	28 (1)

(e)$M_5^{5\times 6}(G_5^{5\times 5})$

6	7 (0)	16 (4)	20 (3)	24 (2)	28 (1)
6	8 (1)	12 (0)	21 (4)	25 (3)	29 (2)
6	9 (2)	13 (1)	17 (0)	26 (4)	30 (3)
6	10 (3)	14 (2)	18 (1)	22 (0)	31 (4)
6	11 (4)	15 (3)	19 (2)	23 (1)	27 (0)

(f)$M_6^{5\times 6}(G_6^{5\times 5})$

Proof: Let $a = m^x_{i_a,j_a},\ b = m^x_{i_b,j_b},\ 1 \le x \le p+1,\ 1 \le i_a,\ i_b \le p$ (if $x = 1, 1 \le i_a,\ i_b \le p+1$), $2 \le j_a,\ j_b \le p+1$, $i_a \ne i_b$ or $j_a \ne j_b$.
(1) If $x = 1$, $i_a = i_b$, then it is clear that $a \ne b$ if $j_a \ne j_b$.
(2) If $x = 1,\ i_a < i_b$, then $b - a = (i_b - i_a)p + (j_b - j_a) > 0$ since $i_b - i_a > 0,\ 1 - p \le j_b - j_a \le p - 1$. That is, $a \ne b$.
(3) If $2 \le x \le p+1,\ j_a < j_b$, then

$$\begin{aligned} b - a &= m^1_{j_b,2} - m^1_{j_a,2} + (g^x_{i_b,j_b-1} - g^x_{i_a,j_a-1}) \\ &= (j_b - j_a)p + (g^x_{i_b,j_b-1} - g^x_{i_a,j_a-1}) \\ &> 0 \end{aligned}$$

since $j_b - j_a > 0,\ 1 - p \le g^x_{i_b,j_b-1} - g^x_{i_a,j_a-1} \le p - 1$. It implies that $a \ne b$.
(4) If $2 \le x \le p+1,\ j_a = j_b$, then

$$\begin{aligned} b - a &= g^x_{i_b,j_b-1} - g^x_{i_a,j_a-1} \\ &= (i_b - i_a)\ mod\ p \\ &\ne 0 \end{aligned}$$

We have that $a \ne b$. ∎

Theorem 2 *Any pair of nodes (a, b) appear on exactly one row in all quorum matrices.*

Proof: Let $(a,\ b)$ be any pair of nodes, without loss of generality, $a < b$.
(1) If $1 = a < b \le p(p+1)+1$. It is clear that the pair $(a,\ b)$ can only appear in M_1, and each b ($2 \le b \le p(p+1)+1$) appears exactly once in M_1, so that the pair $(a,\ b)$ appears exactly on one row in M_1.
(2) If $2 \le a < b \le p+1$. As one can see that the pair $(a,\ b)$ appears exactly once on row 1 of M_1.
(3) If $2 \le a \le p+1 < b \le p(p+1)+1$. The pair $(a,\ b)$ must appear on some row(s) of M_a. Since each b ($p+1 < b \le p(p+1)+1$) appears exactly once in M_a, the pair $(a,\ b)$ appears exactly on one row of M_a.
(4) If $p+1 < a < b \le p(p+1)+1$. Suppose there are two rows (or more) which the pair $(a,\ b)$ appears on, say A and B, $A \ne B$. If A is a row of M_1, since there is no replica of a or b in M_1, B can not be in M_1. It is clear that if the pair $(a,\ b)$ appears on a row of M_1, $(a,\ b)$ will not be in the same row of M_x, $2 \le x \le p+1$, which means there is no such row B of M_x, $2 \le x \le p+1$, contains the pair $(a,\ b)$. If neither A nor B is a row of M_1, suppose the pair $(a,\ b)$ appears on column $j_1,\ j_2$ of row i_1 of M_{x_1} and on column $j_1,\ j_2$ of row i_2 of M_{x_2}, $2 \le j_1,\ j_2 \le p+1$, $1 \le i_1,\ i_2 \le p$, $2 \le x_1,\ x_2 \le p+1$. (If the pair $(a,\ b)$ appears on some row of some quorum matrix and appears on another row of another quorum matrix, the columns which $(a,\ b)$ are on should be the same.)

$$\begin{aligned} (a,\ b) &= (m^1_{j_1,2} + g^{x_1}_{i_1,j_1-1},\ m^1_{j_2,2} + g^{x_1}_{i_1,j_2-1}) \\ &= (m^1_{j_1,2} + g^{x_2}_{i_2,j_1-1},\ m^1_{j_2,2} + g^{x_2}_{i_2,j_2-1}) \end{aligned}$$

We can ignore the m-parts since they are the same.

$$\begin{aligned} (a',\ b') &= (g^{x_1}_{i_1,j_1-1},\ g^{x_1}_{i_1,j_2-1}) \\ &= (g^{x_2}_{i_2,j_1-1},\ g^{x_2}_{i_2,j_2-1}) \end{aligned}$$

extracting the g-parts, then:

$$\begin{aligned}(a', b') &= ([(x_1-2)(j_1-1)+(i_1-1)] \ mod \ p, \ [(x_1-2)(j_1-1)+(i_1-1)] \ mod \ p) \\ &= ([(x_2-2)(j_1-1)+(i_2-1)] \ mod \ p, \ [(x_2-2)(j_2-1)+(i_2-1)] \ mod \ p)\end{aligned}$$

then we know that:

$$[(j_1-1)(x_1-x_2)+(i_1-i_2)] \ mod \ p = 0,$$

$$[(j_2-1)(x_1-x_2)+(i_1-i_2)] \ mod \ p = 0,$$

Since $j_1 \neq j_2$ $(2 \leq j_1, \ j_2 \leq p+1)$ and p is a prime, the two equations above can not both be 0, which means that there are no two rows in quorum matrices contain the same pair $(a, \ b)$. That is, the pair $(a, \ b)$ appears on exactly one row in all quorum matrices. ∎

Theorem 3 *The intersection of the members on any two rows in all quorum matrices is nonempty.*

Proof: Let A and B be any two rows in all quorum matrices, $A \neq B$.
(1) If A and B are in the same M_x, $1 \leq x \leq p+1$. A intersects B on column 1 by definition.
(2) If A is row i_1 of M_1, and B is row i_2 of M_x, $1 \leq i_1 \leq p+1, \ 1 \leq i_2 \leq p, \ 2 \leq x \leq p+1$.

$$A = (1, \ i_1p-(p-2), \ i_1p-(p-2)+1, \ \cdots, \ i_1p-(p-2)+(p-1)),$$

$$B = (x, \ (p+2)+g^x_{i_2,1}, \ (2p+2)+g^x_{i_2,2}, \ \cdots, \ (pp+2)+g^x_{i_2,p}),$$

If $i_1 = 1$, then $A = (2, \ 3, \ \cdots, \ p+1)$, since $x \in B, \ 2 \leq x \leq p+1$, Intersection of A and B is x. Otherwise, $i_1 \neq 1$, then we may find an element E of B, and $E = (i_1-1)p+2+g^x_{i_2,i_1-1} = i_1p-(p-2)+g^x_{i_2,i_1-1}$, since $0 \leq g^x_{i_2,i_1-1} \leq p-1$, intersection of A and B is E.
(3) If $A \notin M_1$ and $B \notin M_1$. Suppose that A is row i_1 of M_{x_1}, and B is row i_2 of M_{x_2}, $1 \leq i_1, i_2 \leq p, \ 2 \leq x_1, x_2 \leq p+1, \ x_1 \neq x_2$, then A and B can be represented as:

$$A = (x_1, \ m^1_{2,2}+g^{x_1}_{i_1,1}, \ m^1_{3,2}+g^{x_1}_{i_1,2}, \ \cdots, \ m^1_{p+1,2}+g^{x_1}_{i_1,p}),$$

$$B = (x_2, \ m^1_{2,2}+g^{x_2}_{i_2,1}, \ m^1_{3,2}+g^{x_2}_{i_2,2}, \ \cdots, \ m^1_{p+1,2}+g^{x_2}_{i_2,p}),$$

We are trying to prove that the intersection of A and B is nonempty, since that $x_1 \neq x_2$ and the m-parts of A and B are the same, we may concentrate on g-parts of them, so that:

$$A' = [(x_1-2)(j_1-1)+(i_1-1)] \ mod \ p, \ 2 \leq j_1 \leq p+1,$$

$$B' = [(x_2-2)(j_2-1)+(i_2-1)] \ mod \ p, \ 2 \leq j_2 \leq p+1,$$

If there exists $J = j_1 = j_2$ (since we have ignored m-parts, A and B intersects if some g-part is the same. Let it be J.) such that:

$$\{[(x_1-2)(J-1)+(i_1-1)]-[(x_2-2)(J-1)+(i_2-1)]\} \ mod \ p = 0,$$

then the intersection of A and B is nonempty. It can be rewritten as

$$[(x_1-x_2)J+(i_1-x_1-i_2+x_2)] \ mod \ p = 0,$$

without loss of generality, let $C_1 = x_1 - x_2,\ C_2 = i_1 - x_1 - i_2 + x_2,\ C_1,\ C_2$ are constants and $C_1 \neq 0$, then:

$$C_1 J + C_2\ mod\ p = 0,$$

Since p is a prime, and $2 \leq J \leq p+1$, there exists J such that $C_1 J + C_2\ mod\ p = 0$. The intersection of A and B is nonempty. ∎

Theorem 4 *Our method can generate a coterie if and only if p is a prime.*

Proof: By Theorem 3, it satisfies the intersection property, and it is clear that it satisfies the minimality property. Thus, it can do generate a coterie. If p is not a prime, in case 3 of the proof of Theorem 3, let C_1 = some factor of p and $C_2 = 1$. It is clear that $C_1 J + C_2\ mod\ p \neq 0,\ 2 \leq J \leq p+1$, which means that the intersection of some rows (A and B) is empty. It will not satisfy the intersection property. ∎

References

[1] A. A. Albert and S. R., *An Introduction to Finite Projective Planes*. New York: Holt, Rinehart, and Winston, 1968.

[2] H. Garcia-Molina and D. Barbara, “How to assign votes in a distributed system,” *J. ACM*, Vol. 32, No. 4, pp. 841–860, 1985.

[3] T. Harada and M. Yamashita, “Nondominated coteries on graphs,” *IEEE Transactions on Parallel and Distributed Systems*, Vol. 8, No. 6, pp. 667–672, June 1997.

[4] T. Ibaraki and T. Kameda, “A theory of coteries: Mutual exclusion in distributed systems,” *IEEE Transactions on Parallel and Distributed Systems*, Vol. 4, No. 7, pp. 779–793, July 1993.

[5] A. Kumar, “Hierarchical quorum consensus: A new algorithm for managing replicated data,” *IEEE Transactions on Computers*, Vol. 40, No. 9, pp. 996–1004, Sep. 1991.

[6] M. Maekawa, “A $\sqrt{N}$ algorithm for mutual exclusion in decentralied systems,” *ACM Transactions on Computer Systems*, Vol. 3, No. 2, pp. 145–159, May 1985.

[7] M. L. Neilsen and M. Mizuno, “Coterie join algorithm,” *IEEE Transactions on Parallel and Distributed Systems*, Vol. 3, No. 5, pp. 582–590, Sep. 1992.